**University of Warsaw**
Faculty of Mathematics, Informatics and Mechanics

# General paradigm for distilling classical key from quantum states - on quantum entanglement and security

*PhD dissertation*

**Karol Horodecki**

**University of Gdańsk**
Faculty of Mathematics, Physics and Informatics

**Thesis Supervisor**
**dr hab. Andrzej Szepietowski, prof. UG**
**University of Gdańsk**
**Institute of Informatics**

Gdańsk, May 2008

Author's declaration:
aware of legal responsibility I hereby declare that I have written this dissertation myself and all the contents of the dissertation have been obtained by legal means.

| | |
|---|---|
| ..... | ..... |
| date | *Karol Horodecki* |

Supervisor's declaration:
the dissertation is ready to be reviewed.

| | |
|---|---|
| ..... | ..... |
| date | *Andrzej Szepietowski* |

*"The wrok on both mathematical theory of communications and the cryptology went forward concurrently from about 1941. I worked on both of them together and I had some of the ideas while working on the other. I wouldn't say one come before another - they were so close together you couldn't separate them"*
*C. Shannon*

*"(...) Błogosławiony niech będzie chaos*
*albowiem z niego wyłoni się forma*

*niech będzie błogosławione swiatło*
*albowiem ono oddzieli nas*
*od ciemności"*
*R. Horodecki*

# Ogólny schemat otrzymywania klucza kryptograficznego ze stanów kwantowych - kwantowe splątanie i bezpieczeństwo[1]

**Słowa kluczowe:**
kwantowa kryptografia, stany bezpieczne, kwantowe splątanie, klucz destylowalny, stany o związanym splątaniu

**AMS Matematyczna Klasyfikacja Dziedzin 2000:**
81P68, 8102 Kwantowe obliczanie i kwantowa kryptografia. Prezentacja badań

Jednym z istotnych problemów kryptografii, jest wytworzenie losowego ciągu bitów tak, aby był znany jedynie zufanym nadawcy i odbiorcy, którzy są oddaleni od siebie. Kwantowa kryptografia pozwala rozwiązać ten problem. Podstawową własnością, która gwarantuje bezpieczeństwo kwantowej kryptografii, jest fakt, że jeśli mierzymy kubit w nieznanym stanie, z dużym prawdopodobieństwem zaburzamy jego stan, próbując go poznać. Niestety, praktyka wykazuje że, trudno wykorzystać tą własność w dowodach bezpieczeństwa kwantowych protokołów rozdzielania klucza. Na szczęście, znany jest inny fenomen - kwantowe korelacje zwane *czystym splątaniem* - który jest użyteczny w dowodach kwantowego bezpieczeństwa. Są to korelacje między dwoma podukładami układu współdzielonego przez osoby zaufane (Alicję i Boba) który jest w tzw. stanie czystym. Jeśli korelacje te są maksymalne miedzy dwoma kubitami, można je w wyniku pomiaru zamienić na jeden bit bezpiecznego klucza, zwanego dalej również kluczem 'klasycznym'.

Teoria splątania rozwijała się równolegle, pozostając w widocznym związku z kwantową kryptografią. W szczególności, znane są protokoły kwantowego rozdzielania klucza bazujące na czystym splątaniu częściowo i lub wyłącznie bazujące na czystych stanach splątanych. Z tego powodu oraz z uwagi na fakt, że czyste splątanie jest często wykorzystywane w dowodach bezpeczeństwa, naturalnym mogło się wydawać że czyste splątanie stanów kwantowych jest jedynym źródłem kwantowego bezpeczeństwa.

Mamy jednak nie tylko czyste splątane, ale również *mieszane* splątane stany kwantowe. Te ostatnie są probabilistycznymi mieszankami stanów czystych. Ich rozkład prawdopodobieństwa może być interpretowany jako nasza niewiedza o tym, w którym ze stanów czystych dwuukladowych znajduje się układ. Wiadomo, że aby dwuukładowy stan zawierał bezpieczny klucz, musi być stanem splątanym. Wiadomo także, że niektóre *mieszane* stany splątane nie mogą być przetransformowane w stany

[1]Praca powstała przy częściowym wsparciu Fundacji na rzecz Nauki Polskiej, oraz Europejskiego Projektu Zintegrowanego SCALA 015714.

czyste splątane, kiedy są współdzielone przez dwie osoby odległe od siebie (zwane też *stanami o związanym splątaniu*).

Mimo że związek między czystym splątaniem i kwantowym bezpieczeństwem jest całkiem dobrze znany, rozumienie relacji miedzy kwantowym bezpieczeństwem i kwantowym splątaniem w ogólności *mieszanych* stanów kwantowych (które nie są czyste) nie jest dostatecznie rozwinięte. Umotywowani tym faktem, w niniejszej rozprawie rozważamy następujące problemy:

- Z jakich stanów bezpiecznych można otrzymać przez pomiar *bezpośrednio dostępny*, klasyczny klucz ?
  Charakteryzujemy dwuukładowe stany $\rho_{AB}$, które mają *bezpośrednio dostępny klasyczny klucz*, w postaci stanów, które nazwaliśmy *stanami bezpiecznymi*. Stany bezpieczne są splątane, ale w ogólności są stanami *mieszanymi*. Stany czyste, maksymalnie splątane, stanowią przykład stanów bezpiecznych. Przez *bezpośrednią dostępność* rozumiemy dostępność za pomocą pomiarów von Neumanna na podukładach $A$ i $B$. Rozważamy również inne, równoważne formalizacje bezpośredniej dostępności. (Rozdział 3)

- Jak mierzyć zawartość bezpieczeństwa stanów kwantowych ?
  Zawartość bezpieczeństwa stanu $\rho_{AB}$ definiujemy na dwa sposoby (i) jako *klucz destylowalny* $K_D$, otrzymywany w formie stanów bezpiecznych za pomocą *lokalnych operacji i klasycznej komunikacji* (LOKK) (ii) jako *klasyczny klucz destylowalny* $C_D$, otrzymywany w formie trójukładowych stanów reprezentujących bezpieczny klucz za pomocą *lokalnych operacji i publicznej (dostępnej dla podsłuchiwacza) komunikacji*. Pokazujemy, że $C_D(|\psi_\rho\rangle\langle\psi_\rho|_{ABE}) = K_D(\rho_{AB})$, gdzie $|\psi_\rho\rangle\langle\psi_\rho|_{ABE}$ jest *puryfikacja* dwuukładowego stanu $\rho_{AB}$. (Rozdział 4)

- Jakie są własności splątania stanów bezpiecznych ?
  Niektóre stany bezpieczne mają więcej destylowalnego klucza $K_D$ niż destylowalnego (czystego) splątania $E_D$. Niektóre, w wyniku pomiaru pojedynczego kubitu tracą znacząco tzw. *koszt splątania*, wykazując efekt zwany *blokowaniem splątania*. (Rozdział 3, Sekcja 3.5)

- Czy można otrzymać bezpieczny klucz ze stanów o związanym splątaniu ?
  Dajemy pozytywną odpowiedź na to pytanie podając przykłady stanów o związanym splątaniu. Niektóre z nich są specyficzną miesznką dwóch ortogonalnych stanów bezpiecznych. Rezultat ten implikuje, że w niektórych przypadkach można skomunikować się bezpiecznie używając kwantowego bezpeczeństwa mimo, że nie można w sposób wierny komunikować kwantowaych danych. (Rozdział 5)

- Jak łatwo jest odróżnić stan bezpieczny od jego zaatakowanej wersji, kiedy jeden z nich jest współdzielony przez odległe od siebie osoby ? Wykazujemy, że niektóre stany bezpieczne są trudno odróżnialne za pomoca operacji LOKK od stanów niebezpiecznych (niesplątanych). Liczba kopii potrzebna do odróżnienia bezpiecznego bitu $\gamma^{(2)}$ od jego zaatakowanej wersji jest conajmniej proporcjonalna do odwrotności *logarytmicznej ujemności* $\gamma^{(2)}$. (Rozdział 6)

Oprócz powyższych rezultatów, przywołujemy pokrótce niektóre z rezultatów badań ostatnich lat, otrzymanych w kontekście stanów bezpiecznych. Prezentujemy również pewne problemy otwarte.

# General paradigm for distilling classical key from quantum states - on quantum entanglement and security[2]

**The Keywords:** quantum cryptography, private states, quantum entanglement, distillable key, bound entangled states

**AMS Mathematical Subject Classification 2000:**

81P68, 8102 Quantum computing and quantum cryptography, Research exposition

## Abstract

One of the important problems of cryptography is how to generate a random sequence of bits, so that it will be known only to the honest parties that are far apart from each other. Quantum cryptography allows to resolve this problem. The fundamental property which guarantees security of the quantum cryptography is that if one does not know the state of a qubit, then with a high probability one disturbs the state while trying to get to know it. Unfortunately, this property appeared to be not easy in use when proving security of quantum key distribution protocols. There is however another phenomenon - quantum correlations called *pure entanglement*, which are quite useful in proving security. These are correlations between two subsystems of a system shared by Alice and Bob, that is in a pure quantum state. If such correlations are maximal, between two qubits, they can be changed via measurement into one bit of a secret key (also called further 'classical' key).

Theory of entanglement has been developed in parallel, and with apparent connection to quantum cryptography. In particular, there are known protocols of quantum key distribution based partially or solely on pure entangled states. This, together with the fact that security proofs often base on pure entanglement, has made natural expectation, that pure entangled quantum states are the only source of quantum security.

There are however not only pure entangled quantum states, but also *mixed* entangled quantum states. The latter are certain probabilistic mixtures of pure quantum states, where the mixing probability can be interpreted as our lack of knowledge in which pure quantum state the bipartite system resides. It is known, that to contain security, a bipartite state must be entangled. Moreover, there are some *mixed* entangled quantum states can not be changed into pure entangled ones, if shared by two distant parties (called *bound entangled states*).

[2]This PhD thesis has been partially supported by Foundation for Polish Science and EU grant IP SCALA 015714.

Although the link between *pure entanglement* and quantum security is quite well developed, the understanding of the relation between quantum security and entanglement of in general *mixed* (impure) quantum states is still in its infancy. Therefore, natural questions arise, that we address in this thesis:

- What are the quantum bipartite states, which have *directly accessible*, classical key ?
  We characterize the bipartite states $\rho_{AB}$, that have *directly accessible* classical key, to be the one that we have called *private states*. The private states are entangled, but in general *mixed*. The pure maximally entangled states are examples of private states. By *direct accessibility* we mean the accessibility via complete von Neumann measurements on *subsystems* of $A$ and $B$. Equivalence of this approach with other formalizations of direct accessibility is also considered.

- How to quantify security content of a bipartite quantum state ?
  We define the secure content of $\rho_{AB}$ in two ways (i) as *distillable key* $K_D$ obtainable in form of a private state via *local operations and classical communication* (LOCC) and (ii) as *classical distillable key* $C_D$, obtainable in form of tripartite states representing secure key via *local operations an public (listened to by Eve) communication*. We show that $C_D(|\psi_\rho\rangle\langle\psi_\rho|_{ABE}) = K_D(\rho_{AB})$, where $|\psi_\rho\rangle\langle\psi_\rho|_{ABE}$ is the *purification* of the bipartite state $\rho_{AB}$. This means that the secure content of a bipartite quantum state is an entanglement measure. We then show, that $K_D$ is upper bounded by an entanglement measure called the *relative entropy of entanglement*. (Chapter 4)

- What are the properties of entanglement of the class of private states ?
  Some private states have more distillable key $K_D$, than distillable (pure) entanglement $E_D$. Some of them after measurement of a single qubit loose drastically an *entanglement cost*, exhibiting effect called *locking of entanglement*. (Chapter 3, Section 3.5)

- Can one obtain secure key from bound entangled states ?
  We answer in positive to this question, providing examples of bipartite states having $E_D = 0$, and still $K_D > 0$. This result implies, that in some cases, one can communicate in private using quantum security, without having possibility for communicating faithfully quantum data. (Chapter 5)

- How easy it is to distinguish the private state from it's attacked copy, when either of two is shared by the honest parties that are far apart?
  Some private states are proved to be hardily distinguishable from insecure

(disentangled) states via LOCC operations. The number of copies needed to distinguish a private bit $\gamma^{(2)}$ from its attacked copy with probability close to one, is shown to be at least proportional to the inverse of the log-negativity of $\gamma^{(2)}$. (Chapter 6)

Apart from the above results, we invoke some of the further research that has been conducted in context of private states in recent years. We collect also some open problems.

## Acknowledgments

Very little of the work presented here would be possible if it was not for the collaboration with Jonathan Oppenheim, and my brothers Michał and Paweł. My thanks are thus to those three, who let me co-work on interesting questions of quantum cryptography and quantum entanglement, and thereby to learn much about the formalism of quantum information theory.

Special thanks are to my brother Michał, who has invited me to quantum information theory, and was the first teacher, already in 1999. It is pleasure to thank Him for the hours spent on 'quantum discussions'.

I would like to thank my supervisor, Andrzej Szepietowski, for his kind assistance during my studies and further PhD studies at UG, that let me shift from 'classical' toward 'quantum'. I also thank Him for patient, and constructive critique, without which this thesis would be simply unreadable. All mistakes that remains in text are on my responsibility.

It is time I thank all the colleagues in quantum, with whom I have discussed or could work with. First, Additi and Ujjwal Sen (De), Jonathan Oppenheim, Barbara Synak-Radtke, Wiesiek Laskowski, Marcin Wieśniak, Andrzej Grudka, Łukasz Pankowski, Marco Piani, Piotr Badziag, Remigiusz Augusiak, Fernando G.S.L. Brandao and Dong Yang, that I could work with in Gdańsk, second Matthias Christandl, Debbie Leung, Hoi-Kwong Lo, Daniel Gottesman, John Smolin and Andreas Winter, most of whom I have met first in Isaac Newton Institute in Cambridge on the scientific programme in 2004. Special thanks are to Debbie, for inviting me to the ICQ of the Waterloo University.

Many thanks are to my mother Jadwiga and sister Justyna for their love and support throughout much of the time. Of course, special thanks are to brothers and my father Ryszard, for encouraging me to join their team.

I want to say also thanks to my friends: Marysia, Ania, Ela, Marek, Łukasz and Tadeusz, to friends from St. Nicola's church, especially those from the St. Nicola's choir, for they let me always take a deep breath of song, talk, and cultural events that we have taken part in together.

# Contents

# Chapter 1

# Introduction

## 1.1 Motivation

One of the well known encryption algorithms is the *one-time pad* due to Vernam and Mauborgne [Ver26, wik08a]. According to this algorithm, the cypher-text $C$ is just a random sequence $R$ of bits added one by one to the bits of the message $M$. Providing the sender and receiver share the same random sequence which is unknown to anybody else, the message is provably secure, as it was shown by Shannon [Sha49]. Due to his proof, any encoding scheme to be secure must bring in a key $R$ which has at least that much of randomness as the message $M$ itself . In other words in one-time pad, the key $R$ must be as long as the message $M$. This is the main drawback of this cypher, summarized in the following problem:

- How to create at a distance a copy of a long random sequence, so that it will be known only to the honest sender and receiver (traditionally called Alice and Bob) ?

Quantum cryptography initiated by Wiesner [Wie83] and Bennett and Brassard [BB84] allows to resolve the above problem. Bennett, and Brassard proposed the protocol based on sending qubits - the counterparts of classical bits. The task of such a protocol (called *quantum key distribution protocol*) is exactly the generation of a random bit string secretly shared between Alice and Bob. To this end, Alice and Bob use a quantum communication channel for sending qubits and an authentic[1] *classical*

[1] Assuming authentic communication channel we assure that Alice and Bob do talk to each other, so that the so called man in the middle attack is excluded. Authentication of messages needs relatively small, but nonzero amount of a secret key shared in advance by the honest parties. For this reason, quantum key agreement is called sometimes a *quantum key growing*.

communication channel for sending classical bits. Security of the quantum key distribution protocols can be derived from axioms of quantum mechanics - a physical theory. In other words, quantum security bases on the fact that an eavesdropper (Eve), has to obey the rules of quantum mechanics, which are widely accepted as they are confirmed by many experiments.

The fundamental property which guarantees security of the quantum cryptography is that if one does not know the state of a qubit, then with a high probability one disturbs the state while trying to get to know it. Unfortunately, this property appeared to be not easy in use when proving security of quantum key distribution protocols. There is however another phenomenon - quantum correlations called *pure entanglement*, which are quite useful in proving security. These are correlations between two subsystems of a system shared by Alice and Bob, that is in a pure quantum state. If such correlations are maximal, between two qubits, they can be changed via measurement into one bit of secret key, also called further 'classical' key.

In recent years a kind of link between security and pure entanglement has been established. In particular, there are known protocols of quantum key distribution based partially or solely on pure entangled states. This, together with the fact that security proofs often base on pure entanglement, has made natural expectation, that pure entangled quantum states are the only source of quantum security.

There are however not only pure entangled quantum states, but also *mixed* entangled quantum states. The latter are certain probabilistic mixtures of pure quantum states, where the mixing probability can be interpreted as our lack of knowledge in which pure quantum state the bipartite system resides. It is also known, that some *mixed* entangled quantum states can not be change into pure ones, if shared by two distant parties.

Although the link between *pure entanglement* and quantum security is quite well developed, understanding of the relation between quantum security and entanglement of in general *mixed* (impure) quantum states is still in its infancy. It is known, that entanglement is necessary condition for security, and a protocol for obtaining classical key from certain mixed states is known, however the characterization of states from which secure key can be obtained is still an open problem. For this reason, natural questions arise which we address in this thesis. The first is a consequence of the fact, that the classical key can be obtained from quantum state in a more or less involved way:

- What are the quantum bipartite states (called further *private states*) which after measurement gives *directly accessible*, classical key ? (Chapters 3 and 4).
- What are the properties of entanglement of the class of private states ? (Chapter 3, Section 3.5)

- How to quantify security content of a bipartite quantum state ? (Chapter 4)
- Can one obtain secure key from entangled quantum states from which no pure entanglement can be obtained [DW05, DW04]? (Chapter 5)
- How easy it is to distinguish the private state from it's attacked copy, when either of two is shared by the honest parties that are far apart? (Chapter 6)

In this thesis we will try to answer the above questions by characterizing class of the quantum states that have secure key (the private states) and using the latter class showing a direct, quantitative link between notions of security obtained from quantum states and entanglement in general.

## 1.2 Quantum cryptography - the idea

Quantum cryptography is a domain of *quantum information theory* that is a fusion of two domains: quantum mechanics and classical information theory. Quantum mechanics, discovered by Planck, Schröedinger, Hiesenberg and Dirac and axiomatized by Landau and von Neumann [NC00] in 30's of XXth century, is up to now the best known physical description of the micro world, and has been confirmed in many experiments. The classical information theory founded by Shannon [Sha48] dates back to 40's of XXth century. It provides a framework for quantification of classical information content of data. Within quantum information theory one asks about new possibilities and restrictions connected with processing and communicating information 'written' on qubits - carriers which exhibits the inherent properties of quantum mechanics.

The birth of the quantum cryptography in 70's of XXth century is due to S. Wiesner [Wie83], who first proposed the use of a discrete quantum systems to store binary information, taking advantages of the rules of quantum mechanics. Unfortunately, Wiesner's proposal was not appreciated that time. His seminal paper rejected by a famous journal, has been published in SIGACT News only in 1983. Subsequently, taking much of the spirit of his approach, C. H. Bennett and G. Brassard [BB84] discovered the first quantum cryptographic protocol (called BB84 after its inventors). The essence of the Wiesner's and Bennett and Brassard's idea can be summarized in the following statement:

- In order to protect a private information one should encode it in such a way, that reading it without additional a priori knowledge would be equivalent to violation of the rules of quantum mechanics.

The classical information is encoded in *bits* - systems, that can be in one of the two states '0' or '1'. The basic notion of quantum information theory is a quantum bit (called a qubit). It is a two-level quantum system which can be not only in states '0' and '1', but also in some intermediate state, that is a *superposition* of these two basis states. The possible states of qubit are then written using Dirac notation as follows[2]:

$$a|0\rangle + b|1\rangle, \tag{1.1}$$

with a and b being the complex numbers that satisfy $|a|^2 + |b|^2 = 1$, and $|0\rangle, |1\rangle$ representing column vectors $(1,0)^T$ and $(0,1)^T$ respectively.

The BB84 protocol allows for generation of a random correlated bits, unknown to Eve, between Alice and Bob linked by a quantum communication channel and an authentic classical communication channel. It is based on *single* qubits, send via the quantum channel (usually an optical fiber) from Alice to Bob. The clue is that Alice sends the qubits set in a state represented by random basis vectors of one of two (again randomly chosen) *basis*: $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$.

According to quantum mechanics, a state measured in some basis is set to be one of the state of this basis. Measurement in a basis, can be viewed, as "asking" in which of basis state the system resides. For example, if a qubit was in state $a|0\rangle + b|1\rangle$, then when measured in basis $\{|0\rangle, |1\rangle\}$ it will change its state to $|0\rangle$ or $|1\rangle$ with probabilities $|a|^2$ and $|b|^2$ respectively.

If an eavesdropper Eve does not know how to measure a qubit, she is likely to change its state which will be detected by Alice and Bob since they can cooperate to compare the send and received data. Thus at the heart of the first protocol of quantum cryptography lays the idea that is often phrased as "information gain implies disturbance".

In this thesis we deal with scenario connected to a different type of a quantum key distribution protocols - the *entanglement* based ones. The first such protocol was proposed by A. Ekert in 1991 [Eke91]. According to his idea, Alice and Bob are provided with pairs of quantumly correlated qubits (entangled qubits) which via measurement and appropriate post processing give a random, correlated, unknown to anyone else string of bits - a secure key.

## 1.3 Quantum entanglement - general facts

The phenomenon that the two particles can be correlated in a "quantum" way has been already observed by Schrödinger [Sch35]. In quantum information theory it is

[2] In fact, the state is represented by a $2 \times 2$ matrix $\begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix}$, see Section 2.1.

one of the central notions which allows for various quantum communication setups [HHHH07]. The best known example of an entangled state[3] is of the following form:

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B), \tag{1.2}$$

and is called a *singlet* state [4]. It is also called an EPR pair (of qubits), as it was erroneously speculated by Einstain, Podolsky and Rosen that properties of this state could prove inconsistency of quantum mechanics [EPR35].

The singlet state is an equal superposition of two *bipartite* states: $|0\rangle \otimes |1\rangle$ and $|1\rangle \otimes |0\rangle$. The subscripts $A, B$ reminds, that the first subsystem is with Alice and the second with Bob. Now, after measuring the subsystems in $\{|0\rangle, |1\rangle\}$, leaves Alice's and Bob's joined state with equal probability in one of these two states: either $|0\rangle_A \otimes |1\rangle_B$ or $|1\rangle_A \otimes |0\rangle_B$. According to quantum mechanics, since the initial state (before measurement) was pure (represented by a single vector), nobody except Alice and Bob could have been correlated with this state and know the result of the measurement. It follows then, that a singlet state can be viewed as a source of one bit of secure correlations. The notable manifestation of entanglement of this state is the fact that sharing singlet and having possibility to send two bits of information, Alice can 'transport' a state of a qubit to Bob [BBC$^+$93]. The protocol which realizes this task is called a *quantum teleportation*.

It is worth noting, that the state (1.2) is represented by a single vector. For this reason it is called a *pure state*, and its entanglement content is called a *pure entanglement*. In fact, the singlet state contains maximal amount of entanglement, and hence belongs to a larger class of states called *maximally entangled states*.

In reality however, one usually deals with imperfect sources of entanglement, and in consequence with *mixed entangled states* (also 'noisy' entangled states). This is when one does not have certainty about the state of a quantum system. For example, the state:

$$\rho_{noisy} = p|\psi_-\rangle\langle\psi_-| + (1-p)|0\rangle_A \otimes |0\rangle_B\langle 0|_A \otimes \langle 0|_B, \tag{1.3}$$

is a mixture of two states: with probability $p$ it is the singlet state defined above [5] and with probability $(1-p)$ it is a product of two pure states: $|0\rangle_A$ with Alice and $|0\rangle_B$ with Bob.

[3] Here and further in this chapter, for simplicity we sometimes say that some states are represented by vector $|\psi\rangle$, although formally, as it is explained in next chapter, they are represented by *projector* onto this vector denoted as $|\psi\rangle\langle\psi|$.

[4] For shortening notation, we will denote $|i\rangle_A \otimes |j\rangle_B$ often as $|i\rangle_A|j\rangle_B$ or $|ij\rangle_{AB}$ or even $|ij\rangle$, if the labels of subsystems are known from the context.

[5] The notation $|\psi_-\rangle\langle\psi_-|$ is up to irrelevant complex factor of modulus 1 an equivalent matrix representation of a normalized vector $|\psi\rangle$ (see the next chapter)

Entanglement is defined by saying which states are *not* entangled. According to definition of Werner [Wer89] the state is not entangled if and only if it can be written in a form

$$\sigma = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \tag{1.4}$$

where again $\rho_X^{(i)}$ is a quantum state localized at site $X$ (A for Alice and B for Bob) and the probabilities $p_i$ forms a distribution. In such a case, the state is called *separable*. If a state is not separable, it is entangled.

Due to phenomenon of mixed entangled states, it was important to ask if one can draw secure key from noisy singlets. The crucial idea of distillation of singlet state was introduced by Bennett and coauthors in [BBP$^+$96, BDSW96]. Namely, from many pairs of mixed state $\rho_{AB}$, Alice and Bob should try to obtain some (usually smaller) number of pairs of qubits in a singlet state using (L)ocal quantum (O)perations and (C)lassical (C)ommunication (LOCC) that is making quantum operations in their laboratories and communicating e.g. via a mobile phone. The amount of pure entanglement that can be extracted in this scenario, called *LOCC scenario* (or equivalently the *distant laboratories* scenario), is called distillable entanglement $E_D(\rho)$ of a state $\rho$. It is equal to the maximal ratio $\frac{k}{n}$ of the number of singlet states $k$ that can be gained from $n$ copies of a state $\rho$.

Establishing the paradigm of distant laboratories has led to development of theory of entanglement in quantitative way through the notion of *entanglement measure* [VPRK97, VP98, Vid00]. The first entanglement measure [6] was just the mentioned distillable entanglement. An entanglement measure that accompanies $E_D$ is called *entanglement cost* $E_C$. It amounts to a minimal ratio of singlet states $k$ that are needed in order to create $n$ copies of the state $\rho$ by means of LOCC operations.

There are known examples of noisy entangled states that can be distilled, i.e. have $E_D > 0$ [BBP$^+$96, BDSW96]. However due to M. Horodecki and coauthors [HHH98], not all mixed entangled states can be transformed to a singlet state. Such states which are entangled (one needs pure entanglement to create them by LOCC), but from many copies of which one can not obtain a singlet state by means of LOCC operations are called *bound entangled states*. Hence, the bound entangled states are those which fulfill simultaneously $E_C > 0$ and $E_D = 0$. The set of states which are bound entangled has not been fully characterized yet. It is known however, that it includes the so called PPT entangled states, that is those entangled states which remain positive under partial transposition[7].

[6] Formally, entanglement measure (in bipartite case) is a function of a bipartite state that fulfills certain *axioms of entanglement measures*, in particular a most constitutive one: not increasing under LOCC operations.

[7] State is PPT if it has (P)ositive (P)artial (T)ransposition that is if $(\mathrm{I}_A \otimes T)\rho_{AB} \geq 0$ for $T$ being

## 1.4 Pure entanglement and quantum cryptography - historical background

As it was already mentioned, the first who used entangled states in quantum cryptography was A. Ekert [Eke91]. According to his proposal, Alice and Bob are provided some number of singlet states. In ideal case, after measuring $n$ singlets $|\psi_-\rangle^{\otimes n}$ each in a basis $\{|0\rangle, |1\rangle\}$, Alice and Bob would obtain $n$-bit, anticorrelated random string. However, since the provider may be in particular just Eve, Alice and Bob can not trust that they were given what they expected to. According to the most general attack called *coherent*, Eve can provide them a big entangled state of $n$ systems $\rho_{AB}^{(n)}$.

In order to rule out the coherent Eve's attack, Ekert proposed that Alice and Bob should sacrify some singlets, to verify if they are able to extract key. Another protocol (BBM) based on singlet was proposed by Bennett, Brassard and Mermin [BBM92]. According to BBM protocol, Alice and Bob measure some singlets in $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ basis and compare if they have anti correlated results. If there are too few of such results, they abort the protocol. It was the first protocol which was based solely on the fundamental fact, that a quantum bipartite system carries the information about its correlations with other systems. Yet, it based on the fact that singlet is a *pure* state, i.e. the state of system that is fully uncorrelated from other systems.

In both Ekert's and BBM protocol, there was an unreal assumption that every noise is introduced by Eve, so if only the honest parties detect her presence, they abort the protocol. As a cure, in [DEJ$^+$96] the process of distillation of singlets was proposed and called a quantum privacy amplification: Alice and Bob should first distill singlets and then generate the key via measurement on almost ideal singlet states.

The pure entanglement-based protocols mentioned above assumed ideal Alice's and Bob's operations, and were not proved to be secure. The first pure-entanglement based protocol security of which was proved, was provided by Lo and Chau [LC99].

The protocol of Lo and Chau, after suitable modification was then used by Shor and Preskill [SP00], to prove in a simply way the security of BB84 protocol. This was the breakthrough which allowed to prove security of many other single-particle based protocols.

The fact, that most of the techniques developed in order to prove security of quantum key distribution protocols were based on obtaining of *pure* entangled states (singlets), has supported the belief, that singlet and in general pure entangled states are the only source of security.

---

operation of transposition of matrix of the state $\rho_{AB}$.

## 1.5 Quantum security beyond pure entanglement

The usefulness for security of entanglement of *mixed* states that is not associated with possibility of distillation of entanglement was first studied by Aschauer and Breigel in [AB02]. They showed, that even if Alice and Bob perform their operations imperfectly, which do not allow them to distill pure entanglement, they can have secure correlations. The Authors introduce the notion of *private entanglement*, i.e. such type of correlations that are shared only by the honest parties, although the parties can not have full access to it.

The qualitative link between entanglement and security (of in general mixed states) has been established by Curty et al. [CLL04a, CGLL05] who showed, that a quantum state from which one obtains secure correlations must be entangled.

### 1.5.1 LOPC, classical key agreement, and collective attacks scenarios

As it was mentioned, most of the security proofs for quantum key distribution protocols use reduction of security to the situation where either Alice or some external provider distributes some entangled states between Alice and Bob while Eve can manipulate with these states in arbitrary way, i.e. perform the *coherent* attack. The generality of these attacks is the main reason for difficulty of any proof of security of quantum key distribution protocols. In [BM97] a substantially restrictive attack was introduced called the *collective attack*, against which security of some protocols can be proved in much easier way [BBB$^+$98].

Namely, Eve attacks each passing state using *the same strategy*: attaching an 'ancillary' system individually to each of the state being distributed between Alice and Bob, and performing some fixed unitary transformation between the state and her system, and taking ancillary system with her, letting the state be distributed between the parties. She then keeps all the additional systems in her lab, and listen to the communication that Alice and Bob exchange via public authenticated channel. Only then, she may decide to measure their systems. The measurement can involve many systems, hence the name 'collective' of this attack.

In the above scenario, which we will refer to as *CAS*, before Alice and Bob launch their operations, in order to obtain key from shared states, the total state shared by Alice, Bob and Eve is of the form $|\phi\rangle\langle\phi|_{ABE}^{\otimes n}$, that is $n$ copies of *the same* pure state $|\phi\rangle\langle\phi|_{ABE}$, such that Alice and Bob have access to its A and B subsystems respectively, and Eve to the subsystem E.

Originally, the security condition imposed on the output state of Alice and Bob in this scenario was that Eve should have small classical correlations (measured by Shannon's mutual information) with the bits of final key, they have extracted. It is

further replaced by the so called *composable* security conditions [BOHL$^+$05a].

In [DW05, DW04], the so called LOPC scenario as the quantum analogue of classical cryptographic concept of *secure key agreement* (called also classical key agreement [GW00]). The secure key agreement originating from the information-theoretic approach of Shannon, was first studied by Wyner [Wyn75] and developed by Csiszár and Körner, Maurer [Mau93] and Ahlswede and Csiszár in [CK78, AC93]. According to secure key agreement, Alice Bob and Eve share triples of random variables with some joint distribution $P(A, B, E)$. Alice and Bob try to obtain from them the key for one-time pad encryption, using public (listened to by Eve) discussion.

In LOPC scenario, Alice and Bob and Eve share $n$ copies of a tripartite quantum state $\rho_{ABE}$, each having access to its subsystem $A$, $B$ and $E$ respectively. Alice and Bob try to transform the bipartite subsystems $AB$ that they share into states useful for one-time pad encryption. To this end they perform Local operations (each on its share) and communicate via public (insecure, but authenticated) channel, so that Eve can listen to this communication. The state $\rho_E$ represents total knowledge of Eve, after the protocol of key distillation is finished.

The security condition imposed on the output states is that for every realization of the key bit-string $K = k$ on Alice's and Bob's subsystem, which should happen with almost uniform probability, the state of Eve's subsystem after the whole public discussion is almost *the same*.

Within this scenario, it has been shown in [DW05, DW04], that on an input state of the form

$$\rho_{cqq} = \sum_i p_i |i\rangle\langle i|_A \otimes \rho_{BE}^{(i)}, \tag{1.5}$$

one can obtain distillable key denoted as $K_D$ at a rate analogous to the formula of Csiszáar and Körner's bound:

$$K_D > I(A:B)_\rho - I(A:E)_\rho, \tag{1.6}$$

with $I(X:Y)_\rho$ being the quantum mutual information [8] - a quantum analogue of classical mutual information. The protocol which achieves the above rate of distillable key, we called further as the Devetak-Winter protocol.

The interrelation between classical key agreement and the quantum information theory has been first explicitly stated by Gisin and Wolf [GW00]. In particular it is observed there that this link can lead to better understanding of the classical key agreement itself. (for further development see [CP02, AMG03, ACM04], and a review of this subject [HHHH07]).

[8] Quantum mutual information is defined as follows: $I(A:B)_\rho = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$ where $S(\rho_X)$ denotes the von Neumann entropy (Shannon entropy of the eigenvalues) of the subsystem $X$ of the state $\rho_{AB}$

**The worst case of LOPC scenario**

In classical key agreement, there is no a priori restriction on the Eve's knowledge about the Alice's and Bob's data. Indeed, given Alice and Bob share a realization of a random variable $A$ and $B$, respectively, with a joined probability distribution $P(A, B)$, Eve can be arbitrarily correlated with them: there is no restriction on distribution $P(A, B, E)$ apart from the fact, that its AB marginal should be $P(A, B)$. In particular Eve can have *a copy* of their data so that $E = AB$.

What is fundamental to all further investigation in this thesis is the fact, that the above situation does not hold when we go to quantum. This is because an unknown quantum state can not be *perfectly copied* [WZ82, BH98]. When Alice and Bob share a bipartite state $\rho_{AB}$, the maximal access that Eve can have is up to irrelevant transformation uniquely defined and is called the *purification* of the state $\rho_{AB}$ (see Section 2.3.2 and 2.9). We will refer to this scenario as to the (quantum) worst-case senario.

Consequently, as it was noted in [DW05, DW04], the worst case in LOPC scenario from cryptographic point of view is when $\rho_{ABE}$ is a *pure state*, so that the LOPC scenario is then a special case of the worst-case senario as we described above. This fact implies also, that the CAS as described in Section 1.5.1, is a special case[9] of the worst-case LOPC scenario: the three parties share many copies of pure states, and process it via LOPC operations (see [DLH01]).

## 1.6 Related research - distinguishing via LOCC operations

The *LOCC distinguishing scenario* has been considered initially by Bennett et al. in [BDF$^+$99, BDM$^+$99]. In the simples case, according to this scheme, Alice and Bob are given a bipartite state which is one of the two $\rho_1$ or $\rho_2$. Their task is to distinguish between them with the highest possible probability of success, by means of LOCC operations.

In [BDF$^+$99, BDM$^+$99] it is shown, that there is a set of pure orthogonal states, which can not be distinguished with certainty by means of LOCC operations (see [WH02, WSHV00]). It was then shown by Leung, Terhal and DiVincenzo [TDL01, DLT02], that there are pairs of mixed states which are (i) almost orthogonal (i.e. distinguishable almost perfectly by quantum operations) but (ii) nearly indistinguishable by LOCC operations, hence called *hiding states*. Their result can be in-

[9] There only minor differences: (i) CAS was originally equipped with different security condition imposed on the output states, that is not composable [BBB$^+$98, BM97, KRBM05]. (ii) in CAS Eve attacks preserving the dimension of the system send from Alice to Bob.

terpreted as the first result on hiding entanglement. Then, Eggeling and Werner [EW02], showed that the phenomenon of hiding bits holds even for separable states. Similar results, in different context has been obtained earlier by Matthews and Winter [MW07]. They show, that the symmetric and antisymmetric Werner states are hardily distinguishable, providing optimal LOCC strategy for distinguishing between them.

## 1.7 Contribution

The contribution of this thesis is generally of two kinds. On one hand it gives insight into quantum cryptography, while on the other it exhibits new phenomena in entanglement theory.

**Chapter 2** contains basic concepts and definitions. In **Chapter 3**, we study the structure of bipartite quantum states $\rho_{AB}$ that contain *directly accessible, classical key*. We assume, that the eavesdropper holds its purifying system in state $\rho_E$, so that there is a pure state $|\psi_\rho\rangle_{ABE}$ with $\mathrm{Tr}_E|\psi_\rho\rangle\langle\psi_\rho|_{ABE} = \rho_{AB}$ and $\mathrm{Tr}_{AB}|\psi_\rho\rangle\langle\psi_\rho|_{ABE} = \rho_E$. The classical key is represented by tripartite state

$$\rho_{key} = \left(\sum_{i=0}^{d-1} \frac{1}{d}|ii\rangle\langle ii|\right) \otimes \rho_E. \tag{1.7}$$

By *direct accessibility* we mean the accessiblity via the complete von Neumann measurements on *subsystems* of $A$ and $B$. In that we focus on states $\rho$ which have two parts: main part and side part. We say, that $\rho$ has directly accessible, classical key if after complete von Neumann measurements on (two subsystems of) main part and tracing out side part together with the purifying state $\rho_E$, it has the form of $\rho_{key}$.

We then define the class of private states, that consists of the main part $AB$ and side part $A'B'$, that are called, *key part*, and *shield* respectively. They are of the form:

$$\gamma_{ABA'B'} = U|\Psi_+\rangle\langle\Psi_+|_{AB} \otimes \rho_{A'B'}U^\dagger, \tag{1.8}$$

where unitary transformation $U$ has the form

$$U = \sum_{kl} |kl\rangle\langle kl| \otimes U_{kl}, \tag{1.9}$$

with $U_{kl}$ arbitrary unitary operations acting on a system $A'B'$ and $|\Psi_+\rangle = \sum_i \frac{1}{\sqrt{d}}|i\rangle_A \otimes |i\rangle_B$ is a maximally entangled state.

We show, that **bipartite states that have directly accessible, classical key are the private states**. We consider also other interpretations of *direct accessibility*,

including those used by other authors in context of private states [RS07, BHH$^+$08]. All they turn out to yield states that are equivalent to private states. Precisely, these states can be easily transformed (by local operations) into some private states, and vice versa (cf. [RS07, BHH$^+$08]).

Private state can be viewed a "twisted maximally entangled state", as it is originally a maximally entangled state $|\Psi_+\rangle$ on $AB$ subsystem, that gets "twisted" by the unitary transformation $U$ into a system $A'B'$. For this reason, we refer to the unitary transformation given in equation (1.9) as to *twisting*.

In **Chapter 4**, we give **definition of distillable key $K_D$ in terms of private states** and **definition of classical distillable key $C_D$ in terms of tripartite quantum states representing secure key** having the form of $\rho_{key}$.

Definition of $K_D$ involves the LOCC scenario: Alice and Bob are supplied $n$ copies of the state $\rho_{AB}$. Alice and Bob can operate on the $n$ copies of a state $\rho_{AB}$ with local quantum operations and communicate 'classically' with each other. Their task is to gain a (approximate) private state with the largest key part (say of $k$ qubits). $K_D$ is then the maximal ratio of $\frac{k}{n}$ in asymptotic limit.

Definition of $C_D$ involves the LOPC scenario, with slightly weaker condition, then that which was studied in [DW05, DW04]. Namely, we also require that Alice and Bob transform many copies of tripartite state $\rho_{ABE}$ via LOPC operations into some *tripartite* state $\rho^{out}$, yet in place of condition of Devetak and Winter, we impose that $\rho^{out}$ must be close to a state representing ideal secure key[10]:

$$||\rho^{out} - \rho^{key}_{ABE}|| \leq \epsilon \tag{1.10}$$

with $\epsilon$ arbitrarily small as a function of $n$. Hence, the task of Alice and Bob is to obtain the *approximate* $\rho^{key}_{ABE}$ with the largest possible amount of key-bits $k$ ($\log d$ according to (1.7). $C_D$ is then the maximal ratio of $\frac{k}{n}$ in asymptotic limit.

We then focus on the worst case of LOPC scenario, that is the case of the input state $\rho_{ABE}$ begin a *pure state*. We show, that:

$$C_D(|\psi_\rho\rangle_{ABE}) = K_D(\rho_{AB}) \tag{1.11}$$

where $|\psi_\rho\rangle_{ABE}$ is a purification of $\rho_{AB}$, that is after ignoring system $E$ of $|\psi_\rho\rangle_{ABE}$, the remaining bipartite state on $AB$ equals $\rho_{AB}$.

The function $K_D$ is an entanglement measure, because it does not increase under LOCC operation. Thus, the **classical distillable key in the worst case LOPC scenario is equal to an entanglement measure**, which provides quantitative link between quantum cryptography and theory of entanglement.

[10]This security condition that is proved to be composable in [BOHL$^+$05b].

This result enabled us to study security content of bipartite states using approach of entanglement theory. We show the **upper bound on distillable key**[11]:

$$K_D \leq E_r^{\infty}. \tag{1.12}$$

where $E_r^{\infty}$ is the regularized relative entropy of entanglement.

In **Chapter 5** we show, that there are bipartite states $\rho$ satisfying

$$K_D(\rho) > 0 \text{ and } E_D(\rho) = 0, \tag{1.13}$$

i.e. that **some bound entangled states are key distillable**. It means that distillability of pure entanglement is only sufficient, but not necessary condition of security. This result has important meaning, as it implies, that there are situations, in which **one can send bits in private, although one can not send faithfully qubits**. Some of the bound entangled key distillable states are special mixtures of two private states.

In **Chapter 6** we consider an *LOCC distinguishing scenario*. We mostly focus on the case when Alice and Bob are given an input bipartite state which is one of the two - a private state $\gamma$ or the $\gamma$ measured already on its key part by Eve (a 'key-part-attacked' private state) denoted as $\upsilon_\gamma$. We then ask how many copies of an input state they have to share in order to achieve the probability of success approaching 1. We show, that there is family of private states, for which this number scales exponentially with the number of qubits these states occupies.

In **Chapter 7** we summarize, focusing on the role of private states in the above results, and the fruitful interrelation between the quantum cryptography and theory of entanglement. In **Appendix** we collect some useful facts that serves a background to main considerations.

Most of these results is the outcome of collaboration with J. Oppenheim and M. and P. Horodeccy, that can be found in [HHHO05c] (extended in [HHHO05a]), as well as Ł. Pankowski and M. and P. Horodeccy presented in [HPHH05]. The content of this thesis is based on the following manuscripts:

1. K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94:160502, 2005. quant-ph/0309110 [HHHO05c]

2. K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim. General paradigm for distilling classical key from quantum states. *after positive reports, resend to IEEE Trans. Inf. Theor.*, 2005 quant-ph/0506189 [HHHO05a]

[11] This result was extended within theory of entanglement [CEH$^+$07], to hold for all entanglement measures satisfying some axioms ( asymptotic continuity, convexity, and sub-normalization on private states).

3. K. Horodecki, Ł. Pankowski, M. Horodecki and P. Horodecki. Low dimensional bound entanglement with one-way distillable cryptographic key. *to appear in Vol 54, No. 6 IEEE Trans. Inf. Theor., Special Issue of the IEEE TIT on Information Theoretic Security, June 2008.* quant-ph/0506203 [HPHH05]

4. K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim. Locking entanglement with a single qubit. *Physical Review Letters*, 94:200501, 2005. qunat-ph/0404096.

5. K. Horodecki. On hiding entanglement using private states, 2008 [Hor08].

In comparison with [HHHO05a], there are two main differences in presentation:

1. The proof of Theorem 2 of [HHHO05a] (Theorem 3.2 of this thesis), which gives characterization of states that have key, is changed so that it does not use the notion of twisting. (Chapter 3)

2. We provide a more direct proof of the fact that there are PPT-KD states (Theorem 10 of [HHHO05a], Theorem 5.7 of this thesis). The construction of the states relevant for showing this fact, given in [HHHO05a], is presented in Section 5.5. (Chapter 5)

In [HPHH05] explicit examples of bound entangled, key distillable states were showed. Some of the results has not been made public yet. The content of Chapter 6 presents some results, that will be extended in [Hor08]. Moreover, the Sections 3.6 and 4.4.2 and 5.5.4, as well as the Observation 5.15 appear originally in this thesis. As we indicated in text, some of the remarked facts will be argued more explicitly in [PHHH08] and [BHH$^+$08]. The first motto of this thesis is cited after D. Kahn [Kah96]. The second is the ending of my father's poem *Still life* [Hor03].

# Chapter 2

# Preliminaries

In this Chapter we introduce basic notions, definitions and facts. Some mathematical facts which are mostly independent of the formalism of quantum information theory, we have moved to Appendix. If it is not explicitly stated we refer to the book by Chuang and Nielsen [NC00]. Sometimes we also refer to particular papers (books), which treat the subject in more detail. In particular, some basics of entanglement theory, which we invoke here as well as the overview on the subject can be found in book by Bengtsson and Życzkowski [BZ06], the PhD thesis of Matthias Christandl [Chr06] and the review papers [PV06, HHHH07]. For the classical information theory we refer to the book by Cover and Thomas [CT91].

## 2.1 Quantum states

According to quantum mechanics, with any physical system one associates some Hilbert space $\mathcal{H}$. It is a vector space over the field of complex numbers $\mathcal{C}$, equipped with a scalar product and complete with a norm based on this scalar product.

In this thesis we deal only with finite dimensional Hilbert spaces. More specifically, we focus on one representative of a Hilbert space, the Cartesian product of the field of complex numbers:

$$\mathcal{H} = \underbrace{\mathcal{C} \times \ldots \times \mathcal{C}}_{d} = \mathcal{C}^d. \tag{2.1}$$

We will alter the notation $\mathcal{H}$ and $C^d$, using the latter to indicate the dimension of the Hilbert space. The quantum system with associated d-dimensional Hilbert space, is called a *qudit*. In special cases of $d = 2, 3, 4$ it is called a *qubit*, *qutrit* and *quforit* respectively.

Before we present the notions of pure and mixed quantum states, we first introduce the so called Dirac notation. The standard basis vectors of a Hilbert space

$v_0 = [1, 0, ...0]^T, v_1 = [0, 1, ...0]^T, ...v_n = [0, ..., 1]^T$ are written as $|0\rangle, |1\rangle, ...|d-1\rangle$ respectively. The symbol $|.\rangle$ is called 'ket' while $\langle .|$ is called 'bra', and denotes hermitian conjugation of 'ket': $\langle\psi| = (|\psi\rangle)^\dagger$. The set $\{|k\rangle\}_{i=0}^{d-1}$ (also denoted as $\{|k\rangle\}$) we will call the *standard basis*. The scalar product of two vectors $|\psi\rangle$ and $|\phi\rangle$ reads:

$$\langle\psi||\phi\rangle \equiv \langle\psi|\phi\rangle. \tag{2.2}$$

Any quantum state is represented by a so called density operator $\rho$ that acts on a Hilbert space $\mathcal{H}$. The density operator is a matrix of dimension $d \times d$ (in case $\mathcal{H} = \mathcal{C}^d$), with complex entries that is (i) *positive* (ii) of trace one. By positivity, we mean that a matrix is diagonalisable and has real, non-negative eigenvalues. If a matrix has all eigenvalues real and positive, we call it strictly positive. Unfortunately, this common agreement in quantum information theory is not in accordance with notation from linear algebra see e.g. [HJ85]. We will denote the properties of a state in the following way:

$$\rho \geq 0, \text{ (positive)} \tag{2.3}$$

$$\mathrm{Tr}\rho = 1 \text{ (of trace one)} \tag{2.4}$$

$\rho \in B(\mathcal{C}^d)$ is positive if and only if

$$\forall_{|\psi\rangle \in \mathcal{C}^d} \langle\psi|\rho|\psi\rangle \geq 0. \tag{2.5}$$

From the above definition of density operator, it follows that it is also hermitian i.e. $\rho^\dagger = (\rho^T)^* = \rho$ The set of all states acting on a Hilbert space $\mathcal{H}$ we will denote as $B(\mathcal{H})$.

We can define now an important notion, which is the *projector* onto a subspace $S \subseteq \mathcal{H}$ of a Hilbert space $\mathcal{H}$. If the orthonormal vectors $\{|s_i\rangle\}_{i=1}^k$ span the subspace $S$, the projector onto $S$ is defined as

$$P_S = \sum_{i=1}^{k} |s_i\rangle\langle s_i|. \tag{2.6}$$

Any projector $P_S$ fulfills the two properties: $P_S^2 = P_S$ and $P_S^\dagger = P_S$ which constitutes its alternative definition. When $k = 1$, $P_S$ projects onto a 1-dimensional subspace spanned by the vector $|s_1\rangle$, and we say that $P_S$ projects onto a vector $|s_1\rangle$. In this case we can denote it also as $P_{|s_1\rangle}$.

When a quantum state $\rho$ has only one positive eigenvalue (equal to one), it is called a *pure state*. In this case, $\rho$ is equal to the projector onto some vector $|\psi\rangle$. In literature, vector and projector onto vector are in some cases used interchangeably, which we also would not avoid here. In particular we will say sometimes that $|\psi\rangle$ is

a state (mostly in cases when $|\psi\rangle$ has large description), burying in mind that we consider a projector[1].

A linear combination of vectors is called a *superposition*. In particular a vector $\psi = [a_0, ..., a_{d-1}]^T$ can be written in Dirac notation as:

$$|\psi\rangle = \sum_{i=0}^{d-1} a_i |i\rangle. \tag{2.7}$$

The normalization condition implies that $\sum_i |a_i|^2 = 1$. The coefficients $a_i$ are called *amplitudes*. We note here, that according to Dirac notation $\langle\psi|$ denotes the following operator:

$$\langle\psi| = (|\psi\rangle)^\dagger = \sum_{i=0}^{d-1} a_i^* \langle i|, \tag{2.8}$$

where by $a_i^*$ we denote the complex conjugation of the amplitude $a_i$.

If the state $\rho$ is not pure, it is called a *mixed state*. This name reflects the fact, that it is a probabilistic mixture of the projectors onto the eigenvectors $|\psi_i\rangle\langle\psi_i|$, which represents some pure states:

$$\rho = \sum_{i=0}^{m-1} p_i |\psi_i\rangle\langle\psi_i|. \tag{2.9}$$

Note that any state can be diagonalized to the above form, with trivial distribution in case of pure state.

The state $\rho \in B(\mathcal{C}^m)$ is called a *maximally mixed state* if it is of the form:

$$\rho_m = \frac{1}{m}\mathrm{I}. \tag{2.10}$$

with $\mathrm{I} = \sum_i |i\rangle\langle i|$ being the identity matrix.

If $\rho = \sum_{i=1}^K q_i \sigma_i$, we say that it is realized by an ensemble $\{(q_i, \sigma_i)\}_{i=1}^K$. In case of $\sigma_i$ being all pure states, the ensemble is called *pure*. The probabilities $q_i$ form a *distribution of the ensemble* $\vec{q} = (q_1, \ldots, q_K)$. If the number of members in ensemble is not relevant, we will omit it, denoting ensemble just as $\{(q_i, \sigma_i)\}$. Let us note here, that the same mixed state $\rho$ can be realized by many different ensembles.

**Example 2.1** *(different ensembles) The state* $\rho = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ *can be written as well as* $\frac{1}{2}(|\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-|)$ *with* $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$.

[1] A reason for this abuse of notation follows from the fact that vector $|\psi\rangle$ represents pure state $|\psi\rangle\langle\psi|$ up to a complex coefficient of modulus 1. This coefficient can not be observed (see section 2.2).

## 2.2 Quantum operations

Any quantum operation is linear. It is described by a linear *superoperator* $\Lambda : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$, with $\dim\mathcal{H}_1 = d$ and $\dim\mathcal{H}_2 = d'$. It can be also described (not uniquely) by the set of $d' \times d$ matrices with complex entries $\{M_m\}_{m=1}^K$, called *operators*. The operators satisfy relation $\sum_{m=1}^K M_m^\dagger M_m = \mathrm{I}_d$ where $\mathrm{I}_d$ is $d \times d$ identity matrix. The operators $M_m$ are also called *Kraus operators*. The superoperator $\Lambda$ acts on a state $\rho$ as follows:

$$\Lambda(\rho) = \sum_{m=1}^{K} M_m \rho M_m^\dagger. \tag{2.11}$$

Introducing a normalizing factor $p_m := \mathrm{Tr}[M_m \rho M_m^\dagger]$ whenever it is nonzero, one can interpret the action of $\Lambda$ as changing state $\rho$ into state $\sigma_m$ :

$$\rho \longrightarrow \sigma_m := \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}[M_m \rho M_m^\dagger]}, \tag{2.12}$$

with probability $p_m$. Instead of the name "quantum operation" or the "superoperator" we say also a *map*.

### 2.2.1 Von Neumann measurements

In special case, when all Kraus operators $M_m$ of a quantum operation $\Lambda$ are projectors, the operation $\Lambda$ is called a *von Neumann measurement*. When in particular all the projectors are of rank 1, i.e. project onto vectors $M_m = |\psi_m\rangle\langle\psi_m|$, and $\{|\psi_m\rangle\}$ forms a basis, the operation is called a *complete von Neumann measurement*(and else *incomplete*). Usually, instead of saying that the complete von Neuamann measurement has been done, we say that the *measurement in basis* $\{|\psi_m\rangle\}$ has been performed.

**Example 2.2** *(measurement in standard basis of a pure state)*

*Let* $|\psi\rangle = \sum_{i=0}^{d-1} a_i|i\rangle$. *Let us measure* $|\psi\rangle\langle\psi|$ *in the standard basis* $\{|i\rangle\}$. *In this case the projectors* $P_k$ *are equal to* $|k\rangle\langle k|$, *and constitutes the complete von Neumann measurement. The state* $|\psi\rangle\langle\psi|$ *after this measurement will become a mixed state, equal to a mixture of states* $|i\rangle\langle i|$ *each with corresponding probability* $|a_i|^2$. *Indeed:*

$$\Lambda(P_{|\psi\rangle}) = \sum_{k=0}^{d-1} P_k P_{|\psi\rangle} P_k = \sum_{k=0}^{d-1} |k\rangle\langle k| \sum_{i,j=0}^{d-1} a_i a_j^* |i\rangle\langle j||k\rangle\langle k| =$$

$$\sum_{i,j,k=0}^{d-1} a_i a_j^* |k\rangle\langle k||i\rangle\langle j||k\rangle\langle k| = \sum_{i,j,k=0}^{d-1} a_i a_j^* \delta_{k,i}\delta_{j,k}|k\rangle\langle k| = \sum_{i=0}^{d-1} |a_i|^2 |i\rangle\langle i| \tag{2.13}$$

### 2.2.2 Reversible quantum operations - unitary operations

As we have already mentioned, quantum operation $\Lambda = \{M_m\}$ can be viewed as map which changes $\rho$ into $\rho_m$ with probability $p_m = \mathrm{Tr} M_m \rho M_m^\dagger$. An exceptional case is when there is only one Kraus operator $M'_m$. Then, by normalization requirement $p_{m'} = 1$. In this case, quantum operation is deterministic: it is just a rotation. Indeed, the unique Kraus operator satisfies $M_{m'}^\dagger M_{m'} = \mathrm{I}$ which (in finite dimension) is equivalent to *unitarity* of $M_{m'}$. That is, $M_{m'} \equiv U$ for some *unitary transformation* $U$. Such operation is *deterministic* and can be viewed as a change of the eigenbasis of the state $\rho$:

$$\rho \longrightarrow U \rho U^\dagger. \tag{2.14}$$

Unitary operation is *reversible*: the inverse operation is $U^\dagger$, that transforms back $U\rho U^\dagger$ into $\rho$.

**Example 2.3** *The Hadamard transformation*

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{2.15}$$

*is a unitary transformation operating on* $\mathcal{C}^2$.

**Example 2.4** *An important example of a unitary transformation is the so called swap operator (or just swap) denoted as* $V$*, that exchanges the states of two systems. It is defined on spaces* $\mathcal{H}_X$ *and* $\mathcal{H}_Y$ *of the same dimensionality* $d$ *as*

$$V_{XY} := \sum_{i=0,j=0}^{d-1,d-1} |i\rangle|j\rangle\langle j|\langle i|_{XY}. \tag{2.16}$$

The important class of the so called Pauli (unitary) operations is presented in Section 2.4, Eq. (2.50).

### 2.2.3 From quantum operations to POVMs

If we are not interested in the form of the output state but just in the probabilities of the outcomes, there is useful mathematical tool called *POVM*. As we have mentioned, the probability of the result $m$ after measurement $\Lambda$ described by the set of operators $\{M_m\}$, equals $\mathrm{Tr} M_m \rho M_m^\dagger$. By property of trace it is equal to $\mathrm{Tr} M_m^\dagger M_m \rho$. The $d \times d$ matrix $E_m := M_m^\dagger M_m$ define so called *POVM elements*. The set of such POVM elements constitutes a POVM associated with the operation $\Lambda$, which we denote as $M_\Lambda = \{E_m\}$. In fact, any set of positive operators which sum up to identity,

contributes to a POVM for certain quantum operation. If we perform an operation $\Lambda$ but are just interested with a POVM, we say that we have *performed* a POVM. With a POVM performed on a quantum state, $\rho$ there is an associated classical random variable $M$. Its probability distribution is defined by the probabilities of particular *outcomes* (labels) of this POVM: $P(M = m) = \mathrm{Tr}\rho E_m$.

## 2.3 Dealing with composite quantum systems

If the quantum system is composite i.e. has $n$ subsystems, the Hilbert space which is associated with it, is a *tensor product* of the Hilbert spaces associated with its subsystems:

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n. \tag{2.17}$$

In case of two subsystems, that are traditionally in hands of Alice and Bob respectively, we will usually write:

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B. \tag{2.18}$$

If the state of each subsystem is prepared as $|\psi_i\rangle\langle\psi_i|$ $(i = 0, 1)$, then the joined state of a system is given by a tensor product of the states of its subsystems

$$|\psi_1\rangle\langle\psi_1|_A \otimes |\psi_2\rangle\langle\psi_2|_B. \tag{2.19}$$

The letter subscripts reminds from which space is each vector. We will omit them if the states themselves are labeled by the corresponding letters $|\psi_A\rangle, |\psi_B\rangle$ or if the labels of subsystems are known from the context. The state with two (three) subsystems is called a bipartite (tripartite) state (and multipartite in general). Any multipartite mixed state is a mixture of pure multipartite states.

The tensor product of two matrices the $m \times n$ matrix $A$ and $p \times q$ matrix $B$ with the corresponding entries $a_{ij}$ and $b_{ij}$ is an $mp \times nq$ matrix:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{bmatrix}. \tag{2.20}$$

In case of the tensor product of $k$ the same matrices (vectors) we use shorten notation: $A^{\otimes k}$ and $|\psi\rangle^{\otimes k}$ respectively.

A tensor product of the Hilbert spaces is also a Hilbert space. A natural basis of the space $\mathcal{H}_{AB}$ is just the set of tensor product of basis from each space:

$$|g_{ij}\rangle := |e_i\rangle \otimes |f_j\rangle. \tag{2.21}$$

For brevity we often write either $|e_i\rangle|f_j\rangle$ or $|e_i f_j\rangle$, or just $|ij\rangle$ - the latter in case of the *standard product basis*.

The scalar product of the vectors of the space $\mathcal{H}_{AB}$ is defined by:

$$\langle\psi| \otimes \langle\phi||\theta\rangle \otimes |\delta\rangle := \langle\psi|\theta\rangle \cdot \langle\phi|\delta\rangle. \tag{2.22}$$

A vector $|\psi\rangle \in \mathcal{H}_{AB}$ can be written with a use of only $\min(dim\mathcal{H}_A, dim\mathcal{H}_B)$ vectors of the form $|e_i\rangle \otimes |f_i\rangle$, where $|e_i\rangle \in \mathcal{H}_A$ and $|f_i\rangle \in \mathcal{H}_B$:

$$|\psi\rangle = \sum_i \lambda_i |e_i\rangle|f_i\rangle. \tag{2.23}$$

The real, positive coefficients $\lambda_i$ are called the *Schmidt coefficients* of the state $|\psi\rangle\langle\psi|$, and the above form of $|\psi\rangle$ is called a *Schmidt decomposition* of a pure state $|\psi\rangle\langle\psi|$.

### 2.3.1 Formalizing the notion of a site

In this section we invoke in a formal way the notion of site, which is used informally in literature. By *site* we mean the collection of systems, on which one is allowed to perform any quantum operation. This notion reflects the intuition, that system corresponds to some 'tool', and the collection of 'tools' gives rise to a 'laboratory'. With the site there is naturally associated Hilbert space: a tensor product of Hilbert spaces of the systems of this site. The number of systems is not fixed a priori, and can vary according to operations that are performed on the systems of site.

In this thesis, we will have at most three sites. Traditionally, with each of them we associate a person, that can perform quantum operations. These are: Alice, Bob (the honest parties) and Eve (the eavesdropper). These three sites will be called $\mathcal{S}_\mathcal{A}$, $\mathcal{S}_\mathcal{B}$ and $\mathcal{S}_\mathcal{E}$ respectively. The systems that belong to site $\mathcal{S}_\mathcal{X}$ will be denoted by a modification of label $X$, e.g. $X'$, $X''$, $\hat{X}$, etc.

### 2.3.2 Operation of partial trace, and purification of a quantum system

We describe now the operation which acting on a state of a system, outputs the state of its subsystem. It is called a *partial trace*.

**Definition 2.1** *For a bipartite state $\rho_{AB} \in B(\mathcal{H}_{AB})$, the state $\rho_A \in B(\mathcal{H}_A)$ of its subsystem $A$ is given by:*

$$\rho_A \equiv \mathrm{Tr}_B(\rho_{AB}) = \sum_{k=0}^{dim(\mathcal{H}_B)-1} \mathrm{I}_A \otimes \langle k|_B \, \rho_{AB} \, \mathrm{I}_A \otimes |k\rangle_B, \tag{2.24}$$

*The operation* $\mathrm{Tr}_B$ *is called a partial trace over system* $B$*.*

A strict description of the above operation requires saying that after *tracing out* a subsystem $B$ of system $AB$ in state $\rho_{AB}$, we obtain subsystem A in state $\rho_A$. For brevity, we usually say more informally, that tracing out system $B$, we obtain subsystem of $\rho_{AB}$ in state $\rho_A$. Even more informally we say shortly that $\rho_A$ is a *subsystem of a state* $\rho_{AB}$. Perhaps more proper name should be "a substate", but neither this, nor other possible words are used in this case, in quantum information theory.

This definition extends to any *multipartite system* $\mathcal{H} = \mathcal{H}_A \otimes \ldots \otimes \mathcal{H}_Z$, so that by the $\mathrm{Tr}_X$ we denote the partial trace over system $X$ of a multipartite system $\mathcal{H}$, with subsystem $X$. In particular, the state of subsystem $B$ of system $AB$ in state $\rho_{AB}$ is given by the *partial trace over system* $A$, defined analogously to (2.1). Note, that partial trace *does not depend on the choice of basis* in which we trace out the system. That is, instead of the standard basis $\{|k\rangle\}$ on system $A$ in the definition of partial trace over system $A$, there can be any orthonormal basis i.e. the set $\{U|k\rangle\}$ for any unitary operation $U$.

### Extension and purification of a bipartite state

**Definition 2.2** *An extension of a quantum bipartite state* $\rho_{AB}$ *to system* $E$ *is any tripartite state* $\rho_{ABE}$ *such that* $\mathrm{Tr}_E \rho_{ABE} = \rho_{AB}$*. The state* $\rho_E = \mathrm{Tr}_{AB}\rho_{ABE}$ *is called extending state of* $\rho_{AB}$*. A system in extending state of* $\rho_{AB}$ *is called extending system of* $\rho_{AB}$*.*

*Any pure extension is called a purification of* $\rho_{AB}$*, and denoted as* $|\psi_\rho\rangle_{ABE}$*. The state* $\mathrm{Tr}_{AB}|\psi_\rho\rangle\langle\psi_\rho|_{ABE}$ *is called a purifying state of* $\rho_{AB}$*. A system in purifying state of* $\rho_{AB}$ *is called a purifying system of* $\rho_{AB}$*.*

If only $\dim E \geq rank(\rho_{AB})$, there exists a purification of $\rho_{AB}$ to system $E$. In particular, there is a *standard purification*, described in example below:

**Example 2.5** *The standard purification of a bipartite state* $\rho_{AB} \in B(\mathcal{C}^{\otimes d_1} \otimes \mathcal{C}^{\otimes d_2})$ *with an eigen decomposition* $\rho_{AB} = \sum_{i=0}^{m-1} p_i |\psi_i\rangle\langle\psi_i|$*, is a tripartite pure state* $|\psi\rangle_{ABE} \in \mathcal{C}^{\otimes d_1} \otimes \mathcal{C}^{\otimes d_2} \otimes \mathcal{C}^{\otimes m}$ *of the form*

$$|\psi\rangle_{ABE} = \sum_{i=0}^{m-1} \sqrt{p_i} |\psi_i\rangle_{AB} \otimes |i\rangle_E. \tag{2.25}$$

*The purifying system according to this purification is called a standard purifying system.*

A purification of quantum state is in a sense its best extension, as it is formalized in observation below. We first invoke the following lemma needed to prove the observation:

**Lemma 2.6** *(adapted from [NC00]) For any two purifications $|\psi\rangle_\rho^{XE}$ and $|\phi\rangle_\rho^{XE'}$ of the state $\rho \in B(\mathcal{H}_X)$, to systems $E$ and $E'$ respectively, there exists an isometry (in case* $\dim E \leq \dim E'$*) or partial isometry (in case* $\dim E > \dim E'$*) $U : E \to E'$ which satisfies:*

$$\mathrm{I}_X \otimes U|\psi_\rho\rangle_{XE} = |\phi_\rho\rangle_{XE'}. \tag{2.26}$$

We can state now desired observation:

**Observation 2.7** *Let $|\psi_\rho\rangle_{ABE}$ be the standard purification of a bipartite state $\rho_{AB}$ to system $E$, for any extension $\rho_{ABE'}$ of $\rho_{AB}$ to system $E'$, there is an operation $\Lambda_E$ such that $\mathrm{I} \otimes \Lambda_E|\psi_\rho\rangle\langle\psi_\rho|_{ABE} = \rho_{ABE'}$.*

**Proof.** Consider the following purification of $\rho_{ABE'}$ to system $E''$:

$$|\phi\rangle_{ABE'E''} = \sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle_{E''}. \tag{2.27}$$

The above state is also a purification of $\rho_{AB}$, to system E'E". Indeed: tracing out subsequently E' and E" we obtain back the $\rho_{AB}$. Now by Lemma 2.6, there exists an izometry $W$ that switches between the purifications:

$$\mathrm{I}_{AB} \otimes W_E|\psi_\rho\rangle_{ABE} = |\phi\rangle_{ABEE'}. \tag{2.28}$$

We can define $\Lambda_E$ as a composition of (i) implementing the isometry[2] $W$ to obtain $|\phi_\rho\rangle_{ABE'E''}$, (ii) tracing out the system $E''$, obtaining desired state $\rho_{ABE'}$ shared by Alice and Bob. ∎

The above observation has the following cryptographical meaning: sharing the purifying system of a bipartite state $\rho_{AB}$ that is held by the honest parties, eavesdropper has the most power that is possible according to axioms of quantum information theory, since he can perform an operation which transforms a purification $|\psi_\rho\rangle_{ABE}$ into some extension $\rho_{ABE'}$ of $\rho_{ABE}$. Such a cryptographic scenario will be referred to as *quantum worst case scenario*, (for short presentation of other scenarios see Section 2.9). Important conclusion about this scenario is that if we prove some property of $|\psi_\rho\rangle_{ABE}$ for *any* quantum operation of Eve, we can work with some fixed purification regardless of other extensions (with other purifications among them), without loosing generality of the proof.

### 2.3.3 Quantum operations as completely positive trace preserving (CPTP) maps and probabilistic quantum operations

Any quantum operation $\Lambda$ is *completely positive*. That is, if $\rho \geq 0$,

$$\Lambda \otimes \mathrm{I}_{\mathcal{H}_B}(\rho) \geq 0. \tag{2.29}$$

[2]It is easy to check, that isometry can be implemented via basic quantum operations.

Quantum operation $\Lambda$ preserves trace of the operators. That is $TrA = Tr\Lambda(A)$ for an operator $A$. For this reason, they are called trace preserving maps. If a superoperator is completely positive, but does not preserve trace (is not *trace preserving*), it can be performed (that is - physically implemented), but only with a probability given by its trace:

$$\rho \longrightarrow \Lambda_{CP}(\rho)/Tr(\Lambda_{CP}(\rho)). \tag{2.30}$$

We refer to such an operation as to *probabilistic quantum operation* or just a *completely positive map*, denoting it as CP. We refer also to the usual quantum operation as to CPTP which means the *completely positive, trace preserving map.*

### 2.3.4 Quantum measurements

Quantum measurements are special quantum operations. Apart from the 'quantum' result (a state) they give 'classical' result, often called a 'flag' that informs how quantum operation was realized i.e. which Kraus operator was applied to the state. With quantum measurements one can easily realize a POVM, if traces out the quantum result of measurement. Formally it is defined as follows:

**Definition 2.3** *Quantum measurement $Q$ is a quantum operation $Q : B(\mathcal{H}_X) \rightarrow B(\mathcal{H}_Y \otimes \mathcal{H}_Z)$, such, that for any state $\rho \in B(\mathcal{H}_X)$,*

$$Q(\rho) = \sum_{i=0}^{d-1} A_i \rho A_i^\dagger \otimes |i\rangle\langle i|_Z, \tag{2.31}$$

*where $\sum_{i=0}^{d-1} A_i^\dagger A_i = \mathrm{I}_X$, and $d = \dim\mathcal{H}_Z$. The states $|i\rangle\langle i|$ are called classical results of the quantum measurement. For $p_i = Tr[A_i \rho A_i^\dagger] > 0$, the states $\frac{1}{p_i} A_i \rho A_i^\dagger$ are called quantum results of the measurement.*

Intuitively, by a *local quantum measurement* we will mean quantum measurement performed on a subsystem of a bipartite state.

**Remark 2.8** *It is important, that the name 'quantum measurement' should not be confused with a similar name used in case of von Neumann measurements which are quantum operations with Kraus being just projectors, acting on a state as $\rho \rightarrow \sum_i P_i \rho P_i$, with $\sum_i P_i = \mathrm{I}$.*

### 2.3.5 Representations of a pure bipartite states and its subsystems

We give here useful representation of a pure bipartite state [Rai97]. Any pure bipartite state $\mathcal{H}_A \otimes \mathcal{H}_B \ni |\psi\rangle_{AB} = \sum_{ij} a_{ij} |i\rangle_A |j\rangle_B$ can be represented in the following

way:

$$|\psi\rangle = \sum_{i=0}^{d_B-1} [X|i\rangle]_A |i\rangle_B, \tag{2.32}$$

where $X$ is a matrix fully representing the state $|\psi\rangle$. It is expressed in the form $X = \sum_{l,k=0}^{d_B-1,d_A-1} a_{kl}|k\rangle\langle l|$. Alternatively, the state $|\psi\rangle$ can be written also with help of a transposition of the matrix $X$:

$$|\psi\rangle = \sum_{i=0}^{d_A-1} |i\rangle_A [X^T|i\rangle]_B. \tag{2.33}$$

As an easy application of this representation we note, that the subsystems of $|\psi\rangle$ are of the form $\rho_A = XX^\dagger$ and $\rho_B = X^T(X^T)^\dagger$.

### 2.3.6 Basic quantum operations

In previous section we have introduced a formal description of quantum operations i.e. using the Kraus operators. There is however a more operational approach to this class of transformations, which shows, that they are built from conceptually easy basic ones.

**Theorem 2.9** *Any quantum operation $\Lambda$ on a quantum state $\rho$ of some system $S$ can be performed using three elementary operations:*

1. *Adding an ancillary system $A$ in a state $\omega$:*

$$\rho \to \rho \otimes \omega. \tag{2.34}$$

2. *Performing some unitary transformation $U$ on both ancillary system $A$ and system $S$:*

$$\rho \otimes \omega \to U\rho \otimes \omega U^\dagger. \tag{2.35}$$

3. *Tracing out some subsystem of the system $SA$.*

We will refer to this implementation of an operation $\Lambda$ as to the *implementation via basic quantum operations* of a quantum operation $\Lambda$.

**Observation 2.10** *The ancillary state $\omega$ for implementing any quantum operation via basic quantum operations, can be taken without loose of generality to be a pure state $|0\rangle \in \mathcal{H}$.*

**Proof.** Let $\omega = \sum_{i=1}^{m} p_i|\psi_i\rangle\langle\psi_i|$. To obtain $\omega$ from a pure state, one takes $|0\rangle\langle 0|_{AB} \in \mathcal{C}^m \otimes \mathcal{C}^m$ and rotate it by appropriate unitary transformation into state $|\phi\rangle =$

$\sum_{i=1}^{m} p_i|i\rangle_A|i\rangle_B$. One then traces out the system $A$, and transforms the system $B$ which is now in state $\sum_i p_i|i\rangle\langle i|$ into $\omega$ by appropriate change of its eigenbasis, achieving the task.

Via basic quantum operations, one can make also embedding of a system into a larger one, and a *partial isometry* (see Appendix A.1).

### 2.3.7 Coherent quantum operations

Using basic quantum operations one can perform every quantum operation via operations which preserve von Neumann entropy of the input system. Such implementation of the quantum operation is called *coherent*. More specifically, for an operation $\Lambda$ there is an operation $\Lambda^{coh}$, such that on input state $\rho_X$, $\Lambda^{coh}$ outputs an extension $\sigma_{XR}$ of $\rho_X$ to system $R$, such that $S(\sigma_{XR}) = S(\rho_X)$, where S is the von Neumann entropy (see Section 2.7.1). Operation $\Lambda^{coh}$ is called *coherent*. This is easily achieved via basic quantum operations: the coherent quantum operation simply does not trace out a system which should be traced out according to implementation via basic quantum operations.

In this section we introduce in a formal way a widely used notion of coherent quantum operations. In particular, we provide definition of coherent quantum operations, and their composition. We also introduce technical term of a *trash bin*. It is then used to collect system $R$ that would have been traced out when some quantum operation were implemented via basic quantum operations. Another technical term is operation on labels of systems called *putting aside*. It means that some system became a subsystem of trash bin. Whenever we would like to treat some system $R$ as subsystem of trash bin, we say that this system has been *put aside*.

The notion of coherent quantum operation and putting aside, will be essential for definition of coherent local operations and public communication (CLOPC) operations, which we provide in Chapter 4. These operations, yet without explicit formal treatment, has been first used in [DW05, DW04].

#### Reversible part of quantum operation

In what follows, for clear presentation we assume without loose of generality, that any implementation of any quantum operation via basic quantum operations, needs the use of the partial trace operation[3].

We begin with definition of *reversible part* of a quantum operation:

[3]If the operation does not need trace out we can force it artificially to use it by first adding ancilla system in a pure state $|0\rangle$, that will be subsequently traced.

**Definition 2.4** *Let $\rho_X \in B(\mathcal{H}_X)$. Consider quantum operation $\Lambda : B(\mathcal{H}_X) \to B(\mathcal{H}_{X'})$ implemented via basic quantum operations acting as follows:*

$$\Lambda(\rho_X) = \mathrm{Tr}_R(U\rho_X \otimes |0\rangle\langle 0|_S U^\dagger)_{X'R}, \tag{2.36}$$

*for some unitary transformation $U$, and system $R$ with $\dim\mathcal{H}_{X'R} = \dim\mathcal{H}_{XS}$. The reversible part of $\Lambda$ is the operation $\Lambda^{rp} : B(\mathcal{H}_X) \to B(\mathcal{H}_{X'R})$ acting as*

$$\Lambda^{rp}(\rho_X) = (U\rho \otimes |0\rangle\langle 0|_S U^\dagger)_{X'R}. \tag{2.37}$$

*We call $X'$ the main system and $R$ the trash system.*

### Convention of trash bins and putting aside

For consistency, and compact notation, we introduce now the following convention:

1. With any site $\mathcal{S}_\mathcal{A}$, we associate a system $R_\mathcal{A}$ called *trash bin*. Any operation acting on system $A$ of this site, will be understood to take input on $AR_\mathcal{A}$, and act on $R_\mathcal{A}$ as identity. When the system $R_\mathcal{A}$ has associated 1-dimensional Hilbert space (the empty trash bin), and whenever it does not lead to ambiguity, we will omit $R_\mathcal{A}$ in notation.

2. With an operation $\Lambda$ transforming some input state $\rho_{AR_\mathcal{A}}$ on system $AR_\mathcal{A}$, into output $\rho^{out}_{A'R_\mathcal{A}R'}$ on system $A'R_\mathcal{A}R'$, we associate an operation on labels of systems called *putting* system $R'$ *aside*, denoted as $PA_{R'}$, which appends $R'$ to the list of subsystems of $R_\mathcal{A}$:

   $$R_\mathcal{A} = XY \to R_\mathcal{A} = XYR', \tag{2.38}$$

   for some subsystems $XY$ of $R_\mathcal{A}$ (if $R_\mathcal{A}$ has initially no subsystems, the operation $PA_{R'}$ makes just substitution: $R_\mathcal{A} := R'$).

### Definition, properties and examples of coherent quantum operations

**Definition 2.5** *For any quantum operation $\Lambda : B(\mathcal{H}_X) \to B(\mathcal{H}_{X'})$, and its reversible part $\Lambda^{rp} : B(\mathcal{H}_X) \to B(\mathcal{H}_{X'R})$, a coherent (version of) $\Lambda$ is a quantum operation of the form:*

$$\Lambda^{coh} = PA_R(\Lambda^{rp}). \tag{2.39}$$

Owing to the above definition, one can see, that instead of operation of partial trace, we use the 'operation' of putting aside, which means that the system is labeled, that it should have been traced out: becomes a subsystem of trash bin.

The 'operation' of putting aside is specially designed for coherent operations, as they gives output with two subsystems. We will use it for other operations (e.g. LOCC) only when we want the latter in a sense to 'mimic' some coherent operations.

We need now the observation, which follows directly from definition of partial trace and extension of a quantum state (see Section 2.3.2):

**Observation 2.11** *For a state $\rho \in B(\mathcal{H}_X)$, its any extension $\rho_{XY}$ on $\mathcal{H}_X \otimes \mathcal{H}_Y$, and any quantum operation $\Lambda$ there holds,*

$$\mathrm{Tr}_Y(\Lambda \otimes \mathrm{I}_Y(\rho_{XY})) = \Lambda(\rho). \tag{2.40}$$

Basing on this we provide important properties of the composition of coherent operations:

**Observation 2.12** *For any two operations $\Lambda_1 : B(\mathcal{H}_X) \to B(\mathcal{H}_{X'R_1})$ and $\Lambda_2 : B(\mathcal{H}_{X'}) \to B(\mathcal{H}_{X''R_2})$ the composition $\Lambda_2^{coh} \circ \Lambda_1^{coh} : B(\mathcal{H}_{XR_\mathcal{A}}) \to B(\mathcal{H}_{X''R_\mathcal{A}})$, satisfies for any state $\rho_{XR_\mathcal{A}}$*

$$\mathrm{Tr}_{R_\mathcal{A}} \Lambda_2^{coh} \otimes \Lambda_1^{coh}(\rho_{XR_\mathcal{A}}) = \Lambda_2 \otimes \Lambda_1(\rho_X). \tag{2.41}$$

*Moreover, if $\rho_{XR_\mathcal{A}}$ is pure, then the state $\Lambda_2^{coh} \otimes \Lambda_1^{coh}(\rho_{XR_\mathcal{A}})$ is also a pure state.*

**Proof.** This observation follows from Def. 2.5 of coherent version of $\Lambda$, Observations 2.11 and 2.10, and the fact that partial trace over two subsystems is a composition of partial traces over each subsystem separately. ∎

It is important to note, that given $\Lambda$, its coherent operation is not uniquely defined. Indeed, there are many ways (depending on choice of unitary transformation and dimension of ancilla system) to obtain its reversible part $\Lambda^{rp}$. Some properties of $\Lambda^{coh}$, as shown above are still unique. Yet, in some cases, we will explicitly specify the ancilla system, unitary transformation and the system which is put aside, since otherwise the resulting operation might not have desired properties. We describe this issue below:

**Example 2.13** *(Different sites) Consider two systems $X$ and $Y$, belonging to different sites $\mathcal{S}_\mathcal{X}$ and $\mathcal{S}_\mathcal{Y}$ respectively. One would like the coherent version of operation of the form $\Lambda_X \otimes \mathrm{I}_Y$ act as identity operation on system $Y$ of site $\mathcal{S}_\mathcal{Y}$, so that we will specify $(\Lambda_X \otimes \mathrm{I}_Y)^{coh}$ to be performed via adding $|0\rangle\langle 0|_S$ on site $\mathcal{S}_\mathcal{X}$, performing $U_{XS} \otimes \mathrm{I}_Y$ on systems $XSY$ and putting aside a subsystem of $XS$, where adding $|0\rangle\langle 0|_S$, performing $U_{XS}$, and tracing out the subsystem, implements $\Lambda_X$ via basic quantum operations.*

## 2.4 Entanglement of pure and mixed bipartite states

In this section we provide the definition of quantum entanglement and the notion of separability. We also discuss the most important classes of bipartite states, such as maximally entangled states, separable states and PPT states.

We define now bipartite quantum states contain interesting type of quantum correlations called entanglement. We invoke here the definition of Werner [Wer89]:

**Definition 2.6** *A bipartite state $\rho_{AB}$ is entangled if it can not be written as a convex combination of tensor product of states: $\sum_{i=1}^{K} p_i \sigma_A^{(i)} \otimes \sigma_B^{(i)}$, where $\vec{p} = (p_1, \ldots, p_K)$ is a probability distribution and for each $i$, $\sigma_A^{(i)}$ ($\sigma_B^i$) are some (in general mixed) states on A (B) subsystem.*

In other words, the state is entangled if it is not a probabilistic mixture of *product states*, i.e. states of the form $\sigma_A \otimes \sigma_B$.

The best known example of an entangled pure state is a state of two qubits called singlet state $|\psi^-\rangle\langle\psi^-|$:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.42}$$

This state is the base for many quantum phenomena such as quantum teleportation [BBP$^+$96] (see example 2.18) and quantum dense coding [BW92].

There is a class of pure bipartite states called *maximally entangled states*. In case of two qubit states, this class is an orbit of pure states generated from the singlet state via local unitary operation:

$$MS^{(2)} := \{|\psi\rangle\langle\psi| \,|\, |\psi\rangle = U \otimes \mathrm{I}|\psi^-\rangle\}, \tag{2.43}$$

where $U$ is a unitary operation. We will use more often (and sometimes call it the singlet state) the state of a form:

$$|\Psi_+^{(d)}\rangle = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |i\rangle_A \otimes |i\rangle_B. \tag{2.44}$$

We will sometimes write also $|\Psi_+\rangle$ if the dimension $d$ is either irrelevant, or known from the context. In general case of two qudit states, the set of maximally entangled states is the following:

$$MS^{(d)} := \{|\psi\rangle\langle\psi| \,|\, |\psi\rangle = U \otimes \mathrm{I}|\Psi_+^{(d)}\rangle\}. \tag{2.45}$$

In consequence, the state $|\Psi_{\mathcal{B}}^{(d)}\rangle\langle\Psi_{\mathcal{B}}^{(d)}|$ with $|\Psi_{\mathcal{B}}^{(d)}\rangle = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |e_i f_i\rangle$ (where $\mathcal{B} = \{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1}$ is an arbitrary product basis) is also an example of maximally entan-

gled state[4]. The maximally entangled states are called in short the *EPR states* after names of Einstein, Podolsky and Rosen.

There is also a distinguished set of four maximally entangled states, that forms an orthonormal basis of $\mathcal{C}^2 \otimes \mathcal{C}^2$ (a basis of a two-qubit system). It is called the Bell basis, and consists of a singlet and three other states:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{2.46}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{2.47}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{2.48}$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.49}$$

The elements of Bell basis are called also the *Bell states*. We denote them as above in accordance with literature, yet in an apparent contradiction with our notation of $|\Psi_+^{(d)}\rangle$. This is because the latter is the $d$-dimensional counterpart of $|\phi^+\rangle$ rather than $|\psi^+\rangle$. This is however also a common notation in literature. We note, that all the Bell states are maximally entangled. This is because they can be generated from the singlet state by the group of so called *Pauli operations* - the unitary transformations acting on a one-qubit system. We present them below:

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$\sigma_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ -i\sigma_3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{2.50}$$

Let us enumerate the Bell states as follows:

$$|\psi_0\rangle = |\psi^-\rangle,\ |\psi_1\rangle = |\phi^-\rangle,\ |\psi_2\rangle = |\psi^+\rangle,\ |\psi_3\rangle = |\phi^+\rangle. \tag{2.51}$$

The singlet state rotated by $\sigma_k$ on Alice's qubit becomes (up to an irrelevant complex phase factor in case $k = 3$) the corresponding $|\psi_k\rangle$ Bell state:

$$|\psi_k\rangle = (\sigma_k \otimes \mathrm{I}_B)|\psi^-\rangle_{AB}. \tag{2.52}$$

[4]For d=2, the set given in eq. 2.45 equals that of given in eq. 2.43, since there is a unitary transformation $U$, such that $U \otimes \mathrm{I}|\psi^-\rangle = |\Psi_+^{(2)}\rangle$

### 2.4.1 Separable states

In the light of Definition (2.6), if the state is *not* entangled, it is called *separable* [Wer89]. It is then a convex combination of product states:

$$\rho_{sep} = \sum_i p_i \sigma_A^{(i)} \otimes \sigma_B^{(i)}, \tag{2.53}$$

i.e. the coefficients $p_i$ form a probability distribution. The set of all separable states in $B(\mathcal{H}_{AB})$ for some fixed $\mathcal{H}_{AB}$ is denoted[5] as SEP. Separable states are mixtures of product states (those which are tensor product of two states $\sigma_A \otimes \sigma_B$). The set of separable states is convex and compact in any finite dimensional Hilbert space [BZ06].

We remark here the following convention. If a state has more subsystems, and we say that it is separable (or product), we have to indicate which tensor product is under consideration. We say then, that it is *separable (product) in* some *cut*. To give example, the state $\rho_{ABA'B'} = \sigma_{AA'} \otimes \sigma_{BB'}$ is product in $AA' : BB'$ cut. The set of states on systems $ABA'B'$, separable in $AA' : BB'$ cut where $\dim A = \dim B = d$ and $\dim A' = \dim B' = d'$ we denote as $SEP^{(d,d')}$. Consequently, $SEP^{(d)}$ denotes the set of separable states on $AB$ with $\dim A = \dim B = d$.

We invoke here the important property of separable states [ABH$^+$01], which needs notion of classes SEP and LOCC operations, as well as the probabilistic SEP and probabilistic LOCC operations, that can be found in Section 2.6.

**Theorem 2.14** *(see [ABH$^+$01]) The set of separable states is closed under (probabilistic) LOCC operations.*

**Proof.** It follows from the fact, that (probabilistic) LOCC operations are in fact (probabilistic) separable operations (see Section 2.6), and that separable operations preserves separability of the state, that follows easily from Eq. (2.53) and Def. of separable operations 2.13.

### 2.4.2 The operation of partial transposition and PPT states

Determining if a given state is separable or entangled is in general a difficult task. There are however some criteria which work for certain classes of states. The first such criterion is due to Peres [Per96], which we invoke below. To this end we need an important notion of *partial transposition*

[5] The same name is used for the so called *separable operations* (see the next section), which should not be mistaken.

**Definition 2.7** *The partial transposition of a bipartite state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ with respect to system $B$, is given by:*

$$\rho_{AB}^{\Gamma} := (\mathrm{I}_A \otimes T_B)\rho_{AB}, \tag{2.54}$$

*where*[6] *$T_B$ denotes the transposition of matrix from $B(\mathcal{H}_B)$.*

The Peres criterion reads:

**Theorem 2.15** *Any bipartite state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ which is separable, has positive partial transposition, that is*

$$\rho_{AB}^{\Gamma} = (\mathrm{I}_A \otimes T_B)\rho_{AB} \geq 0, \tag{2.55}$$

*that is $\rho_{AB}^{\Gamma}$ has non-negative eigenvalues.*

The operation of partial transposition[7] acts on matrix elements of a bipartite state $\rho_{AB}$ as follows:

$$\rho_{AB} = \sum_{i,j,k,l} a_{ijkl}|i\rangle|j\rangle\langle k|\langle l| \rightarrow \rho_{AB}^{\Gamma} = \sum_{i,j,k,l} a_{ijkl}|i\rangle|l\rangle\langle k|\langle j|. \tag{2.56}$$

Some useful properties of this operation we have collected in Section 2.5. We will extend now the definition of the partial transposition of one bipartite system, to a tensor product of bipartite systems.

**Definition 2.8** *For a tensor product of Hilbert spaces $\mathcal{H} = \mathcal{H}_{A_1B_1} \otimes \ldots \otimes \mathcal{H}_{A_nB_n}$ and any state $\rho_{A_1B_1\ldots A_nB_n} \in B(\mathcal{H})$, by the partial transposition of this state along $A_1 \ldots A_n : B_1 \ldots B_n$ cut we mean*

$$\rho_{A_1B_1\ldots A_nB_n}^{T_{B_1\ldots B_n}} = [(\mathrm{I}_{A_1} \otimes T_{B_1}) \otimes \ldots \otimes (\mathrm{I}_{A_n} \otimes T_{B_n})](\rho_{A_1B_1\ldots A_nB_n}), \tag{2.57}$$

*where $T_X$ denotes the transposition on a matrix of state of system $X$.*

For brevity, the partial transposition along some cut we will denote also as $\Gamma$. In what follows we will deal usually with systems consisting of two bipartite systems, and associated spaces $\mathcal{H}_{AB}$ and $\mathcal{H}_{A'B'}$. In this case, for $\rho_{ABA'B'} \in B(\mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'})$ the operator $\rho_{ABA'B'}^{\Gamma}$ denotes the state $\rho_{ABA'B'}$ partially transposed along the $AA' : BB'$ cut. This useful notation may lead to ambiguity which needs a context-dependent interpretation. Below, we give example of a mixed notation that will occur.

[6] We denote the partial transposition as $\Gamma$ following Rains [Rai98], as the symbol $\Gamma$ can be seen as a 'part' of a letter $T$.

[7] One can define analogously partial transposition (p.t.) with respect to system A as $(T_A \otimes \mathrm{I}_A)[\rho_{AB}]$. All facts which are true for $\Gamma$, that will be presented in this thesis, holds also for p.t. with respect to system A. We then use only $\Gamma$ without loosing generality.

**Example 2.16** *Consider $\rho_{ABA'B'} \in B(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^d \otimes \mathcal{C}^d)$. In block matrix form, such a state has a bipartite structure of blocks, so that it reads:*

$$\rho_{ABA'B'} = \begin{bmatrix} A_{0000} & A_{0001} & A_{0010} & A_{0011} \\ A_{0100} & A_{0101} & A_{0110} & A_{0111} \\ A_{1000} & A_{1001} & A_{1010} & A_{1011} \\ A_{1100} & A_{1101} & A_{1110} & A_{1111} \end{bmatrix}. \tag{2.58}$$

*This state after partial transposition with respect to system $BB'$ reads:*

$$\rho^{\Gamma}_{ABA'B'} = \begin{bmatrix} A^{\Gamma}_{0000} & A^{\Gamma}_{0100} & A^{\Gamma}_{0010} & A^{\Gamma}_{0110} \\ A^{\Gamma}_{0001} & A^{\Gamma}_{0101} & A^{\Gamma}_{0011} & A^{\Gamma}_{0111} \\ A^{\Gamma}_{1000} & A^{\Gamma}_{1100} & A^{\Gamma}_{1010} & A^{\Gamma}_{1110} \\ A^{\Gamma}_{1001} & A^{\Gamma}_{1101} & A^{\Gamma}_{1011} & A^{\Gamma}_{1111} \end{bmatrix}. \tag{2.59}$$

*In the above equation, the partial transposition on left hand side is with respect to system $BB'$ and on the right hand side, only with respect to system $B'$, as the partial transposition with respect to system $B$, which is a one qubit system, resulted already in appropriate reordering of the block operators $A_{ijkl}$.*

The state with positive partial transposition $\rho^{\Gamma}_{AB}$ is called a PPT state. The set of all states with this property is denoted as PPT (it should not be confused with the same name that is used for certain set of operations - see the next section). It is easy to see, that this set is convex. What is more important, this set is closed under tensor product:

$$\rho^{\Gamma}_{AB} \geq 0 \,\&\, \sigma^{\Gamma}_{A'B'} \geq 0 \Rightarrow (\rho_{AB} \otimes \sigma_{A'B'})^{\Gamma} \geq 0. \tag{2.60}$$

The Peres criterion means that the set of separable states $SEP$ is a subset of the set of $PPT$ states. Due to P. Horodecki [Hor97], it is known, that this inclusion is proper i.e. that there are entangled PPT states. Other examples of entangled (not separable) states that are PPT can be found e.g. in [BP00, BDM$^+$99, WW01] (see [BL07, Cla06] for a full list). The entangled PPT states belong to the class of *bound entangled* states, for their entanglement is quite different from that of pure states. The phenomenon of bound entangled states is in a sense central to this thesis, which we clarify in Section (2.8). This is because the PPT states posses another important property: they remain PPT under action of LOCC operations, which is stated in theorem below [ABH$^+$01], stated in a more general way that includes probabilistic LOCC operations:

**Theorem 2.17** *(see [ABH$^+$01]) The set of PPT states is closed under (probabilistic) LOCC operations.*

The states which are not PPT (e.g. maximally entangled states), are called NPT. The set of all such states is denoted as NPT. Till now, it is not known if there are NPT bound entangled states [PPHH07]. In particular, the bound entangled states which we provide in this thesis are also PPT.

## 2.5 Some properties of partial transposition of a matrix

In analogy to partial transposition of a state, one can take partial transposition of a linear operator acting on a bipartite Hilbert space $\mathcal{H}_{AB}$ [BZ06]. Such operator has matrix form $\sum_{ijkl} c_{ijkl}|ij\rangle\langle kl|$, and its partial transposed w.r.t to $B$ form reads: $\sum_{ijkl} c_{ijkl}|il\rangle\langle kj|$. In what follows the action of partial transposition on an operator, we will also denote as $\Gamma$. For any matrices $A$ and $B$ (assuming appropriate shapes if needed from the context), the partial transposition $\Gamma$, satisfies:

$$(A \otimes B)^\Gamma = A \otimes B^T \tag{2.61}$$

$$((A \otimes B)^{\otimes n})^\Gamma = ((A \otimes B)^\Gamma)^{\otimes n} \tag{2.62}$$

$$\mathrm{Tr}AB = \mathrm{Tr}A^\Gamma B^\Gamma \tag{2.63}$$

$$\mathrm{Tr}A^\Gamma B = \mathrm{Tr}AB^\Gamma \tag{2.64}$$

$$\mathrm{Tr}A^\Gamma = \mathrm{Tr}A \tag{2.65}$$

$$\Gamma \text{ preserves hermiticity} \tag{2.66}$$

$$\Gamma \text{ is an involution} \tag{2.67}$$

These properties can be easily checked to be satisfied. E.g. To see (2.66), we note that $(A^\Gamma)^\dagger = (A^\dagger)^\Gamma$ for $A = \sum_{ijkl=0}^{d-1} a_{ijkl}|ij\rangle\langle kl|$, which gives hermiticity of $A^\Gamma$ if $A$ is hermitian.

## 2.6 The paradigm of distant laboratories - the LOCC scenario, SEP and PPT operations

In this section we describe an important scheme of processing of quantum data called LOCC scenario. This scheme was introduced in [BBP$^+$96, BDSW96]. It involves two distant laboratories: one of - traditionally - Alice, and the other of Bob. Alice and Bob are given some quantum data (quantum states). Their task is to transform them to some other form, or extract some information. Usually in distant laboratories scenario Alice and Bob are given many copies of the same state $\rho$, so that the input state has form $\rho^{\otimes n}$ for some natural number $n$. The operations which they are allowed to perform are (L)ocal quantum (O)perations (each person in her/his lab) assisted by (C)lassical (C)ommunication (e.g. talking by the phone).

That is, they can perform some measurements locally and then communicate the results of these measurements, so that they can perform then conditioning.

The formal definition of the LOCC operations, that has been worked out in [DHR02] is quite difficult. In what follows we will use a simpler one[8] basing on the one given in [Chr06].

We first introduce the notion of 'locality' of a quantum operation. We use here the notion of *site* which is (in case of Alice) a collection of systems, that are in her possession. With the site we associate a tensor product of the Hilbert spaces associated with the systems. If it is needed, the site is denoted as $\mathcal{S}_{\mathcal{A}}$, $\mathcal{S}_{\mathcal{B}}$ and $\mathcal{S}_{\mathcal{E}}$ for Alice, Bob and Eve respectively. We define here the local operation on Alice's site, with definition of the same operation on Bob's site along similar lines:

**Definition 2.9** *For any quantum operation $\Lambda$, the local operation $\Lambda : B(\mathcal{H}_A) \to B(\mathcal{H}'_A)$ on Alice's site is given by:*

$$\Lambda_A = \Lambda \otimes \mathrm{I}_B : B(\mathcal{H}_A \otimes \mathcal{H}_B) \to B(\mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_B), \tag{2.68}$$

*for some pairs of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_{\tilde{A}}$ on Alice's and $\mathcal{H}_B$ on Bob's site respectively.*

Sometimes, instead of saying that Alice has performed a local $\Lambda$, we say, that she 'did $\Lambda$ locally'. By just 'local $\Lambda$' we mean local $\Lambda$ on Alice's or Bob's site (i.e. without specifying the party).

We also define the operation of classical communication from Alice to Bob, with the same operation from Bob to Alice following similar lines:

**Definition 2.10** *Let $\mathcal{H}_{in} = \mathcal{H}_a \otimes \mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_{out} = \mathcal{H}_a \otimes \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_b$, where $\mathcal{H}_{A,a}$ and $\mathcal{H}_{B,b}$ are some Hilbert spaces on Alice's and Bob's site respectively. The operation of classical communication from Alice to Bob is a quantum operation $\Lambda_A^{(c)} : B(\mathcal{H}_{in}) \to B(\mathcal{H}_{out})$, such that on any state $\rho_{aAB} \in B(\mathcal{H}_{in})$ it acts as follows:*

$$\Lambda_A^{(c)}(\rho_{aAB}) = \sum_{i=0}^{\dim\mathcal{H}_a - 1} P_i \rho_{aAB} P_i \otimes |i\rangle\langle i|_b \tag{2.69}$$

*where $P_i = P_a^{(i)} \otimes \mathrm{I}_A \otimes \mathrm{I}_B$ with $\{P_a^{(i)}\}_{i=0}^{dim\mathcal{H}_a - 1}$ being a von Neumann measurement on system a in standard basis.*

By *classical communication* we mean the operation of classical communication from Alice to Bob or vice versa.

With a help of the above definitions, we can define LOCC operations as follows:

[8] We acknowledge A. Szepietowski and M. Horodecki for inspiring discussion on this definition

**Definition 2.11** *The LOCC operation is a composition of a finite number of the following operations:*

1. *Local quantum operation,*
2. *Classical communication.*

*For a finite dimensional Hilbert spaces $\mathcal{H}_{in}$ and $\mathcal{H}_{out}$, the set of LOCC operations acting on states from $B(\mathcal{H}_{in})$ with the output in $B(\mathcal{H}_{out})$ is denoted as $LOCC_{\mathcal{H}_{in},\mathcal{H}_{out}}$.*

For brevity, in what follows we will often write $LOCC$ instead of $LOCC_{\mathcal{H}_{in},\mathcal{H}_{out}}$ if it does not lead to ambiguity.

Due to the above definition, the only actions which Alice and Bob are allowed to perform are local quantum operation or communicating some classical information which is an outcome of the von Neumann measurement.

We define now the so called *one-way LOCC* operations, which are - intuitively - those where only one party uses classical communication.

**Definition 2.12** *The one-way LOCC operation is a composition of a finite number of either*

1. *Local quantum operation,*
2. *Operation of classical communication from Alice to Bob,*

*or*

1. *Local quantum operation,*
2. *Operation of classical communication from Bob to Alice.*

*For a finite dimensional Hilbert spaces $\mathcal{H}_{in}$ and $\mathcal{H}_{out}$, the set of one-way LOCC operations acting on states from $B(\mathcal{H}_{in})$ with the output in $B(\mathcal{H}_{out})$ is denoted as $LOCC^{A\to B}_{\mathcal{H}_{in},\mathcal{H}_{out}}$ or $LOCC^{B\to A}_{\mathcal{H}_{in},\mathcal{H}_{out}}$ respectively.*

LOCC operations are quantum operations, hence preserve trace. A non-trace preserving LOCC operation is called *probabilistic LOCC operation.* In analogy to definition of LOCC operation, it is a composition of (i) $\Lambda\otimes \mathrm{I}$ where $\Lambda$ is a probabilistic quantum operation (see (2.3.3)) and (ii) a probabilistic classical communication operation, which is described as the usual classical communication operation, only with a weaker condition, that (see Def. 2.10) projectors $P_i$ do not need to some up to identity on system $a$.

### 2.6.1 Quantum teleportation

We now give an example of a one-way protocol, which is one of the basic protocols of quantum information theory. It aims at sending an unknown state $|\psi\rangle$ from one site (say of Alice) to the other site, using the singlet state, and two bits of classical communication. It is called *quantum teleportation* [BBC$^+$93].

**Example 2.18** *Alice would like to send an unknown state of a qubit* $|\psi\rangle_{\tilde{A}} = a|0\rangle + b|1\rangle$ *to Bob. They share a system in the singlet state* $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. *She can also communicate some bits via a telephone to Bob. To achieve this task Alice with cooperation of Bob performs the protocol of teleportation which we describe in points:*

1. *Alice performs a measurement on system* $A\tilde{A}$ *(of her subsystem of a singlet state, and the system of a qubit which state will be transfered) in the Bell basis, which is described by the set of projectors* $\{P_{|\psi_i\rangle^{A\tilde{A}}}\}_{i=0}^3$ *(recall the enumeration of the Bell states* $|\psi_i\rangle$ *given in eq. (2.51)). The resulting state is as follows:*

$$\begin{aligned}\rho_{A\tilde{A}B} = \frac{1}{4}[&P_{|\psi^-\rangle_{A\tilde{A}}} \otimes P_{(a|0\rangle_B + b|1\rangle_B)} \\ &+ P_{|\phi^-\rangle_{A\tilde{A}}} \otimes P_{(a|1\rangle_B + b|0\rangle_B)} \\ &+ P_{|\psi^+\rangle_{A\tilde{A}}} \otimes P_{(b|1\rangle_B - a|0\rangle_B)} \\ &+ P_{|\phi^+\rangle_{A\tilde{A}}} \otimes P_{(a|1\rangle_B - b|0\rangle_B)}].\end{aligned} \tag{2.70}$$

2. *Upon observing the* $|\psi_i\rangle$ *as an outcome of her measurement, Alice sends the label* $i$ *to Bob using two classical bits, that is performs the operation of classical communication as follows:*

$$\Lambda_A^{(c)}(\rho_{A\tilde{A}B}) = \sum_{i=0}^{3} \frac{1}{4} P_{|\psi_i\rangle_{A\tilde{A}}} \otimes P_{|\phi_i\rangle_B} \otimes |i\rangle\langle i|_b \tag{2.71}$$

3. *Having got the outcome* $i$ *of Alice's measurement, Bob performs on his subsystem of a singlet state the corresponding Pauli operation* $\sigma_i$, *of eq. (2.50). That is, acts on system* $bB$ *with a control unitary operation* $U_{bB} = \sum_{i=0}^3 |i\rangle\langle i|_b \otimes \sigma_i^B$. *After this operation, his qubit is in a state* $|\psi\rangle$, *which Alice wanted to transfer i.e. the teleportation is completed.*

*To see this, we observe, that the initial total state of Alice and Bob's systems*

$$|\psi_{\tilde{A}AB}\rangle = |\psi\rangle_{\tilde{A}} \otimes |\psi^-\rangle_{AB}, \tag{2.72}$$

*after changing the order of subsystems to* $A\tilde{A}B$ *can be rewritten as:*

$$\begin{aligned}|\psi_{A\tilde{A}B}\rangle &= \frac{1}{2}[|\psi^-\rangle_{A\tilde{A}} \otimes (a|0\rangle_B + b|1\rangle_B) \\ &\quad +|\phi^-\rangle_{A\tilde{A}} \otimes (a|1\rangle_B + b|0\rangle_B) \\ &\quad +|\psi^+\rangle_{A\tilde{A}} \otimes (b|1\rangle_B - a|0\rangle_B) \\ &\quad +|\phi^+\rangle_{A\tilde{A}} \otimes (a|1\rangle_B - b|0\rangle_B)]. \end{aligned} \tag{2.73}$$

*It is then easy to see, that after the Bell measurement (measurement in Bell basis), Alice will obtain with probability* $(\frac{1}{2})^2 = \frac{1}{4}$ *one of the four Bell states* $|\psi_i\rangle$*, and Bob will have simultaneously a qubit in state* $|\phi_i\rangle$ *which needs just the Pauli rotation* $\sigma_i$*, to be the initial state of a qubit* $|\psi\rangle = a|0\rangle + b|1\rangle$*. The protocol of teleportation is a one way LOCC, since there was only communication from Alice to Bob.*

In general, the LOCC operations are not easy to deal with. There is however another class of operations, broader then LOCC, which is often used in formal investigation to yield certain estimations about the LOCC class. This is a class of the so called *separable operations.*

**Definition 2.13** *Let* $\mathcal{H}_{in} = \mathcal{H}_A \otimes \mathcal{H}_B$ *and* $\mathcal{H}_{out} = \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}}$ *for some Hilbert spaces* $\mathcal{H}_{A,\tilde{A}}$ *and* $\mathcal{H}_{B,\tilde{B}}$ *on Alice's and Bob's site respectively. Separable operation* $\Lambda^{sep} : B(\mathcal{H}_{in}) \to B(\mathcal{H}_{out})$ *is a quantum operation which on any bipartite state* $\rho_{AB} \in B(\mathcal{H}_{in})$ *act as follows:*

$$\Lambda^{sep}_{AB}(\varrho) = \sum_{i=0}^{s} A_i \otimes B_i \varrho_{AB} A_i^\dagger \otimes B_i^\dagger, \tag{2.74}$$

*where* $\sum_{i=0}^{s} A_i^\dagger A_i \otimes B_i^\dagger B_i = \mathrm{I}_A \otimes \mathrm{I}_B$ *with* $s$ *being a natural number [VP98, Rai97]. For a fixed* $\mathcal{H}_{in}$ *and* $\mathcal{H}_{out}$*, the set of separable operations is denoted as* $SEP_{\mathcal{H}_{in},\mathcal{H}_{out}}$*.*

*In general case when* $\sum_{i=0}^{s} A_i^\dagger A_i \otimes B_i^\dagger B_i \leq \mathrm{I}_A \otimes \mathrm{I}_B$*, the operation* $\Lambda^{sep}$ *is called a probabilistic separable operation. The set of probabilistic separable operations we denote as* $Prob(SEP)$*.*

It is known, that any LOCC operation is also a separable operation, but not vice versa [VP98, Rai97, BDF$^+$99]. That is, we have the following formal statement:

$$LOCC_{\mathcal{H}_{in},\mathcal{H}_{out}} \subset SEP_{\mathcal{H}_{in},\mathcal{H}_{out}} \tag{2.75}$$

where $\mathcal{H}_{in}$ and $\mathcal{H}_{out}$ are any finite dimensional Hilbert spaces. We will write $SEP$ instead of $SEP_{\mathcal{H}_{in},\mathcal{H}_{out}}$ if it does not lead to ambiguity.

There is also another class of operations which is broader then SEP, called *PPT operations* [Rai99, Rai00].

**Definition 2.14** *A quantum operation $\Lambda : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is a PPT operation if conjugated by partial transposition remains completely positive i.e. the map $(\Lambda[(\cdot)^\Gamma])^\Gamma : B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is quantum operation. For a fixed $\mathcal{H}_1$ and $\mathcal{H}_2$, the set of PPT operations is denoted as $PPT_{\mathcal{H}_1,\mathcal{H}_2}$.*

We will usually omit the input and output Hilbert space, denoting $PPT_{\mathcal{H}_1,\mathcal{H}_2}$ as $PPT$. It is known, that there holds $SEP \subset PPT$ and the inclusion is proper, which means:

$$SEP_{\mathcal{H}_1,\mathcal{H}_2} \subset PPT_{\mathcal{H}_1,\mathcal{H}_2}. \tag{2.76}$$

## 2.7 Quantum distance measures

A basic distance measure which we will use is the *trace norm distance*

$$D(\rho,\sigma) = \frac{1}{2}\mathrm{Tr}|\rho-\sigma|, \tag{2.77}$$

where the modulus of the normal operator $A$ equals the $|A| = \sqrt{A^\dagger A}$. This distance is based on the *trace norm* $||A|| := Tr|A|$, as it equals $\frac{1}{2}||\rho-\sigma||$ (See also Appendix A.1.1). Since the two quantities: $D(\rho,\sigma)$ and $||\rho-\sigma||$ are related only by a constant factor independent of dimension, in Chapters 3-6, with a little abuse of language, we will refer to $||\rho-\sigma||$ as to the trace norm distance.

The most important property of the trace distance is that it is not increasing under quantum operations.

**Lemma 2.19** *For any quantum operation $\Lambda$, and any two quantum states $\rho$ and $\sigma$ there holds*

$$D(\rho,\sigma) \geq D(\Lambda(\rho),\Lambda(\sigma)). \tag{2.78}$$

Another measure of how close are the states is the so called *fidelity*, which is dual function to the distance measures.

For any $\rho$ and $\sigma$ from the set $B(\mathcal{H})$ for some finite-dimensional Hilbert space $\mathcal{H}$, the fidelity between two states is defined as:

$$F(\rho,\sigma) := \mathrm{Tr}\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}. \tag{2.79}$$

When two states are the same, fidelity equals 1, and zero when they are orthogonal. If one of the states is pure, the fidelity equals:

$$F(|\psi\rangle,\sigma) = \sqrt{\langle\psi|\rho|\psi\rangle} = \sqrt{\mathrm{Tr}\rho|\psi\rangle\langle\psi|}. \tag{2.80}$$

The fidelity and trace norm distance are related by the following inequalities [Fv97]:

**Lemma 2.20** *For any finite dimensional Hilbert space $\mathcal{H}$ and any two states $\rho, \sigma \in B(\mathcal{H})$ there holds:*

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}. \tag{2.81}$$

The above relation allows to use the fidelity and trace norm distance interchangeably. This proves useful, because the fidelity can be expressed also in an alternative way due to Ulman's theorem [Uhl76] (see in this context [Joz94, NC00]):

**Theorem 2.21** *(adapted from [NC00])*

*For any finite-dimensional Hilbert space $\mathcal{H}_Q$ and any two states $\rho, \sigma \in B(\mathcal{H}_Q)$ there holds:*

$$F(\rho,\sigma) = \max_{|\psi_\rho\rangle, |\psi_\sigma\rangle} |\langle\psi_\rho|\psi_\sigma\rangle|, \tag{2.82}$$

*where the maximization is taken over purifications $\psi_\rho \in \mathcal{H}_Q \otimes \mathcal{H}_R$ and $\psi_\sigma \in \mathcal{H}_Q \otimes \mathcal{H}_R$ of $\rho$ and $\sigma$ respectively, with* $\dim\mathcal{H}_R \geq \dim\mathcal{H}_Q$.

Moreover, for any *fixed* purification of one of the states (say $|\psi'_\rho\rangle$), the fidelity equals maximization over the second purification only, i.e. we have the following lemma, which is direct generalization of analogous lemma from [NC00]:

**Lemma 2.22** *(adapted from [NC00])*

*For any finite-dimensional Hilbert space $\mathcal{H}_Q$ and any two states $\rho, \sigma \in B(\mathcal{H}_Q)$ there holds:*

$$F(\rho,\sigma) = \max_{|\psi_\sigma\rangle} |\langle\psi'_\rho|\psi_\sigma\rangle|. \tag{2.83}$$

*where $|\psi'_\rho\rangle \in \mathcal{H}_Q \otimes \mathcal{H}_R$ with* $\dim\mathcal{H}_R \geq \dim\mathcal{H}_Q$ *is any purification of $\rho$ and the maximization is taken over $|\psi_\sigma\rangle \in \mathcal{H}_Q \otimes \mathcal{H}_R$ denoting a purification of $\sigma$.*

In duality to the trace norm distance, the fidelity is not *decreasing* under quantum operations:

**Lemma 2.23** *For any quantum operation $\Lambda$, and any two quantum states $\rho$ and $\sigma$ there holds*

$$F(\rho,\sigma) \leq F(\Lambda(\rho), \Lambda(\sigma)). \tag{2.84}$$

### 2.7.1 The von Neumann entropy and entropic functions

For any state $\rho$ its von Neumann entropy is defined as

$$S(\rho) = -Tr\rho\log\rho. \tag{2.85}$$

The $\log A$ is an operator with log of eigenvalues of $A$ instead of that of $A$. We will use also notation $S_\rho$. In other wrods, it is the Shannon entropy of its eigenvalues, that is defined for a random variable $X$ over an alphabet $\mathcal{X}$, with a distribution $\{P(X = x) = p_x\}$ as $H(X) := \sum_{x\in\mathcal{X}} p_x \log \frac{1}{p_x}$.

The von Neumann entropy of the state $\rho \in \mathcal{B}(\mathcal{C}^d)$ fulfills the following properties:

1. $S(\rho)$ is non-negative on all states, zero only on pure states.

2. $S(\rho)$ is upper bounded by $\log d$ where $d$ is the dimension of the Hilbert space on which the state resides. This value is attained by the maximally mixed state

3. $S(\rho)$ is a strictly concave function, that is

$$S(\sum_i p_i\rho_i) \geq \sum_i p_i S(\rho_i), \tag{2.86}$$

   for all ensembles $\{(p_i, \rho_i)\}$, and equality holds if and only if $p_i = 1$ for some $i$, or all the states $\rho_i$ are equal to each other (comp. [Mor05]).

4. $S(\rho)$ is a continuous function, as given by the so called Fannes inequality [Fan73]:

   **Lemma 2.24** *(Fannes inequality) For the states $\rho$ and $\sigma$ from $B(\mathcal{H})$ with $dim\mathcal{H} = d$, that satisfies $D(\rho, \sigma) \leq e^{-1}$, there holds*

$$|S(\rho) - S(\sigma)| \leq D(\rho, \sigma) \log d + \eta(D(\rho, \sigma)), \tag{2.87}$$

   *with $\eta(x) = -x \log x$.*

5. The von Neumann entropy of a pure state is zero.

6. The von Neumann entropies of subsystems of any bipartite pure state $|\psi\rangle_{AB}$ are equal:

$$S(\rho_A) = S(\rho_B), \tag{2.88}$$

   with $\rho_X = Tr_X|\psi\rangle\langle\psi|_{AB}$, where $X \in \{A, B\}$.

7. (joint entropy theorem)

$$S(\sum_i p_i|i\rangle\langle i| \otimes \rho_i) = H(\vec{p}) + \sum_i p_i S(\rho_i). \tag{2.89}$$

For a bipartite state $\rho_{AB}$ its quantum mutual information is defined as

$$I(A:B)_\rho := S(A)_\rho + S(B)_\rho - S(AB)_\rho, \tag{2.90}$$

where we use an alternative notation, also common in literature: $S(X)_\rho = S(\rho_X)$. According to this notation, it is default, that entropy $S$ is evaluated on respective subsystems of the bipartite state $\rho$.

The states

$$\rho = \sum_{ij} p_{ij} |e_i f_j\rangle\langle e_i f_j|, \tag{2.91}$$

are called *classically correlated*, since they are diagonal in a product basis $\mathcal{B} = \{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1}$. For these states $I(A:B)_\rho$ equals the Shannon's mutual information of the variables $A$ and $B$ with a joined probability distribution $(p_{ij})$. In particular, when this distribution is homogeneous, we say that the state $\rho$ is *maximally correlated*. This is because its mutual information amounts to $\log d$ which is maximal for classical mutual information. However, it should be also noted, that in general the quantum mutual information can be larger than $\log d$. In particular, $I(A:B)_{|\Psi_+^{(d)}\rangle} = 2\log d$.

The analogue of the classical relative entropy distance is defined as:

$$S(\rho||\sigma) := Tr\rho\log\rho - Tr\rho\log\sigma, \tag{2.92}$$

if only[9] $supp\,\sigma \subset supp\,\rho$. As in classical case, quantum relative entropy is not a distance in mathematical sense, as it is not symmetric. It is however related to the trace norm distance by the following inequality [BZ06]:

$$S(\rho||\sigma) \geq 2[D(\rho,\sigma)]^2. \tag{2.93}$$

The relative entropy fulfills also the condition of monotonicity.

**Theorem 2.25** *[Lin75, Uhl77] For any completely positive map* $\Lambda$*,*

$$S(\rho||\sigma) \geq S(\Lambda(\rho)||\Lambda(\sigma)). \tag{2.94}$$

Analogously as in classical case, the quantum mutual information of a bipartite state $\rho_{AB}$ can be viewed as the relative entropy distance of $\rho_{AB}$ from the tensor product of its subsystems $\rho_A$ and $\rho_B$:

$$I(A:B)_\rho = S(\rho_{AB}||\rho_A \otimes \rho_B). \tag{2.95}$$

[9] By the $supp(\rho)$ we mean the subspace spanned by the eigenvectors of $\rho$ corresponding to its nonzero eigenvalues.

Another important entropic function is the so called Holevo quantity $\chi$. It is a function of an *ensemble*:

$$\chi(\{(p_i, \rho_i)\}_{i=1}^K) = S(\sum_{i=1}^K p_i \rho_i) - \sum_{i=1}^K p_i S(\rho_i). \tag{2.96}$$

It is also known [OP93], that the Holevo quantity is bounded from above by the Shannon entropy of the mixing probability distribution:

$$\chi(\{(p_i, \rho_i)\}) \leq H(\vec{p}). \tag{2.97}$$

## 2.8 Entanglement measures and the phenomenon of bound entanglement

In section (2.4) we have defined entanglement in a qualitative way. It is then tempting to ask a quantitative question: "how much a given state is entangled ?". The theory of entanglement measures tries to answer this question. In case of pure states, the situation is rather clear. Under reasonable assumptions, there is unique measure of entanglement - a function which quantifies it. In case of mixed states however, there seems to be a whole ZOO of different functions which measure how much the state is entangled [Chr06]. The measures which we introduce here will quantify only bipartite entanglement, as we deal here mostly with bipartite entangled states. We also present the phenomenon of *bound entanglement*, which is central to this thesis.

We will invoke here two types of entanglement measures. Those of the first type - *distillable entanglement* and *entanglement cost* are based directly on the so called distant laboratories paradigm, that we have introduced in Section 2.6. They are called *operational entanglement measures*, because they are defined via optimal realization of certain tasks. The idea of operational entanglement measures was introduced by Bennett and coauthors already in paper introducing the distant laboratories paradigm [BBP$^+$96, BDSW96].

The measures of second type are called *axiomatic entanglement measures*. Due to idea of Vedral and coauthors [VPRK97, VP98], and Vidal [Vid00], they are build up formally, so as to satisfy some reasonable axioms. There are quite many axiomatic entanglement measures [PV06, HHHH07]. We will deal here only with few of them, namely: the *relative entropy of entanglement* [VPRK97, VP98], the measure called *negativity* [ZHSL98] (as well as *logarithmic negativity* [VW02]). We invoke also the *entanglement of formation* [BBP$^+$96, BDSW96], which is closely related to the operational measure - entanglement cost.

### 2.8.1 Monotonicity axiom and other properties of entanglement measures

The most intuitive feature, that share all entanglement measures (both operational and axiomatic) is the so called monotonicity condition [BDSW96, VPRK97, VP98]. In what follows, we consider $\mathcal{H}_{in} = \mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_{out} = \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$, for any finite Hilbert spaces $\mathcal{H}_A$ through $\mathcal{H}_{B'}$.

- For a function $E : B(\mathcal{H}_{in}) \to \mathrm{R}_{\geq 0}$ of a bipartite state to be an entanglement measure[10], it is necessary that $E$ can not be increased by any LOCC operation $LOCC \ni \Lambda : B(\mathcal{H}_{in}) \to B(\mathcal{H}_{out})$ performed on any bipartite state $\rho_{AB} \in B(\mathcal{H}_{in})$, that is:
$$E(\rho_{AB}) \geq E(\Lambda(\rho_{AB})). \tag{2.98}$$

This statement reflects the intuition that entanglement is a different type of correlations than that which can be created via local quantum operations and classical communication. More formally, there are two types of the above monotonicity. The first is just called a *monotonicity*, and the second is called a *strong monotonicity*.

The strong monotonicity condition says, that entanglement measure should not increase on average i.e.
$$E(\rho) \geq \sum_i p_i E(\sigma_i), \tag{2.99}$$
where $\rho$ is transformed via an LOCC operation $\Lambda$ into $\sigma_i$ with probability $p_i$.

Another important postulate, which is in fact indicated by the axiom of monotonicity [HHHH07] is the axiom of *vanishing on separable states*:

- For a function $E$ of a bipartite state to be an entanglement measure, it is necessary that $E(\rho) = 0$ for any $\rho \in SEP$.

According to Vidal [Vid00], the monotonicity (the usual or strong), and vanishing on separable states are the only mandatory postulates that any entanglement measure has to satisfy. Vidal has also coined the name '*entanglement monotone*' for those functions which are monotonic under LOCC, that is which are either only decreased or increased LOCC operation. We will also use this name. For the purpose of this thesis, we collect the two axioms discussed above in a definition of entanglement measure:

[10] To be more precise one should define entanglement measure $E$ as a family of functions $f_{n_1,n_2}$ each defined on $\mathcal{C}^{\otimes n_1} \otimes \mathcal{C}^{\otimes n_2}$ which is consistent, i.e. for natural $k, l, m, n$ with $k \geq m$ and $l \geq n$, there exists an embedding $V$ which is a product of two isometries, such that $f_{k,l}(V(\rho)) = f_{m,n}(\rho)$. In what follows, for a bipartite state $\rho \in \mathcal{C}^{n_1} \otimes \mathcal{C}^{n_2}$ by $E(\rho)$ we mean $f_{n_1,n_2}(\rho)$. This convention is an implicit one in algebra, as the same is assumed e.g. for the trace of a matrix

**Definition 2.15** *A function of bipartite state which is monotonous under LOCC operations in either usual or strong sense, and vanishes on separable states is called an entanglement measure (or equivalently an entanglement monotone).*

Also, we will use informally the notion of *operational entanglement measure* which refers to those entanglement monotones which are defined via some task e.g. of transforming $n$ copies of a state $\rho$ into some $k$ copies of other state $\sigma$, by means of LOCC operations (see Section 2.8.2).

There are however some additional postulates which are welcome. The postulates correspond to some properties of entanglement measures, which proved useful in quantitative approach to entanglement. They are satisfied by certain axiomatic entanglement measures.

1. Normalization: $E(|\psi^-\rangle^{\otimes n}) = n$
2. Asymptotic continuity:
$$||\rho_n - \sigma_n|| \to 0 \Rightarrow \frac{|E(\rho_n) - E(\sigma_n)|}{\log d_n} \to 0, \tag{2.100}$$
where $\rho_n, \sigma_n \in B(\mathcal{H}_n)$ and $dim\mathcal{H}_n = d_n$.
3. convexity:
$$E(\sum_i p_i \rho_i) \leq \sum_i p_i E(\rho_i), \tag{2.101}$$
for any ensemble of states $\{p_i, \rho_i\}$.

Additionally, some entanglement measures may have another property called *additivity* i.e. satisfy:
$$E(\rho^{\otimes n}) = nE(\rho). \tag{2.102}$$
It is sometimes also called an *additivity on tensor product*, to distinguish it from what we call *full additivity*, which is stated as follows:
$$E(\rho \otimes \sigma) = E(\rho) + E(\sigma), \tag{2.103}$$
for any two states $\rho$ and $\sigma$. If some entanglement measure is not additive, then one can consider its *regularization*, defined as:
$$E^\infty(\rho) := \lim_{n\to\infty} \frac{E(\rho^{\otimes n})}{n}. \tag{2.104}$$

We now illustrate the fact that axiomatic approach leads to the clarified view on entanglement measures with the following theorem [HHH00].

**Theorem 2.26** *(Extremal measures theorem) For entanglement measure $E$ which is monotonic under LOCC, asymptotically continuous and satisfies $E(|\Psi_+^{(d)}\rangle) = \log d$ we have*

$$E_D \leq E^\infty \leq E_C. \tag{2.105}$$

### 2.8.2 Distillable entanglement and entanglement cost

Informally, the *distillable entanglement* measures how much pure entanglement ( of pure entangled states) can be obtained from many copies of a system in some state $\rho$, via LOCC operations. That is, Alice and Bob share $n$ copies of a system in some (generally in a mixed) state $\rho$. Their task is to obtain a maximal possible number of copies $k$ of system in state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ of eq. (2.42). To this end, they can only perform quantum operations in their laboratories, and communicate classically (e.g. via phone), that is perform LOCC operations. The maximal ratio $\frac{k}{n}$ is the distillable entanglement of the input state $\rho$.

Formally, one has to deal with inaccuracy of the operations. Instead of many copies of the singlet state, they will obtain some state $\sigma_n$ which should for high $n$ approach the desired outcome $|\psi^-\rangle^{\otimes k}$, in trace norm distance. For this reason, the definition of distillable entanglement reads[11] [Hor01, PV06]:

**Definition 2.16** *For a bipartite state $\rho_{AB} \in B(\mathcal{C}^{d_1} \otimes \mathcal{C}^{d_2})$ consider a sequence $P_n$ of LOCC operations, such that $P_n(\rho_{AB}^{\otimes n}) = \sigma_n$, where $\sigma_n \in B([\mathcal{C}^2 \otimes \mathcal{C}^2]^{\otimes m_n})$.*

*The set $\mathcal{P} \equiv \cup_{n=1}^{\infty}\{P_n\}$ is called a protocol of distillation of the state $\rho_{AB}$ if*

$$\lim_{n\to\infty} ||\sigma_n - |\psi^-\rangle\langle\psi^-|^{\otimes m_n}|| = 0. \tag{2.106}$$

*For a given protocol of distillation $\mathcal{P}$, its rate is given by*

$$\mathcal{R}(\mathcal{P}) = \limsup_{n\to\infty} \frac{m_n}{n}. \tag{2.107}$$

*The entanglement distillation of the state $\rho_{AB}$ is then given as:*

$$E_D(\rho_{AB}) = \sup_{\mathcal{P}} \mathcal{R}(\mathcal{P}), \tag{2.108}$$

*where supremum is taken over all distillation protocols $\mathcal{P}$ of $\rho_{AB}$.*

If the state has zero $E_D$ we say, that it is *not distillable*. The second measure, which we invoke in this section is called *entanglement cost*. It is dual to the distillable

[11] Other formal definitions are possible. They are however equivalent to the above one [Rai98].

entanglement, as it measures how much pure entanglement one needs to invest in order to create many copies of a given output state $\rho$. Again, only LOCC operations are allowed - this time in process of creation. The minimal ratio of the number of $k$ of systems in a singlet state to the number of output state $n$ equals entanglement cost, and denoted as $E_C$.

The formal definition of entanglement cost is the following [Hor01, PV06]:

**Definition 2.17** *For a bipartite state $\rho_{AB} \in B(\mathcal{C}^{d_1} \otimes \mathcal{C}^{d_2})$ consider a sequence $P_n$ of LOCC operations, such that $P_n(|\psi^-\rangle\langle\psi^-|^{\otimes n}) = \sigma_n$, where $\sigma_n \in B([\mathcal{C}^2 \otimes \mathcal{C}^2]^{\otimes m_n})$.*

*The set $\mathcal{P} \equiv \cup_{n=1}^{\infty}\{P_n\}$ is called a protocol of formation of the state $\rho_{AB}$ if*

$$\lim_{n\to\infty} ||\sigma_n - \rho_{AB}^{\otimes m_n}|| = 0. \tag{2.109}$$

*For a given protocol of formation $\mathcal{P}$, its rate is given by*

$$\mathcal{R}(\mathcal{P}) = \limsup_{n\to\infty} \frac{n}{m_n}. \tag{2.110}$$

*The entanglement cost of the state $\rho_{AB}$ is then given as:*

$$E_C(\rho_{AB}) = \sup_{\mathcal{P}} \mathcal{R}(\mathcal{P}), \tag{2.111}$$

*where supremum is taken over all protocols $\mathcal{P}$ of formation of $\rho_{AB}$.*

Let us note, that the operational measures are by definition monotonic. The two, which we have presented here, straightforwardly satisfy the normalization condition $E_D(|\psi^-\rangle\langle\psi^-|) = E_C(|\psi^-\rangle\langle\psi^-|) = 1$, and vanish on separable states. $E_D$ and $E_C$ are also asymptotically continuous [BZ06]. It is however quite hard to find exact values of operational measures. Instead, there are known some upper and lower bounds on them, in form of some axiomatic measures, which are more computable. An axiomatic measure, which is directly related to entanglement cost is *entanglement of formation*, defined as

$$E_f(\rho_{AB}) := \inf_{\{p_i, |\psi_i\rangle_{AB}\}} \sum_i p_i S_A(|\psi_i\rangle_{AB}), \tag{2.112}$$

where the infimum is taken over all pure ensembles of $\rho_{AB}$ (that is such that $\rho_{AB} = \sum_i p_i|\psi_i\rangle\langle\psi_i|_{AB}$), and $S_A$ denotes the entropy of subsystem $A$ of bipartite pure state $|\psi_i\rangle$. It is shown in [HHT01], that regularized $E_f$ equals entanglement cost (see eq. (2.104)):

$$E_C = E_f^{\infty}. \tag{2.113}$$

Note that if the entanglement of formation was an additive measure, we would have the formula for entanglement cost. This is however one of the difficult open problems (see Werner's list [Wer99]).

### 2.8.3 Relative entropy of entanglement

The relative entropy of entanglement is defined as follows:

$$E_r(\rho) := \inf_{\sigma \in SEP} S(\rho||\sigma), \tag{2.114}$$

where $SEP$ denotes the set of separable states and $S(\rho||\sigma) = Tr\rho \log \rho - Tr\rho \log \sigma$ is the relative entropy distance. It is shown to be strongly monotonic. This measure is usually associated with a kind of distance between the state $\rho$ and the convex set of separable states. However, the relative entropy of entanglement is not a distance in mathematical sense, as e.g. it is not symmetric.

The relative entropy is not additive for some states [VW01], hence we sometimes deal with its regularization:

$$E_r^{\infty}(\rho) := \lim_{n \to \infty} \frac{E_R(\rho^{\otimes n})}{n}. \tag{2.115}$$

Both the relative entropy and the regularized relative entropy of entanglement are upper bounds on the distillable entanglement. The regularized relative entropy of entanglement is also a lower bound on entanglement cost [HHH00]. As it is usual in case of entanglement measures, acting on a bipartite state with a unitary transformation which is a tensor product of two (local) unitary transformation on each site does not change the relative entropy of entanglement. Formally we have the following lemma:

**Lemma 2.27** *For any bipartite state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$, and two arbitrary unitary transformations $U_A$ and $U_B$ acting on a Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively we have:*

$$E_r(\rho_{AB}) = E_r(U_A \otimes U_B \rho_{AB} U_A^{\dagger} \otimes U_B^{\dagger}). \tag{2.116}$$

**Proof.** This lemma follows easily from the fact that the von Numann entropy is not changed under unitary rotation, the tensor product of unitary transformations maps separable states into separable states, and the property of trace $\mathrm{Tr}XY = \mathrm{Tr}YX$ for square $n \times n$ matrices.

### 2.8.4 Negativity and logarithmic negativity

The other measure of entanglement was introduced in [ZHSL98]. It is a quantitative version of the Peres criterion. Due to Peres criterion, for a state to be separable, it should become positive operator after partial transposition. Hence, if a state becomes negative operator (has negative eigenvalues) after partial transposition, it

must be entangled. One can then ask "how much negative" the state becomes after partial transposition. The entanglement measure which reports this, called *negativity* is defined for a bipartite state $\rho$ as

$$\mathcal{N}(\rho) = \sum_{\lambda<0} |\lambda|, \tag{2.117}$$

where $\lambda$ are eigenvalues of $\rho^\Gamma$ (where $\Gamma$ is partial transpose).

This measure has an advantage, that it is easily computable in comparison to other measures of entanglement, even those axiomatic like relative entropy of entanglement.

In [VW02] it was shown, that the negativity fulfills the monotonicity condition (is an entanglement monotone). There also a variation of this measure was introduced, called *logarithmic negativity* (also log negativity). It is defined as

$$E_N(\rho) := \log ||\rho^\Gamma||, \tag{2.118}$$

and it is related to $\mathcal{N}$ as follows: $E_{\mathcal{N}}(\rho) = \log(\frac{2\mathcal{N}(\rho)+1}{2})$. The log negativity is an upper bound [VW02] on distillable entanglement, i.e. for any bipartite state $\rho$ there holds:

$$E_N(\rho) \geq E_D(\rho). \tag{2.119}$$

### 2.8.5 The phenomenon of bound entanglement

We provide now the definition of bound entangled states.

**Definition 2.18** *[HHH98] A bipartite state $\rho_{AB} \in B(\mathcal{C}^{d_1} \otimes \mathcal{C}^{d_2})$ is called bound entangled if it is entangled and not distillable, i.e. if there holds $E_D(\rho_{AB}) = 0$.*

The first bound entangled states were already present in [Hor97], yet they were shown to have this property in [HHH98]. This is because the states from [Hor97] were entangled and PPT (see section 2.4), and in [HHH98] general result is shown, which we state below:

**Theorem 2.28** *[HHH98] Any bipartite entangled PPT state is bound entangled.*

Up to now, no algorithm is known which determines if a given state is bound entangled. It is relatively easy, to provide example of a PPT state. Yet it is then hard to determine, if such state is entangled. There are however some constructions of the families of bound entangled states, [BP00, BDM$^+$99, WW01] (see [Cla06] for many other results in this filed).

In case of the first examples of bound entangled states, it was not clear if such states has nonzero entanglement cost. Vidal and Cirac was the first to show, that

certain bound entangled states (those introduced in [BDM$^+$99]) has nonzero entanglement cost. Further such results were provided in [VWW04, HV00]. Due to the recent result of Yang and coauthors, [YHHSR05], it is known, that any state which is entangled, has nonzero entanglement cost, hence the above definition of bound entangled states can be rephrased in the following manner:

**Definition 2.19** *(see [YHHSR05]) A bipartite state $\rho_{AB} \in B(\mathcal{C}^{d_1} \otimes \mathcal{C}^{d_2})$ is bound entangled if and only if there holds:*

$$0 = E_D(\rho_{AB}) < E_C(\rho_{AB}). \tag{2.120}$$

This definition clarifies the name of this class of states. Their entanglement is called bound, as it can not be turned into a form of entanglement of pure states. The bound entangled states exemplifies extremal irreversibility of the creation-distillation process in distant laboratories scenario. To create a bound entangled states one needs pure entanglement, but having created, one can not regain this kind of entanglement at all.

The phenomenon of existence of bound entangled states is in a sense central to this thesis. The main result of this manuscript shows that there are states which, though bound entangled, are at the same time key distillable (see Chapter 5).

## 2.9 bipartite and tripartite distant sites scenarios

Having described the formal background, we can formulate the entanglement as well as cryptographic scenarios which we deal with in further chapters.

**Chapter 3**

The most basic scenario is called the quantum worst case scenario, discussed informally in Section 1.5.1. It involves the sites of Alice, Bob and Eve. The three parties share a *pure tripartite quantum state* $|\psi\rangle_{ABE}$, so that each of the parties have access to its corresponding subsystem $A$, $B$ and $E$ respectively. This scenario is static, in a sense, that we do not consider yet any operations performed on the state. We use it in order to study the structure of *bipartite* states $\rho_{AB}$, so that they are secure with respect to Eve, who holds its *purifying system* $E$.

We will mostly focus on bipartite states of systems which satisfy:

$$\dim A = d \times d_{A'} \text{ and } \dim B = d \times d_{B'}, \tag{2.121}$$

for some natural $d$, where $\{0, \ldots d-1\}$ will be the range of secret key (see also Section 3.8) Thus we will consider bipartite states with *four* subsystems. For easier notation we label the subsystems as them as A and A' for Alice and B and B' for

Bob, so that they share a bipartite state: $\rho_{ABA'B'}$. It turns out that according to the sequence of labels, the matrix of $\rho_{ABA'B'}$ has easier description, and recalls the usual bipartite matrix with only *two* subsystems $A$ and $B$, but with blocks of matrices instead of matrix elements (see e.g. Section 3.4). The system $AB$ of a state $\rho_{ABA'B'}$ will be sometimes called main part *key part* and the system $A'B'$ will be called side part. When the state $\rho_{ABA'B'}$ will be perfect for cryptography (the so called *private states*) , instead of main part we will say the key part, (the part from the key can be obtained) and instead of side part we will say shield (the part sharing of which makes key part secure).

**Chapter 4: the LOCC scenario, LOPC scenario, and the worst-case LOPC scenario**

In this chapter we consider two scenarios. The first is bipartite, second is tripartite.

The bipartite scenario is the LOCC scenario scenario, which we have discussed in Section 1.3. It involves the site of Alice and that of Bob. They share $n$ systems in the same state $\rho_{AB}$ for some natural $n$. This scenario is 'dynamic' in a sense, that they can also perform the LOCC operations on the whole shared state $\rho_{AB}^{\otimes n}$.

The tripartite scenario steaming from classical cryptography is the *LOPC scenario*, discussed in Section 1.5.1 (see also [DW05, DW04]). In this scenario we consider three sites: for Alice, Bob the eavesdropper Eve. Alice, Bob and Eve share $n$ systems in the same state $\rho_{ABE}$ for some natural $n$. They can perform the so called *LOPC* operations (local operations and public communication) on the whole shared state $\rho_{ABE}^{\otimes n}$. These operations are introduced in Section 4.2, with clear correspondence to the LOCC operations. We focus on the special case of the LOPC scenario, where $\rho_{ABE}$ is a *pure* state, so that Alice, Bob and Eve share $|\phi\rangle\langle\phi|_{ABE}^{\otimes n}$ for some pure state $|\phi\rangle_{ABE}$. This is the worst case of LOPC scenario, since due to observation 2.7, it is the most generous to Eve, while giving to Alice and Bob $n$ copies of the state $\rho_{AB} = \mathrm{Tr}_E \rho_{ABE}$.

# Chapter 3

# Private states

In this chapter we present a slightly improved and extended version of the material, that can be found in [HHHO05a], Sections II-V, and [HPHH05]. We introduce here the notion of *private states*. We then prove, that these are quantum states, that contain directly accessible, ideally secure classical key. Till recent, only the maximally entangled states were considered as those which have directly accessible key. The class of private states is much broader than the class of maximally entangled states, containing apart from the latter, also a wide class of mixed entangled states.

In Section 3.1 we provide a definition of quantum states that have secure key. Subsequently, in Section 3.2 we define the class of so called *private states* and show, that these are precisely those bipartite states which have a key. Private states have easy description involving only three elements: a maximally entangled state $|\Psi_+^{(d)}\rangle$ on $d \otimes d$-dimensional system $AB$, an arbitrary state $\rho$ on some additional bipartite system $A'B'$ and a special unitary rotation $U$. The subsystem $AB$ of the private state $\gamma$ is called a *key part*, as it provides a key when measured. The subsystem $A'B'$ is called a *shield*, as its role is just 'shielding' the key part from Eve. The $|\Psi_+^{(d)}\rangle$, and $\rho$ in the structure of the private state are together subjected to unitary operation called *twisting*.

Basing on the notion of twisting, we introduce the operation of *privacy squeezing*, which acts on a private state giving a more entangled state with similar security to that of the original state (see Section 3.3.2). It serves as a mathematical tool that allows for easy estimation of security content of a quantum state.

In Section 3.4 we explore variety of notations for the class of private bits and private dits. We then pass to study entanglement properties of private states. We also give two examples of the families of pbits (with special form of a 'shield'), denoted as $\rho_{flower}^{(d)}$ and $\gamma^V$. In Section 3.5 we study entanglement properties of these states. We prove, that for $\gamma^V$, the amount of key contained in the state is strictly

greater than the distillable entanglement.

We then study how some entanglement measures evaluated on $\rho^{(d)}_{flower}$, change if one traces out a qubit of its key part system. We show, that $E_N$, $E_C$ (and $E_f$) can decrease by arbitrarily large amount (as a function of dimension of its shield d). This effect revealed by the family of (generalized) flower states we call *locking of entanglement*, since holding a single qubit one can controll arbitrarily large amount of entanglement. We also show that $E_r$ ($E_r^\infty$) is not lockable.

In Section 3.6 we propose then the so called *irreducible private states* - the states containing exactly $\log d$ bits of key, that can be associated with 'units' of privacy (see Section 3.6). We also discuss the states which approximate private bits in trace norm distance. We argue that these are states with a special submatrix with trace norm close to $\frac{1}{2}$. This result seems to be a generalization of an analogous property of states approximating maximally entangled states in two qubits, where submatrix is just a matrix element.

In Section 3.8 we discuss what happens if we change the interpretation of 'direct accessibility' of classical key. Two such interpretations leads to the two classes of states $C_2$ (cf. [RS07]) and $C_3$. We show that they are equivalent in a sense that any state from these classes can be changed into private states by adding locally (separately on Alice and Bob's site) some ancilla states and performing locally unitary transformations. Since such local operations do not change entanglement monotones of bipartite states, we consider these definitions as equivalent to the one we have chosen.

In Section 3.9.1 we consider some practical reasons which justify the choice of definition of the states which have key (definition 3.1), and in consequence - dealing with private states. At the very end of this chapter we also comment on the results obtained further on this subject in literature.

## 3.1 Defining secure key

In this section we provide a definition of states that have ideal secure key. Since other definitions of security are possible, we explain why we choose this one. In what follows we first introduce the scenario that we are going to deal with in this chapter.

### 3.1.1 Scenario for definition of secure key - the worst case tripartite scenario

In scenario we assume in this chapter, the honest parties traditionally called Alice and Bob are given a bipartite state $\rho_{AB}$. The eavesdropper called Eve is given the standard purifying system $\rho_E$ of $\rho_{AB}$. In turn, the three parties share a (tripartite)

pure state $|\psi_\rho\rangle^{ABE}$, which is the standard purification of state $\rho_{AB}$, each holding its corresponding subsystem.

The above scenario we call the worst case tripartite scenario, since having the purifying system of $\rho_{AB}$, Eve has the most power she can have while Alice and Bob are sharing the state $\rho_{AB}$. This is because by local operation on the standard purifying system, Eve can obtain any other extending system of $\rho_{AB}$, in particular, any other purifying system (see Observation 2.7).

This scenario will be developed in Chapter 4, where we introduce the key distillation protocol. There Alice and Bob will transform the state. Here we just study the very structure of the state, so that it contain secure key.

As it will appear natural in context of secret key content, we consider the bipartite systems of Alice and Bob that has two subsystems each. To avoid double prime notation we call them $A$ and $A'$ on Alice's site and $B$ and $B'$ on Bob's. We will consider hence a bipartite states $\rho_{ABA'B'}$, yet with four subsystems. We assume also that systems $A$ and $B$ are of the same dimension $d$ so that $\{0, \ldots, d-1\}$ is the range of key. We will sometimes refer to $AB$ as to the main part and to $A'B'$ as to the side part (see Section 3.2, where these systems are called key part and shield respectively).

Considering the state $\rho_{ABA'B'}$, we will be actually interested in the subsystem $ABE$ of the purification $|\psi_\rho\rangle_{ABA'B'E}$ of $\rho_{ABA'B'}$, after it was measured in basis $\mathcal{B} = \{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1}$ on $AB$. Such state has the form

$$\rho_{ccq} = \sum_{i,j=0}^{d-1} p_{ij} |e_i f_j\rangle_{AB}\langle e_i f_j| \otimes \rho_{ij}^E. \tag{3.1}$$

A state of this form is called a ccq state[1]. To indicate the product basis $\mathcal{B}$ on $AB$ of the *ccq* state, we sometimes call it a $\mathcal{B}$-ccq state. In the above context, when we know the origin of such state, we will call it *the ccq state of the state* $\rho_{ABA'B'}$. For states with only two subsystems: $\rho_{AB}$ by its $\mathcal{B}$-ccq state we mean the state obtained via a purification of the state $|\psi_\rho\rangle_{ABE}$, measured on $AB$ in basis $\mathcal{B}$.

### 3.1.2 Definition of secure key

We begin with some intuitions which lead to the definition of states that have ideally secure key (called also states from class $C_1$). In particular, we consider the following "predefinition":

[1]The name *ccq* stands for 'classical-classical-quantum', reflecting the intuition, that subsystems of Alice and Bob are in a sense in 'more classical' state being the output of measurement in basis $\mathcal{B}$, then the state of Eve's subsystem, which is not measured. It was coined in [HHHO05a] after similar name of cqq states in [DW05] (see also [Chr02]).

- We say, that bipartite quantum state has key if it has directly accessible, classical key.

In what follows we will explain what we will mean by "classical key" and its "direct accessibility", which will lead to the definition of quantum states that have key.

**classical key**

Following [DW05, DW04] (see also [Chr02]), to formalize what we mean by the classical key, we base on classical cryptography [Wyn75, CK78, Mau93, AC93, Mau93]. There, ideally secure key is represented by the following distribution:

$$P_{ideal} = P(K_A, K_B)P(E) \tag{3.2}$$

where $P(K_A, K_B) = \frac{1}{d}\delta_{ij}$ with $\{i, j = 0, ..., d-1\}$, and $P(E)$ is some distribution of Eve, which is independent from that of Alice and Bob.

Basing on this approach, one easily finds the quantum analogue of distribution 3.2 to have form:

$$\left(\frac{1}{d}\sum_{i=0}^{d-1}|ii\rangle\langle ii|_{AB}\right)\otimes\rho_E. \tag{3.3}$$

Since change of the alphabet does not spoil the security of key, in general we can have the following state:

$$\rho_{ccq}^{ideal} := \left(\frac{1}{d}\sum_{i=0}^{d-1}|e_if_i\rangle\langle e_if_i|_{AB}\right)\otimes\rho_E. \tag{3.4}$$

In what follows, we will treat this state as representing the classical key. We will refer to this state also as the *ideal $\mathcal{B}$-ccq state*, or just an ideal ccq state in case of standard product basis.

**direct accessibility**

To formalize the direct accessibility we base on example of a maximally entangled state:

$$|\Psi_+^{(d)}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|e_if_i\rangle. \tag{3.5}$$

According to Definition 2.2, and Lemma 2.6, any purification of this state has the form $|\psi_{ABE}\rangle = |\Psi_+^{(d)}\rangle_{AB}\otimes|\phi\rangle_E$ for some pure state $|\phi\rangle_E$ on system E. Hence one gets a state $\rho_{ccq}^{ideal}$ after measurement of $|\psi_{ABE}\rangle$ on system AB in a product basis $\{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1,d-1}$.

Our intuition is that the access via complete von Neumann measurements performed on the systems $A$ and $B$ of bipartite state $\rho_{AB}$ is an example of direct access.

Following this intuition as a direct access we will mean in general the complete von Neumann measurements on *subsystems* of systems $A$ and $B$. This is because, we understand that one 'has key', when one 'knows' (have a labeled system) where to measure in order to get it.

Thus we arrived at the need for splitting systems $A$ and $B$ into two: $A = A_{key}A_{rest}$ and $B = B_{key}B_{rest}$, where $A_{key}$ and $B_{key}$ (of the same dimension $d$) are distinguished as those, on which complete von Neumann measurement yields key. For this reason we will consider states of *four* subsystems: two on Alice's and two on Bob's site. In what follows, for simplicity, the $A_{key}$ and $B_{key}$ we label as $A$ and $B$ and are sometimes called the main part. The $A_{rest}$ and $B_{rest}$ will be denoted as $A'$ and $B'$. These are additional systems together called sometimes a side part. In case of the state which has ideally secure key, we will call main part as key part and side part as a shield.

**Definition of quantum states that have $\mathcal{B}$-key.**

**Definition 3.1** *(of states that have $\mathcal{B}$-key) Let $\rho_{ABA'B'} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ with $\dim\mathcal{H}_A = \dim\mathcal{H}_B = d$. The state $\rho_{ABA'B'}$ is called* **secure** *with respect to a basis $\mathcal{B} = \{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1}$ if the state obtained via measurement on $AB$ subsystem of its purification in basis $\mathcal{B}$ followed by tracing out $A'B'$ subsystem (i.e. its ccq state) is of the form:*

$$\left(\sum_{i,j=0}^{d-1} p_{ij}|e_if_j\rangle\langle e_if_j|_{AB}\right) \otimes \rho_E. \tag{3.6}$$

*Such a state $\rho_{ABA'B'}$ will be also called "$\mathcal{B}$ secure". Moreover if the distribution $\{p_{ij}\} = \{\frac{1}{d}\delta_{ij}\}$ so that the ccq state is of the form*

$$\left(\sum_{i=0}^{d-1} \frac{1}{d}|e_if_i\rangle\langle e_if_i|_{AB}\right) \otimes \rho_E, \tag{3.7}$$

*the state $\rho_{ABA'B'}$ is said to* **have $\mathcal{B}$-key**.

If the basis $\mathcal{B}$ is known from a context, or just assumed to be a product of computational basis, we say that a given state $\rho$ has key.

**Remark 3.1** *Note, that if Alice or Bob wants to obtain key from the state $\rho_{ABA'B'}$ that have $\mathcal{B}$-key, she has to measure its subsystem $A(B)$ in basis $\mathcal{B}$. The resulting state on system $AB$ can be directly used to encrypt via the one-time pad cypher. The system $A'B'$ they do not have to use, just keep it away from Eve. Thus the operation of partial trace in definition above is not done by Alice and Bob, and serves here as a mathematical tool of ignoring subsystems $A'B'$.*

The states which satisfy definition 3.1 will be referred to as from class $C_1$. Of course, there is no a priori reason why to choose such an interpretation of 'direct accessibility', as described in previous section. In particular, one can have objection, that this approach distinguishes only special class of bipartite states - those which have dimension of Alice's and Bob's subsystem dividable by common number $d$. To cover the case of *arbitrary bipartite state*, one has to change the meaning of 'direct accessibility'. We address this problem in Section 3.8. We consider two other meanings of 'direct accessibility' which gives rise to the two different definitions of quantum states that have 'directly accessible classical key' (called states from classes $C_2$ (cf. [RS07]) and $C_3$, respectively). We show however, that the states from class $C_2$ and $C_3$ one can easily transform into some states from $C_1$ (by adding locally pure ancillary state and performing unitary transformation) and vice versa, they can be easily obtained from some states of class $C_1$. For this reason we can focus now just on characterization of states from class $C_1$.

## 3.2 Private states - characterizing the class of quantum states that have key

In this section we define the class of private states. The main result of this Chapter is theorem 3.2 which shows, that the states which have $\mathcal{B}$-key, are exactly private states.

### 3.2.1 Private states - definition

**Definition 3.2** *(of private states) A state $\rho_{ABA'B'}$ of a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'}$ with dimensions $d_A = d_B \equiv d$, $d_{A'}$ and $d_{B'}$, of the form*

$$\gamma^{(d)} = \frac{1}{d} \sum_{i,j=0}^{d-1} |e_i f_i\rangle\langle e_j f_j|_{AB} \otimes U_i \sigma_{A'B'} U_j^\dagger, \tag{3.8}$$

*where the state $\sigma_{A'B'}$ is an arbitrary state of subsystem $A'B'$, $U_i$'s are arbitrary unitary transformations, is called* **private state** *or* **pdit**. *In case of $d = 2$ the state is called* **pbit**. *A pdit is denoted as $\gamma^{(d)}_{\mathcal{B}}$ or $\gamma^{(d)}$ if the basis $\mathcal{B} = \{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1}$ is either irrelevant, or it is just a standard product basis. The set of all private states with $4 \geq \dim AB \leq d \times d$ and $\dim A'B' \leq d' \times d'$ will be denoted as $PS^{(d,d')}$.*

These states are also called $\gamma$-states. The part $AB$ will be further called as the **key part** of the pdit, while the subsystem $A'B'$ its **shield**. This is because from the $AB$ subsystem one directly has secure key, which is in general case secure due to the fact, that $A'B'$ is kept by Alice and Bob - acting as a shield. This reflects the

intuitive fact, that the less entangled is the key part, the more needed is the shield, to keep the latter away from Eve.

Let us note, that the shield may reside also only on one site (say Alice's) - this is when $d_{B'} = 1$. It can be also absent (when $d_{A'} = d_{B'} = 1$) - in that case the $AB$ system is in maximally entangled state $|\Psi^{(d)}\rangle_{AB} = \sum_{i=0}^{d-1} \frac{1}{d}|e_i f_i\rangle$ which does not need any shield to be secure. Then, also, the unitary transformations $U_i$ reduces to some complex phases $e^{\phi_i}$. Thus the set of maximally entangled states is the subset of the set of private states:

$$\forall_{2\leq d,d'<\infty}\ MS^{(d)} \subset PS^{(d,d')}. \tag{3.9}$$

To indicate both dimensions of the key part and shield, we denote the private states from $PS^{(d,d')}$ as $\gamma^{(d,d')}$. We will sometimes denote as $PS$ the set of all private states, i.e. with arbitrary dimensions of key part and shield.

In special case, where the unitary transformations $U_i$ are identity (perhaps with some phases $e^{\phi_{ij}}$ on diagonal), we call the private state a *basic pdit* or *basic pbit* depending on the dimension of its key part.

To express this formally, we introduce some notations. By $P_{AB}^{(d),\mathcal{B}}$ we mean the projector onto the state $\sum_{i=0}^{d-1} \frac{1}{\sqrt{d}}|e_i f_i\rangle$. Sometimes, we will also denote this projector as $P_{\mathcal{B}}^{(d)}$, omitting the information about system. If we omit also the basis $\mathcal{B}$ in super or subscript, we mean that this basis is chosen to be a product of two standard basis.

**Definition 3.3** *(of a basic pdit) A state $\rho_{ABA'B'}$ of a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'}$ with dimensions $d_A = d_B \equiv d$, $d_{A'}$ and $d_{B'}$, of the form*

$$\rho_{ABA'B'} = P_{AB}^{(d),\mathcal{B}} \otimes \sigma_{A'B'}, \tag{3.10}$$

*is called a* **basic pdit**.

Let us note, that the definition of private states does not invoke the purifying system, as it is in definition 3.1. Despite of this fact, the two definitions are equivalent.

**Theorem 3.2** *Any state $\rho_{ABA'B'}$ of a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'}$ with dimensions $d_A = d_B \equiv d$, $d_{A'}$ and $d_{B'}$, has $\mathcal{B}$-key if and only if it is of the form*

$$\rho_{ABA'B'} = \frac{1}{d}\sum_{i,j=0}^{d-1} |e_i f_i\rangle\langle e_j f_j|_{AB} \otimes U_i \sigma_{A'B'} U_j^\dagger \tag{3.11}$$

*where the state $\sigma_{A'B'}$ is an arbitrary state of subsystem $A'B'$, $U_i$'s are arbitrary unitary transformations and $\mathcal{B} = \{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1}$.*

**Proof.** ($\Leftarrow$) Let us consider the following state:

$$|\psi\rangle_{ABA'B'E} = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |e_i\rangle_A \otimes |f_i\rangle_B \otimes |\psi^{(i)}\rangle_{A'B'E}, \tag{3.12}$$

where $|\psi^{(i)}\rangle_{A'B'E} = U_i \otimes \mathrm{I}_E |\psi\rangle_{A'B'E}$ with $|\psi\rangle_{A'B'E}$ being some fixed purification of the state $\sigma_{A'B'}$. It is easy to see that $|\psi\rangle_{ABA'B'E}$ is a purification of the pdit $\rho_{ABA'B'}$ (see Sec. 2.3.2). After measuring this purification on $AB$ system in basis $\mathcal{B}$, we obtain the state:

$$\sigma_{ABA'B'E} = \sum_{i=0}^{d-1} \frac{1}{d} |e_i f_i\rangle\langle e_i f_i|_{AB} \otimes U_i \otimes \mathrm{I}_E |\psi\rangle\langle\psi| U_i^\dagger \otimes \mathrm{I}_E \tag{3.13}$$

By linearity of the partial trace, we have

$$Tr_{A'B'} \sigma_{ABA'B'E} = \sum_{i=0}^{d-1} \frac{1}{d} Tr_{A'B'} (|e_i f_i\rangle\langle e_i f_i|_{AB} \otimes U_i \otimes \mathrm{I}_E |\psi\rangle\langle\psi| U_i^\dagger \otimes \mathrm{I}_E) \tag{3.14}$$

Since partial trace does not depend on the choice of basis (see Section 2.3), for each $i$ we can trace the system $A'B'$ in different basis, namely in $\{U_i|k\rangle\}_{k=0}^{d_{A'}d_{B'}-1}$. This gives, that the subsystem $ABE$ of the latter state has form:

$$\sum_{i=0}^{d-1} \frac{1}{d} |e_i f_i\rangle\langle e_i f_i|_{AB} \otimes \rho_E \tag{3.15}$$

where $\rho_E = Tr_{A'B'} |\psi\rangle\langle\psi|_{A'B'E}$. The above state has desired form of the state $\rho_{ccq}^{ideal}$, which ends the proof of this part of theorem.

**Proof.** ($\Rightarrow$)

In this part we assume, that the state $\rho_{ABA'B'}$ has $\mathcal{B}$-key i.e. that after measurement on it's $AB$ part, one gets perfectly correlated state, uncorrelated with Eve:

$$\left( \sum_{i=0}^{d-1} \frac{1}{d} |e_i f_i\rangle\langle e_i f_i|_{AB} \right) \otimes \rho_E. \tag{3.16}$$

Let us consider general pure state for which dimensions of $A, B$ are $d$, dimensions of $A', B'$ are $d_{A'}, d_{B'}$ respectively, and dimension of subsystem $E$ is the smallest one which allows for the whole state being a pure one.

$$|\psi\rangle = |\psi\rangle_{ABA'B'E} = \sum_{ijklm} a_{ijklm} |e_i f_j k l m\rangle. \tag{3.17}$$

one can rewrite it as

$$|\psi\rangle = \sum_{ij} |e_i f_j\rangle_{AB} |\tilde{\psi}^{(ij)}\rangle_{A'B'E}. \tag{3.18}$$

with $|\tilde{\psi}^{(ij)}\rangle_{A'B'E} = \sum_{klm} a_{ijklm} |klm\rangle$.

It is easy to see, that the scalar product $\langle\tilde{\psi}^{(ij)}|\tilde{\psi}^{(ij)}\rangle$ equals the probability of obtaining the state $|e_i f_j\rangle\langle e_i f_j|_{AB}$ on the system $AB$ after measurement in basis $\mathcal{B}$. Now, since the subsystem $\rho_{ABE}$ (after measurement in $\mathcal{B}$ on AB) must be maximally correlated, the vectors $|\tilde{\psi}^{(ij)}\rangle$ should satisfy $\langle\tilde{\psi}^{(ij)}|\tilde{\psi}^{(ij)}\rangle = \frac{1}{d}\delta_{ij}$. We can normalize these states (in case $i = j$) to have:

$$|\psi^{(ii)}\rangle := \frac{|\tilde{\psi}^{(ii)}\rangle}{\sqrt{\langle\tilde{\psi}^{(ii)}|\tilde{\psi}^{(ii)}\rangle}} = \sqrt{d}|\tilde{\psi}^{(ii)}\rangle \tag{3.19}$$

so that the total state has a form:

$$|\psi\rangle = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |e_i f_i\rangle_{AB} |\psi^{(ii)}\rangle_{A'B'E}. \tag{3.20}$$

"Cryptographical" interpretation of this state is the following: if Alice and Bob gets $i-$th result, then Eve gets subsystem $\rho_i^E$ of a state $|\psi^{(ii)}\rangle_{A'B'E}$. Indeed, its ccq state is of the form

$$\rho_{ccq} = \sum_{i=0}^{d-1} \frac{1}{d} |e_i f_i\rangle_{AB}\langle e_i f_i| \otimes \rho_i^E, \tag{3.21}$$

with $\rho_i^E = \mathrm{Tr}_{A'B'}(|\psi^{(ii)}\rangle\langle\psi^{(ii)}|_{A'B'E})$. Now the condition (3.16) implies that, $\rho_i^E$ should be all equal to each other. In particular, it follows that rank of Eve's total density matrix is no greater than dimension of $A'B'$ system, hence we can assume that $d_E = d_{A'} \times d_{B'} = d'$. Indeed: each $|\psi^{(ii)}\rangle_{A'B'E}$ has rank of subsystems $E$ and $A'B'$ equal, since it is a pure state. Denote this rank as $r_i$. By elementary algebra, we have:

$$\dim A'B' \geq rank(\rho_{A'B'}) \geq \max_j r_j \geq r_i \tag{3.22}$$

where $\rho_{A'B'} = \mathrm{Tr}_{ABE}(|\psi\rangle\langle\psi|)$. Now, since $\rho_i^E$ are equal for each $i$, they have also equal ranks $r_i = r_E$, equal to rank of the total Eve's density matrix. Then, the assertion follows from the above inequality.

It is convenient to rewrite the pure state $|\psi^{(ii)}\rangle$ in the form

$$|\psi^{(ii)}\rangle_{A'B'E} = \sum_{k=0}^{d'-1} |k\rangle_{A'B'} X_i |k\rangle_E, \tag{3.23}$$

(see discussion in Section 2.3.5), where $\{|k\rangle\}$ is standard basis of $A'B'$ and of $E$ system, $X_i$ is $d_E \times d_E$ matrix that fully represents this state. It is easy to check, that $\rho_i^E = X_i X_i^\dagger$. Consider now singular value decomposition[2] of $X_i$ given by $V_i\sqrt{\rho_i}U_i^\dagger$ where $\rho_i$ is now diagonal in basis $\{|k\rangle\}$. One then gets that $\rho_i^E = V_i\rho_i V_i^\dagger$. The state (3.23) may be also rewritten as

$$|\psi^{(ii)}\rangle_{A'B'E} = \sum_k X_i^T|k\rangle_{A'B'}|k\rangle_E, \tag{3.24}$$

where $T$ is transposition in basis $\{|k\rangle\}$. Thanks to this representation, the whole state $\rho_{ABA'B'}$ can be written as follows:

$$\rho_{ABA'B'} = \frac{1}{d}\sum_{i,j=0}^{d-1}|e_if_i\rangle\langle e_jf_j|_{AB}\otimes X_i^T(X_j^\dagger)^T. \tag{3.25}$$

We can express this state using states $\rho_j^E$, i.e. states accessible to Eve. Substituting $X_i = V_i\sqrt{\rho_i}U_i^\dagger$ we obtain

$$\rho_{ABA'B'} = \frac{1}{d}\sum_{i,j=0}^{d-1}|e_if_i\rangle\langle e_jf_j|_{AB}\otimes(U_i^*\sqrt{\rho_i}V_i^T)(V_j^*\sqrt{\rho_j}^*U_j^T). \tag{3.26}$$

We insert now the identity matrices of the form $V_i^TV_i^*$ and $V_j^TV_j^*$ respectively (note, that $V_i$ are unitary transformations, and so are the $V_i^T$), to get:

$$\rho_{ABA'B'} = \frac{1}{d}\sum_{i,j=0}^{d-1}|e_if_i\rangle\langle e_jf_j|_{AB}\otimes(U_i^*V_i^T)[V_i^*\sqrt{\rho_i}^TV_i^T][V_j^*\sqrt{\rho_j}^*V_j^T](V_j^*U_j^T).$$

Let us recall here, that $\sqrt{\rho_j}$ is positive as emerging from the singular value decomposition. Moreover it is diagonal in standard basis, hence we have $\sqrt{\rho_j}^* = \sqrt{\rho_j}^T$. This allows us to write:

$$\begin{aligned}\rho_{ABA'B'} = \frac{1}{d}\sum_{i,j=0}^{d-1}|e_if_i\rangle\langle e_jf_j|_{AB}\otimes\\ (U_i^*V_i^T)\underbrace{V_i^*\sqrt{\rho_i}^TV_i^T}_{=\sqrt{\rho_i^E}^T}\underbrace{V_j^*\sqrt{\rho_j}^TV_j^T}_{=\sqrt{\rho_j^E}^T}(V_j^*U_j^T).\end{aligned} \tag{3.27}$$

[2]For a formulation of the singular value decomposition see Section A.1.2 in Appendix.

Denoting by $W_i$ the unitary transformation $U_i^* V_i^T$ one gets:

$$\rho_{ABA'B'} = \frac{1}{d} \sum_{i,j=0}^{d-1} |e_i f_i\rangle\langle e_j f_j|_{AB} \otimes W_i \sqrt{\rho_i^E}^T \cdot \sqrt{\rho_j^E}^T W_j^\dagger.$$

However, as mentioned above, Eve's density matrices are equal to each other, i.e. $\rho_i^E = \rho_j^E \equiv \tilde{\sigma}$ for all $i, j$ where $\tilde{\sigma}$ is an arbitrary state on system E. We then obtain

$$\rho_{ABA'B'} = \frac{1}{d} \sum_{i,j=0}^{d-1} |e_i f_i\rangle\langle e_j f_j|_{AB} \otimes W_i \sigma W_j^\dagger{}_{A'B'}. \tag{3.28}$$

with $\sigma = \tilde{\sigma}^T$. This completes the proof of theorem 3.2. ∎

Owing to this characterization of quantum states that have key, we have that the notion of states that have $\mathcal{B}$-key is equivalent to the notion of private state which is secure in basis $\mathcal{B}$. In what follows, with exception of Section 3.8, we will use only the latter notion.

## 3.3 Private states as "twisted" EPR states

In this section we present the structure of private states. We show, that they consist of maximally entangled states (called also an EPR state), tensored with some arbitrary state on the $A'B'$ system, rotated (together) by a suitable unitary operation called *twisting*. We define below the notion of twisting, and show its property which proves useful in further considerations.

**Definition 3.4** *Given a product basis $\mathcal{B} = \{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1}$ of system $AB$, the unitary operation acting on system $ABA'B'$ of the form*

$$U = \sum_{k,l=0}^{d-1} |e_k f_l\rangle\langle e_k f_l|_{AB} \otimes U_{A'B'}^{kl}, \tag{3.29}$$

*is called $\mathcal{B}$-twisting, or shortly twisting.*

Using operation of $\mathcal{B}$-twisting, we can rewrite the private state of (3.8)

$$\gamma^{(d)} = \frac{1}{d} \sum_{i,j=0}^{d-1} |e_i f_i\rangle\langle e_j f_j|_{AB} \otimes U_i \sigma_{A'B'} U_j^\dagger, \tag{3.30}$$

in the following, more appealing form

$$\gamma^{(d)} = U P_{\mathcal{B}}^{(d)} \otimes \sigma_{A'B'} U^\dagger. \tag{3.31}$$

The state $P_{\mathcal{B}}^{(d)}$ has many matrix elements equal to zero. In turn, not all unitary transformations from definition of twisting are used here. In fact, unitary transformations $U_i$ in equation (3.30) are to be identified with transformations $U^{kk}$ from equation (3.29).

In special case, where private state has no shield, the twisting is in a sense trivial, i.e. it acts on $AB$ multiplying the states $|e_i f_i\rangle$ by some complex phases $e^{\phi_i}$ respectively.

Note, that we can take $\sigma_{A'B'}$ to be classically correlated (see Eq. (2.91)) in the sense that it is diagonal in some product basis. Indeed, twisting can change the state $\sigma_{A'B'}$ into any other state having the same eigenvalues (simply, twisting can incorporate a unitary transformation acting solely on $A'B'$).

It is clear now, that any private state can be viewed as maximally entangled state "twisted" into system A'B'. Thanks to this, the states which have key, are closely connected with the maximally entangled state, which has been so far a "symbol" of quantum security. As we shall see, the maximally entangled state may get twisted so much, that after measurement in many bases of the $AB$ part the outcomes will be correlated with Eve, which is not the case for the maximally entangled state itself. Still, however the basis $\mathcal{B}$ will remain secure.

### 3.3.1 Invariance of ccq state under twisting

In this section, we show that twisting does not change the ccq state of a given bipartite state. We have the following theorem.

**Theorem 3.3** *For any state $\rho_{AA'BB'}$ and any $\mathcal{B}$-twisting operation $U$, the states $\rho_{AA'BB'}$ and $\sigma_{ABA'B'} = U\rho_{AA'BB'}U^\dagger$ have the same ccq states w.r.t $\mathcal{B}$, i.e. after measurement in basis $\mathcal{B}$, the corresponding ccq states are equal: $\tilde{\rho}_{ABE} = \tilde{\sigma}_{ABE}$*

**Proof.** To show that subsystem $\rho_{ABE}$ is not affected by $\mathcal{B}$ controlled unitary with a target on $A'B'$ we will consider the whole pure state:

$$|\psi\rangle = |\psi\rangle_{ABA'B'E} = \sum_{ijklm} a_{ijklm}|ijklm\rangle \tag{3.32}$$

(without loss of generality we take $\mathcal{B}$ to be standard basis). After von Neumann measurement on $\mathcal{B}$ and tracing out the $A'B'$ part, the output state is the following:

$$\tilde{\rho}_{ABE} = \sum_{ijklmn} a_{ijklm}\bar{a}_{ijkln}|ij\rangle\langle ij| \otimes |m\rangle\langle n|. \tag{3.33}$$

Let us now subject $|\psi\rangle$ to controlled unitary $U_{ABA'B'} \otimes I_E$,

$$|\tilde{\psi}\rangle = U_{ABA'B'} \otimes I_E|\psi\rangle = \sum_{ijklm} a_{ijklm}|ij\rangle U^{ij}|kl\rangle|m\rangle, \tag{3.34}$$

and then on the output state $|\tilde{\psi}\rangle$ perform a complete measurement on $\mathcal{B}$ reading the output:

$$P_{ij}|\tilde{\psi}\rangle\langle\tilde{\psi}|P_{ij} = \sum_{klmstn} a_{ijklm}\bar{a}_{ijstn}$$
$$|ij\rangle\langle ij|_{AB} \otimes U^{ij}|kl\rangle\langle st|(U^{ij})^{\dagger}_{A'B'} \otimes |m\rangle\langle n|_E. \tag{3.35}$$

Performing partial trace and summing over $i, j$ we obtain the same density matrix as in (3.33) which ends the proof. ∎

The above theorem shows that two states which differ by some twisting $U$, have the same *ccq* state obtained by measuring their main parts, and tracing out their side parts.

### 3.3.2 Privacy squeezing

In the previous section we showed, that given a state $\rho_{ABA'B'}$, the $\mathcal{B}$-twisting does not affect its $\mathcal{B}$-ccq state. It is then interesting to ask how the whole state $\rho_{ABA'B'}$ changes when subjected to such an operation. We will show now a particularly interesting example of twisting which proves useful in further considerations.

**Remark 3.4** *In this section, as well as in Sections 3.4-3.6, we will for simplicity of notation use the standard product basis in place of $\mathcal{B}$ in definition of private state and twisting, however the results holds for an arbitrary product basis.*

**Lemma 3.5** *For any state $\sigma_{ABA'B'} \in B(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^d \otimes \mathcal{C}^{d'})$ expressed in the form $\sigma_{ABA'B'} = \sum_{ijkl=0}^{1} |ij\rangle\langle kl| \otimes A_{ijkl}$ there exists twisting $U_{ps}$ such that $\rho_{AB} = \mathrm{Tr}_{A'B'}[U_{ps}\sigma_{ABA'B'}U_{ps}^{\dagger}]$ has the form*

$$\rho_{AB} = \begin{bmatrix} \times & \times & \times & ||A_{0011}|| \\ \times & \times & \times & \times \\ \times & \times & \times & \times \\ \times & \times & \times & \times \end{bmatrix}, \tag{3.36}$$

*where $\times$ stands for non-important elements of $\rho_{AB}$.*

**Proof.** The proof is constructive. Twisting, is by definition (3.29) determined by the set of unitary transformations. As we consider pbit, we have four unitary transformations which determine it: $\{U_{kl}\}_{k,l=0}^{1}$. We take now the singular value decomposition $VR\tilde{V}$ of the operator $A_{0011}$, where $V, \tilde{V}$ are unitary transformations, and $R$ - nonnegative diagonal operator. By unitary invariance of the trace norm, we obtain $||A_{0011}|| = ||R|| = \mathrm{Tr}R$. We then define a twisting $U_\tau$ by choosing $U_{00} = V^{\dagger}$,

$U_{11} = \tilde{V}$, and $U_{01} = U_{10} = I$. The $AB$ subsystem of state $\sigma_{ABA'B'}$ twisted by $U_\tau$ reads

$$\rho_{AB} = \sum_{ijkl=0}^{1} \mathrm{Tr}(U_{ij} A_{ijkl} U_{kl}^\dagger) |ij\rangle\langle kl|. \tag{3.37}$$

Thus, by construction of $U_\tau$ we have indeed, that the element $|00\rangle\langle 11|$ of the matrix of $\rho_{AB}$ is equal to $\mathrm{Tr} U_{00}^\dagger V R \tilde{V} U_{11}^\dagger = \mathrm{Tr} R = ||A_{0011}||$, which proves the lemma. ∎

**Corollary 3.6** *Consider a state with two qubit main part, i.e. of the form (where blocks are operators acting on the side part):*

$$\sigma_{ABA'B'} = \begin{bmatrix} A_{0000} & 0 & 0 & A_{0011} \\ 0 & A_{0101} & A_{0110} & 0 \\ 0 & A_{1001} & A_{1010} & 0 \\ A_{1100} & 0 & 0 & A_{1111} \end{bmatrix}, \tag{3.38}$$

*there exists twisting such that the state after partial trace over side part (the $A'B'$ system) has a form*

$$\rho_{AB} = \begin{bmatrix} ||A_{0000}|| & 0 & 0 & ||A_{0011}|| \\ 0 & ||A_{0101}|| & ||A_{0110}|| & 0 \\ 0 & ||A_{1001}|| & ||A_{1010}|| & 0 \\ ||A_{1100}|| & 0 & 0 & ||A_{1111}|| \end{bmatrix}. \tag{3.39}$$

**Proof.** The construction of the twisting is similar as in lemma above. This time one has to consider also the singular value decomposition of the operator $A_{0110} = WSW'$. ∎

We can see now, that with any state $\rho_{ABA'B'}$, which has two qubit main part $AB$, we can associate a state obtained in the following way:

1. For state $\rho_{ABA'B'}$ find twisting $U_{ps}$, such, that (according to lemma 3.5) it changes upper-right element of $AB$ subsystem of $\rho_{ABA'B'}$ into $||A_{0011}||$.
2. Apply $U_{ps}$ to $\rho_{ABA'B'}$ obtaining $\rho'_{ABA'B'} = U_{ps} \rho_{ABA'B'} U_{ps}^\dagger$.
3. Trace out the side part ($A'B'$ subsystem) of state $\rho'_{ABA'B'}$ obtaining two-qubit state
$$\rho'_{AB} = \mathrm{Tr}_{A'B'} \rho'_{ABA'B'}. \tag{3.40}$$

This operation we will call **privacy squeezing** , or shortly **p-squeezing** , and the state $\rho'_{AB}$ which is the output of such operation on the state $\rho_{ABA'B'} \in \mathcal{B}(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^d \otimes \mathcal{C}^{d'})$ the *p-squeezed state of* the state $\rho_{ABA'B'}$.

The operation analogous to privacy squeezing with some twisting $U \neq U_{ps}$ in place of $U_{ps}$ we call the **approximate privacy squeezing**, when it is optimal enough for our purpose. E.g. when the twisting $U$ makes the main part close to maximally entangled state.

In Chapter 4, Theorem 4.25, we prove, that the ccq state of p-squeezed state denoted as $[\rho^{ps}]^{ccq}$ has no more secret correlations than that of the original state. The intuition behind is as follows: it emerges from the operation of twisting which preserves security in some sense, i.e. it does not change the ccq state which can be obtained from the original state (see Theorem 3.3). The next operation performed in definition of p-squeezed state is tracing out $A'B'$ part which means giving the $A'B'$ subsystem to Eve. Such operation can not increase security of the state (see Theorem 4.4).

We will be interested in applying p-squeezing in the case, where the main part of the initial state was weakly entangled, or completely separable. Then the p-squeezing operation will make it entangled.

We can say, that the operation of privacy squeezing pumps the entanglement of the state which is distributed along subsystems $AA'BB'$ into its main part $AB$. The entanglement once concentrated in the two qubit part, may be much more powerful than the one spread over the whole system. Further in the manuscript, we will see that from the bound entangled state, the operation of p-squeezing can produce approximately a maximally entangled state of two qubits. Then the analysis of how much key one can draw from the ccq state is much easier in case of the p-squeezed states.

## 3.4 Private bits - representations

In this section we will present various forms of pdits and pbits. We will first write the pbit in matrix form according to its original definition. We can write it in block form

$$\gamma^{(2)}_{ABA'B'} = \frac{1}{2}\begin{bmatrix} U_0\sigma_{A'B'}U_0^\dagger & 0 & 0 & U_0\sigma_{A'B'}U_1^\dagger \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ U_1\sigma_{A'B'}U_0^\dagger & 0 & 0 & U_1\sigma_{A'B'}U_1^\dagger \end{bmatrix}, \tag{3.41}$$

where $\sigma_{A'B'}$ is arbitrary state on $A'B'$ subsystem, and $U_0$ and $U_1$ are arbitrary unitary transformations which act on $A'B'$.

### 3.4.1 "Generalized EPR form" of pdit

Since by Theorem 3.2 pdits are the only states that contain $\mathcal{B}$-key, they could be called generalized EPR states (maximally entangled state). We have seen in Section 3.3 that they can be viewed as "twisted EPR states". One can notice an even closer connection. Namely, a pdit can be viewed as an *EPR states with operator amplitudes*. Indeed, one can rewrite equation (3.25) in a more appealing form

$$\gamma^{(d)}_{A'B'AB} = \Psi\Psi^\dagger, \tag{3.42}$$

with

$$\Psi = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} Y_i \otimes |e_i f_i\rangle. \tag{3.43}$$

We have written here (unlike in the rest the of the manuscript) first the $A'B'$ system and then the $AB$ one, so that this form of pdit would recall a form of pure state. Thus instead of complex numbers the amplitudes are now operators. Thus if $d = 2$, the matrix form of $\gamma^{(d)}_{A'B'AB}$ is the following:

$$\gamma^{(2)}_{ABA'B'} = \frac{1}{2} \begin{bmatrix} Y_0Y_0^\dagger & 0 & 0 & Y_0Y_1^\dagger \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ Y_1Y_0^\dagger & 0 & 0 & Y_1Y_1^\dagger \end{bmatrix}. \tag{3.44}$$

Let us consider the polar decomposition of operators $Y_i$. From definition of pdit it follows that

$$Y_i = U_i\sqrt{\rho}, \tag{3.45}$$

where $U_i$ is unitary transformation and $\rho$ is a normalized state as so is the $\sigma_{A'B'}$ state in form (3.41). This reflects the fact, that pbit, like maximally entangled state of two qubits has coefficients which can have different phase, but the same amplitudes.

There is yet another similarity to EPR states, namely the norm of upper-right block $Y_0Y_1^\dagger$ is equal to $\frac{1}{2}$, like the modulus of the coherence of the EPR state.

### 3.4.2 "$X$-form" of pbit

In special case of pbits (d=2) one can have representation by just one normalized operator:

$$\gamma^{(2)}_{ABA'B'} = \frac{1}{2} \begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sqrt{X^\dagger X} \end{bmatrix}, \tag{3.46}$$

for any operator $X$ satisfying $||X|| = 1$. If the normalization term $\frac{1}{2}$ is included in the operator $X$ we will say, that the pbit is in *normalized $X$-form*, and consequently $||X|| = \frac{1}{2}$.

Justification of equivalence of this form and standard form is the following. To see that the state (3.46) is a pbit consider singular value decomposition $U\sigma W$ of $X$, with $U$ and $W$ unitary transformations and $\sigma$ being diagonal, positive matrix. Since $X$ has trace norm 1, the same is for $\sigma$ (trace norm is unitarily invariant - see Section A.1.1 of Appendix). Therefore $X$ can be viewed as $X = U\rho W$ with $\rho$ being a legitimate state. Identifying $U_0 = U$ and $U_1 = W^\dagger$ we obtain the standard form.

Conversely, any pbit can be presented in $X$-form, with $X = Y_0 Y_1^\dagger$, with $Y_i$ satisfying equation (3.45). We have for example:

$$\sqrt{Y_0 Y_1^\dagger (Y_0 Y_1^\dagger)^\dagger} = \sqrt{Y_0 Y_1^\dagger Y_1 Y_0^\dagger} = \sqrt{U_0 \sqrt{\rho}\sqrt{\rho} U_1^\dagger U_1 \sqrt{\rho}\sqrt{\rho} U_0^\dagger} = \sqrt{U_0 \rho^2 U_0^\dagger} = Y_0 Y_0^\dagger \tag{3.47}$$

It is important, that in nontrivial cases $X$ should be non-positive operator. Otherwise the pbit is equal to basic pbit. Indeed, if it is positive, then since its trace norm is 1, it is itself legitimate state, call it $\rho$. Then $\sqrt{XX^\dagger} = \sqrt{X^\dagger X} = \rho$, so that

$$\rho_{ABA'B'} = \frac{1}{2} \sum_{i,j=0}^{1} |ii\rangle\langle jj| \otimes \rho = |\phi_+\rangle\langle\phi_+| \otimes \rho,$$

which is a basic pbit (3.10).

In higher dimension to have the $X$-form we need more than one operator, and the operators depend on each other, which is not as simple representation as in case of pbit. For example in $d = 3$ case we have:

$$\gamma^{(3)}_{ABA'B'} = \frac{1}{3} \begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & 0 & X & 0 & 0 & 0 & XY \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & 0 & \sqrt{X^\dagger X} & 0 & 0 & 0 & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ (XY)^\dagger & 0 & 0 & 0 & Y^\dagger & 0 & 0 & 0 & \sqrt{Y^\dagger Y} \end{bmatrix},$$

where the operators $X$ and $Y$ satisfy: $||X|| = 1$ and $X = WY^\dagger$ for arbitrary unitary transformation $W$.

**"Flags form": special case of $X$-form**

If the operator $X$ which represents pbit in $X$-form is hermitian, the pbit can be seen as a mixture of two basic pbits :

$$\gamma^{(2)}_{ABA'B'} = p|\phi^+\rangle\langle\phi^+| \otimes \rho^+_{A'B'} + (1-p)|\phi^-\rangle\langle\phi^-| \otimes \rho^-_{A'B'}, \tag{3.48}$$

where $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$. Derivation of this form is straightforward, if we consider decomposition of X into positive and negative part[3]:

$$X = X_+ - X_-, \tag{3.49}$$

where $X_+$ and $X_-$ are by definition orthogonal, and positive. Thus denoting $p = \mathrm{Tr}X_+$, together with assumption of $X$-form that $||X|| = \mathrm{Tr}|X| = 1$, we can rewrite $X$ as

$$X = p\rho_+ - (1-p)\rho_-, \tag{3.50}$$

where $\rho_\pm$ are normalized positive and negative parts of $X$. Moreover, since the states $\rho_+$ and $\rho_-$ are orthogonal: $\mathrm{Tr}\rho_-\rho_+ = 0$, we obtain the form (3.48).

### 3.4.3 Private bits - examples

We will give now two examples of private bits, and study its entanglement distillation properties.

1. Let us consider state $\gamma^V \in B(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^d \otimes \mathcal{C}^d)$ of the following form:

$$\gamma^V = \frac{1}{2}\begin{bmatrix} \frac{\mathrm{I}}{d^2} & 0 & 0 & \frac{V}{d^2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{V}{d^2} & 0 & 0 & \frac{\mathrm{I}}{d^2} \end{bmatrix}, \tag{3.51}$$

   where $V$ is the swap unitary transformation: $V = \sum_{i,j=0}^{d-1} |ij\rangle\langle ji|$. It is easy to check, that $\gamma^V$ is a pbit in $X$-form with $X = \frac{V}{d^2}$. Indeed, since trace norm is unitarily invariant (see A.1.1), we have: $||\frac{V}{d^2}|| = ||\frac{V}{d^2}V|| = ||\frac{\mathrm{I}}{d^2}|| = 1$.

   Since $X$ is hermitian, we can represent $\gamma^V$ in"flags form". Considering the positive and negative part of $V$, we observe that:

$$\gamma^V = p|\phi^+\rangle\langle\phi^+| \otimes \rho_s + (1-p)|\phi^-\rangle\langle\phi^-| \otimes \rho_a, \tag{3.52}$$

[3]The positive part of the hermitian operator $X$ is the operator $X_+$ build out of $X$ by setting its negative eigenvalues to zero. The negative part of $X$ is the operator $X_-$ build out of $X$ by setting nonnegative eigenvalues to zero and taking modulus of such obtained operator [Bha97].

where

$$\rho_s = \frac{2}{d^2+d} P_{sym} \quad \rho_a = \frac{2}{d^2-d} P_{asym}, \tag{3.53}$$

are so called symmetric and antisymmetric Werner states i.e. normalized projectors $P_{sym} = \frac{1}{2}(\mathrm{I}+V)$ and $P_{asym} = \frac{1}{2}(\mathrm{I}-V)$ onto symmetric and antisymmetric space respectively [Wer89]. The probability of mixing equals $p = \frac{1}{2}(1+\frac{1}{d})$. Since these Werner states are orthogonal, they correspond to "flag" states $\rho^{+}_{A'B'}$ and $\rho^{-}_{A'B'}$ from Eq. 3.48 respectively.

2. The second example is the state known as "flower state", which was shown [HHHO05b] to lock entanglement cost (we discuss this phenomenon in Section 3.5.2). We have that $\gamma^{(2,d)}_{flower} \in B(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^{d^2} \otimes \mathcal{C}^{d^2})$ is of the form:

$$\gamma^{(2,d)}_{flower} = \frac{1}{2} \begin{bmatrix} \sigma & 0 & 0 & \frac{1}{d}U^T \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{d}U^* & 0 & 0 & \sigma \end{bmatrix}, \tag{3.54}$$

where $\sigma$ is classical maximally correlated state: $\sigma = \sum_{i=0}^{d-1} \frac{1}{d}|ii\rangle\langle ii|$, and $U$ is the embedding of unitary transformation $W = \sum_{i,j=0}^{d-1} w_{ij}|i\rangle\langle j| = H^{\otimes \log d}$ with $H$ being Hadamard transformation (see Eq. (2.15)) in the following way:

$$U = \sum_{i,j=0}^{d-1} w_{ij}|ii\rangle\langle jj|.$$

This state is a pbit in $X$-form. In this case $X = U^T$. To see this consider unitary transformation $S := U^* + \sum_{i \neq j} |ij\rangle\langle ij|$. Composing $S$ with $U^T$ does not change the norm, which is unitarily invariant (see Section A.1.1 of Appendix), so that

$$||\frac{1}{d}U^T|| = ||\frac{1}{d}U^T S|| = ||\frac{1}{d}\sum_{i=0}^{d-1}|ii\rangle\langle ii||| = 1. \tag{3.55}$$

Thus we see, that $||X|| = 1$. We have also $\sqrt{XX^\dagger} = \sigma$:

$$\sqrt{\frac{1}{d^2}U^T U^*} = [\frac{1}{d^2}\sum_{i=0}^{d-1}|ii\rangle\langle ii|]^{\frac{1}{2}} = \sigma. \tag{3.56}$$

## 3.5 On entanglement properties of private states and locking entanglement measures

In this section we will show some entanglement properties of the private bits presented in previous section. To this end we use here the notion of *distillable key* $K_D$, introduced in next chapter. We first show the gap between distillable entanglement and distillable key for some pbits. Further we study the change of some entanglement measures under tracing out a qubit from the key part system. This contributes to the effect of *locking of entanglement measure*. Informally speaking, an entanglement measure $E$ is called *lockable* if evaluated on some state $\rho_{AA'B}$, it can decrease by a lot after tracing out (or in general a quantum operation on) a system $A$ of small dimensionality in comparison with the change of $E$. In this section, we will show that for the family of private states (3.54), the $E_N$, $E_C$ (and $E_f$) are lockable in this sense. In Section 3.5.3 we show also that $E_r$ is not lockable, and use this fact to give a bound on $E_r$ for private states.

### 3.5.1 Log negativity of some private states, and the gap between $E_D$ and $K_D$

The formal definition of the amount of security contained in bipartite quantum state, called *distillable key* ($K_D$) is given in Section 4.1. It is argued also in Section 4.4, that $K_D$ is an entanglement measure. It is then tempting to compare its value to other entanglement measures. In this section, we show that in case of $\gamma^V$ given in Eq. (3.51), the distillable entanglement $E_D$ is strictly smaller then the amount of secure key $K_D$ gained from these states. To this end we will compute the log-negativity $E_N(\rho)$ of the state, which is an upper bound on $E_D$ [VW02] (see Section 2.8.4).

**Lemma 3.7** *For any pbit $\gamma_{ABA'B'}$ in $X$-form, if $\sqrt{XX^\dagger}^\Gamma \geq 0$ and $\sqrt{X^\dagger X}^\Gamma \geq 0$, its log negativity satisfies $E_N(\gamma_{ABA'B'}) = \log(1 + ||X^\Gamma||)$, where $\Gamma$ is transposition performed on the system $B'$.*

**Proof.** Due to example 2.16 (see Section 2.4.2), the pbit $\gamma$ in $X$-form after partial transposition on $BB'$ subsystem changes into

$$\gamma^\Gamma_{ABA'B'} = \frac{1}{2}\begin{bmatrix} \sqrt{XX^\dagger}^\Gamma & 0 & 0 & 0 \\ 0 & 0 & X^\Gamma & 0 \\ 0 & (X^\dagger)^\Gamma & 0 & 0 \\ 0 & 0 & 0 & \sqrt{X^\dagger X}^\Gamma \end{bmatrix}. \tag{3.57}$$

We have

$$||\gamma^\Gamma|| = \frac{1}{2}(||[\sqrt{XX^\dagger}]^\Gamma|| + ||[\sqrt{X^\dagger X}]^\Gamma|| + ||A||), \tag{3.58}$$

where

$$A = \begin{bmatrix} 0 & (X)^\Gamma \\ (X^\dagger)^\Gamma & 0 \end{bmatrix}. \tag{3.59}$$

The operators $[XX^\dagger]^\Gamma$ and $[X^\dagger X]^\Gamma$ are positive, so that

$$||[\sqrt{XX^\dagger}]^\Gamma|| + ||[\sqrt{X^\dagger X}]^\Gamma|| = \mathrm{Tr}(\sqrt{XX^\dagger} + \sqrt{X^\dagger X})^\Gamma = 2\mathrm{Tr}\gamma^\Gamma = 2. \tag{3.60}$$

The last equality comes from the fact that $\Gamma$ preserves trace. To evaluate norm of $A$, we note that due to unitary invariance of trace norm we have $||A|| = ||\sigma_1 \otimes \mathrm{I}_{A'B'} A||$, with $\sigma_1^{AB}$ being a corresponding Pauli operation given in Eq. (2.50), that acts on system $AB$. Consequently

$$||A|| = ||X^\Gamma|| + ||(X^\dagger)^\Gamma|| = 2||X^\Gamma||. \tag{3.61}$$

The last equality follows form the fact that $\Gamma$ commutes with Hermitian conjugation, and trace norm is invariant under Hermitian conjugation $||X|| = ||X^\dagger||$. The log-negativity entanglement measure is defined as $E_N(\rho) = \log(||\rho^\Gamma||)$, thus we get

$$E_N(\gamma) = \log(1 + ||X^\Gamma||), \tag{3.62}$$

which proves the lemma.∎

Using the above lemma, one can check the negativity of the state $\gamma^V$. We have in this case $X = \frac{V}{d^2}$, with $d \geq 2$. Since $V^\Gamma = dP_+^{(d)}$, we obtain $E_N(\gamma^V) = \log(1 + \frac{1}{d})$. It implies:

$$E_D(\gamma^V) \leq E_N(\gamma^V) = \log(1 + \frac{1}{d}) < 1 \leq K_D(\gamma^V), \tag{3.63}$$

which demonstrates a desired gap between distillable key and distillable entanglement:

$$E_D(\gamma^V) < K_D(\gamma^V). \tag{3.64}$$

### 3.5.2 Locking of $E_N$, $E_c$ and $E_f$ with private states

Before we invoke a formal definition of locking of an entanglement measure, it is instructive to present details of the result from which locking of entanglement originates.

#### unlocking classical correlations

In [DHL$^+$04], it is shown, that a measure of classical correlations denoted as $I_c$ can increase arbitrarily after sending a single bit of information. More precisely, consider

the following family of states:

$$\rho^{cl}_{aAB} = \frac{1}{2}\left[|0\rangle\langle 0|_a \otimes \left(\sum_{i=0}^{d-1}\frac{1}{d}|i\rangle\langle i|_A \otimes |i\rangle\langle i|_B\right) + |1\rangle\langle 1|_a \otimes \left(|i\rangle\langle i|_A \otimes W|i\rangle\langle i|_B W^\dagger\right)\right], \tag{3.65}$$

with $W = \sum_{k,l=0}^{d-1} w_{kl}|k\rangle\langle l|$ being any unimodular matrix i.e. satisfying $|w_{kl}| = \frac{1}{\sqrt{d}}$. Exemplary can be $W = \sum_{kl}\frac{1}{\sqrt{d}}e^{\frac{1}{d}2\pi i(kl)modd}|k\rangle\langle l|$ [Wer01]. The classical correlations measure $I_c$ is defined in [DHL$^+$04] as follows:

$$I_c(\rho_{AB}) = max_{M_A\otimes M_B} I(A:B), \tag{3.66}$$

where maximum is taken over POVMs $\{M_A^{(i)}\}_{i=0}^{K_A-1}$ and $\{M_B^{(i)}\}_{i=0}^{K_B-1}$on Alice's and Bob's subsystem respectively, with $I(A:B)$ begin the mutual information of the random variable of pairs of outcomes of these POVMs:

$$P(A=i, B=j) = TrM_A^{(i)} \otimes M_B^{(j)}\rho_{AB}. \tag{3.67}$$

It is shown in [DHL$^+$04], that $I_c(\rho^{cl}_{aAB}) \leq \frac{1}{2}\log d$, but after communication of a single bit (a state of system $a$) from Alice to Bob, $I_c$ increases to $\log d$. This result can be seen as 'unlocking' of classical correlations, since system $a$ can be seen as a 'lock' to the quantity $I_c$, on the state. The properties of $I_c$ on the state $\rho^{cl}_{aAB}$ are collected in the following theorem:

**Theorem 3.8** *(compare [DHL$^+$04]) For the state $\rho^{cl}_{aAB}$ defined by (3.65), there holds:*

1. $I_c(\rho^{cl}_{aAB}) \leq \frac{1}{2}\log d$
2. $I_c(\rho^{cl}_{aAB}) = \sup_{\Lambda_B}\chi(\{(p_i, \rho^{(i)}_{aA})\})$, *where $\rho^{(i)}_{aA}$, are states on Alices's site which appears conditionally upon classical outcome $|i\rangle\langle i|$ of the quantum measurement $\Lambda_B = \{B_i \otimes |i\rangle\}$ on system $B$ (see (2.96)).*
3. $I_c(\rho^{cl}_{ABb}) = \log d$, *where $\rho^{cl}_{ABb}$ is $\rho^{cl}_{aAB}$ with system $a$ on Bob's site labelled as $b$.*
4. $I_c((\rho^{cl}_{aAB})^{\otimes n}) = nI_c(\rho^{cl}_{aAB})$

### Locking of $E_C$ and $E_N$ with pbits

We first provide precise definition of lockability. The effect of locking of entanglement measures described in [HHHO05b], via examples, was formalized in [Chr06] by means of the converse property, with an acronym Non Lock:

**Definition 3.5** *[Chr06] An entanglement measure $E$ is said to be nonlockable (has Non Lock property), if there is $c \geq 0$ such that for all $\rho_{aAB}$,*

$$E(\rho_{aAB}) \leq E(\rho_{AB}) + c \log Rank(\rho_a), \tag{3.68}$$

*where $\rho_{AB} = \mathrm{Tr}_a \rho_{aAB}$.*

According to the above definition, $E$ is *lockable* (has Lock property), if there is a family of states $\{\rho^c_{aAB}\}$ with increasing parameter $c$, such that $E(\rho^c_{aAB}) - E(\rho^c_{AB}) > c \log Rank(\rho_a)$. If the difference $E(\rho^c_{aAB}) - E(\rho^c_{AB})$ is explicit function of $c$, we will say, that E is $(\kappa \downarrow \Delta)$ − Tr-lockable, with $\kappa = \log Rank(\rho_a)$ and $\Delta(c) = E(\rho^c_{aAB}) - E(\rho^c_{AB})$. We then say also, that family $\{\rho^c_{aAB}\}$ reveals $(\kappa \downarrow \Delta)$ − Tr-lockability of $E$.

We can pass now to show, that the family of flower states $\{\gamma^{(2,d)}_{flower}\}^{\infty}_{d=2}$ introduced in (3.54) reveals lockability of $E_C$. We have already argued, that these states are pbits in $X$-form, defined as:

$$\gamma^{(2,d)}_{flower} = \frac{1}{2} \begin{bmatrix} \sigma & 0 & 0 & \frac{1}{d}U^T \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{d}U^* & 0 & 0 & \sigma \end{bmatrix}, \tag{3.69}$$

where $\sigma$ is classical maximally correlated state: $\sigma = \sum_{i=0}^{d-1} \frac{1}{d} |ii\rangle\langle ii|$, and $U$ is an embedding of a unimodular unitary transformation $W = \sum_{i,j=0}^{d-1} w_{ij} |i\rangle\langle j|$, in the following way:

$$U = \sum_{i,j=0}^{d-1} w_{ij} |ii\rangle\langle jj|. \tag{3.70}$$

(To be precise, in (3.54) we considered $W = H^{\otimes \log d}$, but this can be extended to unimodular unitary transformations in context we are going to present). One can see the connection between this state and the state $\rho^{cl}_{aAB}$ which reveals 'unlocking' of $I_c$ (3.65). We make this connection explicit now. Consider a purification $|\psi_\gamma\rangle_{ABA'B'E}$ of the state $\gamma^{(2,d)}_{flower}$ of systems $ABA'B'$ to system $E$. It is straightforward to check, that:

$$\mathrm{Tr}_{AA'} |\psi_\gamma\rangle\langle\psi_\gamma|_{ABA'B'E} = \rho^{cl}_{BB'E}, \tag{3.71}$$

where in (3.65) one identifies $a$, $A$ and $B$ with $B$, $B'$ and $E$ respectively.

We are ready to formulate the main theorem of this section:

**Theorem 3.9** *The family of private states $\{\gamma^{(2,d)}_{flower}\}^{\infty}_{d=2}$ reveals $(1 \downarrow \frac{1}{2}\log d)$ − Tr-lockability of $E_C$.*

**Proof.** Due to the so called duality relation [KW04], for any pure tripartite state $|\psi\rangle_{ABE}$, one can reformulate the entanglement of formation $E_f$ of its bipartite subsystem $AB$, as a function of subsystem $BE$: the difference between entropy of Bob's

system and maximal Holevo quantity of the ensamble of Bob's matrix obtained after measurement on system $E$ and communicating the classical results to system $B$. Precisely we have:

$$E_f(\rho_{AB}) = S(B)_{|\psi\rangle_{ABE}} - \sup_{\Lambda_E} \chi_{BE} \tag{3.72}$$

with $\sup_{\Lambda_E} \chi_{BE} = \sup_{\Lambda_E} \chi(\{(p_i, \rho_B^{(i)})\})$, where $\rho_B^{(i)}$, are states on Bob's site which appears conditionally on the classical outcome $|i\rangle\langle i|$ of a quantum measurement $\Lambda_E$ with some Krause operators $E_i \otimes |i\rangle$ on system $E$ (see (2.96)).

In particular, we have:

$$E_f(\gamma_{flower}^{(2,d)}) = S(BB')_{|\psi_\gamma\rangle_{ABA'B'E}} - \sup_{\Lambda_E} \chi_{BB'E}. \tag{3.73}$$

where $|\psi_\gamma\rangle_{ABA'B'E}$ is a purification of $\gamma_{flower}^{(2,d)}$ on systems ABA'B' to system $E$. As it follows from Eq. (3.71), the subsystem $BB'E$ of $|\psi_\rho\rangle_{ABA'B'E}$ equals just $\rho_{BB'E}^{cl}$.

We will employ now the properties of $I_c(\rho_{BB'E}^{cl})$, given in Theorem 3.8, providing the change of labels $a \to B$, $A \to B'$, $B \to E$ and $b \to e$, respectively.

By properties (2) and (4), and due to the fact that $E_C = E_f^\infty$ (see (2.113) Section 2.8.2), the equality (3.73) reads:

$$E_C(\gamma_{flower}^{(2,d)}) = S(BB')_{|\psi_\gamma\rangle_{ABA'B'E}} - I_c(\rho_{BB'E}^{cl}). \tag{3.74}$$

Let us now trace out system $B$ (a single qubit) of the purification $|\psi_\gamma\rangle_{ABA'B'E}$, and purify the resulting state on system $e$, on Eve's site, obtaining new pure state $|\tilde{\psi}\rangle_{AA'B'Ee}$. Applying duality relation (3.72), to $|\tilde{\psi}\rangle_{AA'B'Ee}$ one gets:

$$E_C(\tilde{\gamma}_{flower}^{(2,d)}) = S(B')_{|\tilde{\psi}\rangle_{AA'B'Ee}} - I_c(\tilde{\rho}_{B'Ee}^{cl}), \tag{3.75}$$

where $\tilde{\gamma}_{flower}^{(2,d)}$ is the flower state after tracing out system $B$ and $\tilde{\rho}_{B'Ee}^{cl}$ is just a state $\tilde{\rho}_{BB'E}^{cl}$ with system $B$ on Eve's site, labelled by e. We have used here the fact, that $I_c((\tilde{\rho}_{B'Ee}^{cl})^{\otimes n}) = nI_c(\tilde{\rho}_{B'Ee}^{cl})$. This fact holds for the same reason as property (4).

We check now, how the values of $E_C$ and $I_c$ change in parallel: in (3.74) we had $I_c(\rho_{BB'E}^{cl}) \leq \frac{1}{2}\log d$ (by property (1)) and $S(BB') = 1 + \log d$, hence $E_C(\gamma_{flower}^{(2,d)}) \geq 1 + \frac{1}{2}\log d$. Passing[4] to (3.75), due to property (3), there is $I_c(\tilde{\rho}_{B'Ee}^{cl}) = \log d$. Since entropy of system $B'$ equals just $\log d$, we have that $E_C(\tilde{\rho}_{B'Ee}^{cl}) = 0$.

Hence, after tracing out a single qubit (system $B$) of $\gamma_{flower}^{(2,d)}$, $E_C$ has decreased from $1 + \frac{1}{2}\log d$ to zero. This ends the proof of Theorem 3.9. ∎

Since $E_C = E_f^\infty$, the above theorem proves also that $E_f$ has Lock property.

We now state the result for locking of $E_N$, again revealed by the flower states.

[4] In [CW05] it is argued, that in fact $E_C(\gamma_{flower}^{(2,d)}) = 1 + \frac{1}{2}\log d$ in this case.

**Theorem 3.10** *The family of private states* $\{\rho^{(d)}_{flower}\}$ *is* $(1 \downarrow \log(\sqrt{d}+1)) -$ Tr*-lockability of* $E_N$*.*

**Proof.** By Lemma 3.7 $E_N(\rho^{(d)}_{flower}) = \log(1+||\frac{1}{d}(U^T)^\Gamma||)$, where $U = \sum_{ij} w_{ij}|ii\rangle\langle jj|$ with $W$ a unimodular unitary transformation. Repeating analogous considerations to that given in example 3.54, we get that it equals $\log(1+\sqrt{d})$. If we however trace out one qubit of the key part of the private state $\rho^{(d)}_{flower}$, we obtain a separable state, with $E_N = 0$. ∎

### 3.5.3 Nonlockability of $E_r$ and the upper bound on $K_D$ for private states

We now consider entanglement contents of a pbit in terms of the measure of entanglement called relative entropy of entanglement (see Section 2.8.3). In Section 4.5 we will show, that for *any* state, the relative entropy of entanglement is an upper bound on distillable key, which is the amount of secure key $K_D$, that can be distilled from many copies of the state via LOCC operations (see Def. 4.1 for details). It is then easy to see, that for any pbit $\gamma$, its relative entropy of entanglement $E_r(\gamma)$ is greater than $\log d$ since $K_D(\gamma) \geq \log d$ by definition of pdits. The question we address here, is an upper bound on the relative entropy of the pdit. We relate its value to the states which appear on the shield of the pdits, when Alice and Bob get key by measuring the key part of the pdit. To show this in a short way we first provide a general fact, that $E_r$ is not lockable.

#### $E_r$ is not lockable

We provide in this section a proposition from which it follows easily that $E_r$ has property Non Lock.

**Proposition 3.11** *For any bipartite state* $\rho_{AA':B} \equiv \rho$ *and any complete von Neumann measurement* $\Lambda_A$ *on the one qubit system* $A$ *there holds:*

$$E_r(\rho) - E_r(\Lambda_A \otimes \mathrm{I}_{A'B}(\rho)) \leq 1 \tag{3.76}$$

$$E_r(\rho) - E_r(\mathrm{Tr}_A(\rho)) \leq 2. \tag{3.77}$$

**Proof.** Both statements of this theorem are consequence of the following property of relative entropy of entanglement [LPSW99] (see [EFP$^+$00] in this context):

$$\sum_i p_i E_r(\rho_i) - E_r(\sum_i p_i\rho_i) \leq S(\sum_i p_i\rho_i) - \sum_i p_i S(\rho_i) \tag{3.78}$$

where $S$ stands for the von Neumann entropy of the state.

For the first part of the proof, it suffices to notice that any complete von Neumann measurement can be implemented via applying randomly some unitary transformations. Consider the following basic quantum operations: add on Alice's site an ancillary system in state $\tau = \frac{1}{2}[|0\rangle\langle 0| + |1\rangle\langle 1|]$ and perform the controlled unitary operation $U = \sum_{i=0}^{1} |i\rangle\langle i|_{anc} \otimes \sigma_A^{(i)}$ with $\sigma^{(0)} = \mathrm{I}_A$ and $\sigma^{(1)} = \sigma_2$ - a Pauli operation (see Eq. (2.50). This operation followed by tracing out the ancilla $\tau$ will have the desired effect:

$$Tr_{anc}[U(\tau \otimes \rho)U^{\dagger}] = \sum_i \tilde{p}_i \tilde{\rho}_i = \Lambda_A \otimes \mathrm{I}_{A'B}(\rho) \tag{3.79}$$

where $\tilde{\rho}_i = \sigma_i \otimes \mathrm{I}_{A'B}(\rho)$ and $p_i = \frac{1}{2}$. Taking now in (3.78) $\rho_i = \tilde{\rho}_i$ and $p_i = \tilde{p}_i$, one gets:

$$E_r(\rho) - E_r(\sum_i p_i \rho_i) \leq S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i), \tag{3.80}$$

since local unitary transformations do not change $E_r$ (see Lemma 2.27). By (3.79) it is equivalent to:

$$E_r(\rho) - E_r(\Lambda_A \otimes \mathrm{I}_{A'B}(\rho)) \leq S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i) \leq H(\vec{p}), \tag{3.81}$$

where last inequality follows from (2.97) with $H(\vec{p})$ being the Shannon entropy of the distribution $\vec{p}$ defined by probabilities $p_i$. For our choice of $p_i$ this gives: $S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i) \leq 1$ which proves (3.76).

The property (3.77) can be proved in similar vain. Instead of tracing out, we apply 'total' dephasing, which is equivalent to transformation of $\rho_{AA'B}$ into $\frac{\mathrm{I}}{2} \otimes \rho_{A'B}$. To this end we a need bigger ancilla system in state $\tau^{\otimes 2}$ and the controlled unitary composed from all four Pauli operations (Eq. (2.50): $U = \sum_{i=0}^{3} |i\rangle\langle i|_{anc} \otimes \sigma_A^{(i)}$. The unitary transformations $\sigma^{(i)}$ are well known examples of the ones which applied randomly change any state of 1-qubit system into the maximally mixed state (see for example, [BR03, MTd00]). ∎

The above Proposition can be generalized as follows:

**Corollary 3.12** *For any $\rho_{AA'B} \in \mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B$, such that $\dim \mathcal{H}_A = d$, and any complete von Neumann measurement $\Lambda_A$ on the system $A$ there holds:*

$$E_r(\rho) - E_r(\Lambda_A \otimes \mathrm{I}_{A'B}(\rho)) \leq \log d \tag{3.82}$$

$$E_r(\rho) - E_r(\mathrm{Tr}_A(\rho)) \leq 2 \log d. \tag{3.83}$$

**Proof.** It follows the same arguments as Proposition 3.11, with Pauli transformations replaced by appropriate groups of unitary transformations. In (3.82) one uses a special set of unimodular matrices, $\{WS_jW^\dagger\}_{j=0}^{d-1}$ with $W = \sum_{kl} \frac{1}{\sqrt{d}} e^{\frac{1}{d}2\pi i(kl)modd} |k\rangle\langle l|$, $S_j = \sum_{k=0}^{d-1} |(k+j)\text{mod d}\rangle\langle k|$ is the shift operation (see [Chr06]). In (3.83) one uses the group of unitary transformations which turns any state into the maximally mixed state on $\mathcal{H}_{A'}$ [Wer01]. ∎

Obviously, Proposition 3.11 and the above corollary hold as well for the regularized relative entropy of entanglement: $E_r^\infty = \lim_{n\to\infty} \frac{E_r(\rho^{\otimes n})}{n}$.

**Upper bound on relative entropy of entanglement of private states.**

Having shown how $E_r$ behaves after von Neumann measurement, we are ready to prove the following theorem:

**Theorem 3.13** *For any pdit $\gamma_{ABA'B'} \in \mathcal{B}(\mathcal{C}^d \otimes \mathcal{C}^d \otimes \mathcal{C}^{d'_A} \otimes \mathcal{C}^{d'_B})$, written in a form $\gamma_{ABA'B'} = \sum_{i,j=0}^{d-1} |ij\rangle\langle ij| \otimes U_i \rho_{A'B'} U_j^\dagger$, we have*

$$E_r(\gamma_{ABA'B'}) \leq \log d + \frac{1}{d} \sum_{i=0}^{d-1} E_r(\rho^{(i)}_{A'B'}) \tag{3.84}$$

*where $\rho^{(i)}_{A'B'} = U_i \rho_{A'B'} U_i^\dagger$.*
**Proof.** From Corollary 3.12, we have that:

$$E_r(\gamma_{ABA'B'}) - E_r(\gamma^{meas}_{ABA'B'}) \leq \log d \tag{3.85}$$

with $\gamma^{meas}_{ABA'B'} = \sum_{j=0}^{d-1} \frac{1}{d} |jj\rangle\langle jj|_{AB} \otimes \rho^{(j)}_{A'B'}$ being $\gamma_{ABA'B'}$ measured by complete von Neumann measurement in standard basis on system $AB$. By convexity of the relative entropy of entanglement, we have:

$$E_r(\gamma_{ABA'B'}) - \sum_{j=0}^{d-1} \frac{1}{d} E_r(|jj\rangle\langle jj|_{AB} \otimes \rho^{(j)}_{A'B'}) \leq \log d. \tag{3.86}$$

This, providing the fact that $E_r(|jj\rangle\langle jj|_{AB} \otimes \rho^{(j)}) = E_r(\rho^{(j)})$, which is clearly true for any entanglement measure, proves the thesis. ∎

**Remark 3.14** *An analogous theorem to the above holds for $E_r^\infty$ in place of $E_r$, the proof of which can be found in [HHHO05a].*

## 3.6 Irreducible private states - units of privacy

In Section 3.2 we have characterized states which contain ideal key, called pdits. A pdit has $AB$ subsystem called here the key part. The amount of $\log d$ of key can be obtained from such pdit by just complete measurement in some basis performed on this key part of pdit . However, as it follows from characterization given in Theorem 3.2, pdits have also the $A'B'$ subsystem, called here the shield. This part can also serve as a source of key. Indeed there are plenty of such pdits that contain more than $\log d$ key, due to their shield. Therefore not every pdit can serve as a unit of privacy and we need the following definition:

**Definition 3.6** *Any pdit $\gamma$ (with $d$-dimensional key part) for which $K_D(\gamma) = \log d$ is called irreducible.*

Hence, irreducible *pdits* are those, for which measuring their key part is an optimal protocol of drawing key. They are called *irreducible* in opposite to those, which can be reduced by distillation protocol to some pdits which has more than $\log d$ of key. The irreducible private bits are intuitively associated with units of privacy. Indeed, a 'physical apparatus', providing some irreducible pbit 'on demand', can be seen as a standard of unit of privacy, like there are standards of some physical units such as meter and second.[5]

It appears to be difficult to characterize the class of irreducible pdits. However we are able to show a subclass of pdits, which are irreducible. To this end we use a result, which is proved in Section 4.5, namely that the relative entropy of entanglement is an upper bound on distillable key. Having this we can state the following proposition:

**Proposition 3.15** *Any pdit $\gamma$, with $E_r(\gamma) = \log d$, is irreducible.*
**Proof.** By definition of *pdit* we have $K_D(\gamma) \geq \log d$ and by Theorem 4.18 from Section 4.5 we have $K_D(\gamma) \leq E_r(\gamma)$ ∎

We can provide now a class of pdits which have $E_r = \log d$ and by the above proposition are irreducible.

**Proposition 3.16** *For any pdit $\gamma_{ABA'B'} \in \mathcal{B}(\mathcal{C}^d \otimes \mathcal{C}^d \otimes \mathcal{C}^{d'_A} \otimes \mathcal{C}^{d'_B})$, written in a form $\gamma_{ABA'B'} = \sum_{i,j=0}^{d-1} |ij\rangle\langle ij| \otimes U_i \rho_{A'B'} U_j^\dagger$, if the states $\rho^{(i)}_{A'B'} := U_i \rho_{A'B'} U_i^\dagger$ are separable for $i \in \{0, \ldots, d-1\}$, the pdit is irreducible.*
**Proof.** Due to bound on relative entropy of pdit given in Theorem 3.13 we have that $E_r(\gamma) \leq \log d$ since the states $\rho^{(i)}_{A'B'}$ are separable and hence have relative entropy of

[5]Note, that the name 'pbit' is a private bit, along with 'ebit', that is short for entangled bit. One can consider also just a single bit of privacy, that can be called 'sebit' (secure bit). It is easy to see, that most of the results presented in this chapter, up to suitable modifications, hold in this case in similar vain [PHHH08].

entanglement equal to zero. $E_r(\gamma)$ is also not less then $\log d$, since it is greater than the amount of distillable key. ∎

Note, that examples (3.51), (3.54) given in Section 3.4.3 fulfill the assumptions of this theorem, and are therefore irreducible pbits. They are also the first known non trivial states (different than pure state) for which the amount of distillable key has been calculated. Using the bound of relative entropy on distillable key, one can also show, that the class of *maximally correlated states* has $K_D = E_D = E_r$, since for the latter $E_D \leq E_r$.

### Construction of a subfamily of $K_D = E_r$ irreducible private states

Due to Proposition 3.16, it is clear that to construct pdits with $K_D = E_r$ we need to be sure that the states $U_i \rho_{A'B'} U_i^\dagger$ which appear on shield upon measuring the key part in standard, basis have zero relative entropy of entanglement, i.e. that they are separable. We do this basing on the notion of *absolutely separable states* [KZ01, Hil05]. These are states, with the following property:

$$U \sigma U^\dagger \in SEP, \tag{3.87}$$

for any unitary $U$. The set of such states is a convex subset of separable states.

Take now a basic pdit: the maximally entangled state, tensored with an absolute separable state:

$$P_+^{(d),\mathcal{B}} \otimes \sigma_{abs}. \tag{3.88}$$

By Proposition 3.16, it is a basic pdit with $K_D = E_r$. Apply now any $\mathcal{B}$-twisting $U = \sum_{ij} |e_i f_j\rangle\langle e_i f_j| \otimes U_{ij}$. This will give a private state $\gamma$, which after measurement in basis $\mathcal{B}$ has upon result $|e_i f_i\rangle\langle e_i f_i|$ on key part, state $\rho_i = U_{ii} \sigma_{abs} U_{ii}^\dagger$ on the shield (note that Proposition 3.16 holds also for any product basis $\mathcal{B}$ in place of standard product basis). Since $\rho_i$ are separable by definition of $\sigma_{abs}$, we have $K_D(\gamma) = E_r(\gamma)$.

Since the above construction holds for any $\mathcal{B}$-twisting for fixed $\mathcal{B}$, we obtain an *orbit* of irreducible private states with desired property. The orbit corresponds to the group of $\mathcal{B}$-twistings.

This construction has natural difficulty, since it is hard to provide an absolutely separable state. Till now such states are constructed only for $\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes 2}$ and $\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes 3}$ (see [KZ01, Hil05] and the references provided in formulation of 15th Open problem in Quantum Information Theory available at [Wer99]). In [Hil05], the absolutely $PPT$ states are characterized, and the characterization involves exponential number of matrix inequalities, which does not give hope for easy providing *explicitly* some new examples. Nevertheless, it shows that the class of irreducible private states with a property $K_D = E_r$ is quite reach.

## 3.7 Approximate private bits

We dealt so far with states that have ideally secure key, which are private states. In this section we consider states which approximates private bits, that is which are close in trace norm distance to some private bit (see Section 2.7). In particular, we present here a special property of such states. In Section 3.4, we saw that pbits have similar form to the maximally entangled states of two qubits. In particular, the norm of the upper-right block in standard form as well as in normalized $X$-form of pbit is equal to $\frac{1}{2}$. We will show here, that for general state the norm of that block tells how close the state is to a pbit: any state which is close in trace norm to pbit must have the norm of this block close to $\frac{1}{2}$, and vice versa.

We will need the following lemma that relates the value of coherence to the distance from the maximally entangled state of two qubits $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The projector onto this state we denote here as $P_+^{(2)}$.

**Lemma 3.17** *For any bipartite state $\rho_{AB} \in B(\mathcal{C}^2 \otimes \mathcal{C}^2)$ expressed on the form $\rho_{AB} = \sum_{ijkl=0}^{1} a_{ijkl}|ij\rangle\langle kl|$ we have:*

$$\mathrm{Tr}\rho_{AB}P_+^{(2)} \geq 1-\epsilon \Rightarrow Re(a_{0011}) > \frac{1}{2} - \epsilon \tag{3.89}$$

*and*

$$Re(a_{0011}) > \frac{1}{2} - \epsilon \Rightarrow \mathrm{Tr}\rho_{AB}P_+^{(2)} \geq 1-2\epsilon \tag{3.90}$$

**Proof.** Assume first, that $\mathrm{Tr}\rho_{AB}P_+^{(2)} > 1-\epsilon$. We have:

$$\mathrm{Tr}\rho_{AB}P_+^{(2)} = \frac{1}{2}(a_{0000} + a_{1111} + 2Re(a_{0011})) \tag{3.91}$$

This is however less than or equal to $\frac{1}{2}(1 + 2Re(a_{0011}))$, and the assertion follows. For the second part of the lemma, assume that $Re(a_{0011}) > \frac{1}{2} - \epsilon$. We then have

$$\mathrm{Tr}\rho_{AB}P_+^{(2)} > \frac{1}{2}(a_{0000} + a_{1111} + 1 - 2\epsilon).$$

We now bound the term $a_{0000} + a_{1111}$. By positivity of the state, we have that $\sqrt{a_{0000}a_{1111}} \geq |a_{0011}| \geq Re(a_{0011})$. Now, by arithmetic-geometric mean inequality, we have that $a_{0000} + a_{1111} \geq 2\sqrt{a_{0000}a_{1111}}$ which gives the proof. ∎

We can prove now that approximate pbits have norm of an appropriate block close to $\frac{1}{2}$.

**Proposition 3.18** *If the state* $\sigma_{ABA'B'} \in B(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^d \otimes \mathcal{C}^{d'})$ *written in the form* $\sigma_{ABA'B'} = \sum_{ijkl=0}^{1} |ij\rangle\langle kl|_{AB} \otimes A_{ijkl}$ *fulfills*

$$||\sigma_{ABA'B'} - \gamma_{ABA'B'}|| \leq \epsilon \tag{3.92}$$

*for some pbit* $\gamma_{ABA'B'}$ *and* $0 < \epsilon < 1$*, then* $||A_{0011}|| \geq \frac{1}{2} - \epsilon$.

**Proof.** The pbit $\gamma_{ABA'B'}$ is a twisted EPR state, which means that there exists twisting $U$ which applied to basic pbit $P_+^{(2)} \otimes \rho$ gives $\gamma_{ABA'B'}$. We apply this $U$ to both states $\sigma_{ABA'B'}$ and $\gamma_{ABA'B'}$ and trace out the $A'B'$ subsystem of both of them. Since these operations can not increase the norm distance between these states (see Section 2.7), so that we have for $\sigma_{AB} = \mathrm{Tr}_{A'B'} U \sigma_{ABA'B'} U^\dagger$

$$||\sigma_{AB} - P_+^{(2)}|| \leq \epsilon. \tag{3.93}$$

It implies, by equivalence of norm and fidelity (lemma 2.20) that

$$F(\sigma_{AB}, P_+^{(2)}) \geq 1 - \frac{1}{2}\epsilon. \tag{3.94}$$

We have also that $F(\sigma_{AB}, P_+^{(2)})^2 = \mathrm{Tr}\sigma_{AB} P_+^{(2)}$ so that

$$\mathrm{Tr}\sigma_{AB} P_+^{(2)} > 1 - \epsilon. \tag{3.95}$$

Now by lemma (3.17) this yields $|a_{0011}| \geq Re(a_{0011}) \geq \frac{1}{2} - \epsilon$, where $a_{0011}$ is coherence of the state $\rho_{AB} = \sum_{ijkl=0}^{1} a_{ijkl} |ij\rangle\langle kl|$. However, we have

$$|a_{0011}| = |\mathrm{Tr} U_{00} A_{0011} U_{11}^\dagger| = |\mathrm{Tr} U_{11}^\dagger U_{00} A_{0011}| \tag{3.96}$$

where $U_{00}$ and $U_{11}$ come from twisting, that we have applied. The last equality follows from the property of trace: $\mathrm{Tr}XY = \mathrm{Tr}YX$, for matrices $X$ and $Y$ of proper shape so that multiplication can be performed. Using now the fact that $\|A\| = \sup_U \mathrm{Tr}UA$ (see Appendix A.2), where supremum is taken over unitary transformations we get

$$\|A_{0011}\| \geq |a_{0011}| \geq \frac{1}{2} - \epsilon. \tag{3.97}$$

This ends the proof. ∎

Now we will formulate and prove the converse statement, saying that when the norm of the right upper block is close to 1/2, then the state is close to some pbit.

**Proposition 3.19** *If the state* $\sigma_{ABA'B'} \in \mathcal{B}(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^d \otimes \mathcal{C}^{d'})$ *with a form* $\sigma_{ABA'B'} = \sum_{ijkl=0}^{1} |ij\rangle\langle kl|_{AB} \otimes A_{ijkl}$ *fulfills* $||A_{0011}|| > \frac{1}{2} - \epsilon$ *for some* $0 < \epsilon < \frac{1}{8e^2}$*, then there exists pbit* $\gamma$ *such, that*

$$||\sigma_{ABA'B'} - \gamma_{ABA'B'}|| \leq \delta(\epsilon) \tag{3.98}$$

*where*

$$\delta(\epsilon) = 2\sqrt{4\sqrt{2\epsilon} + \eta(2\sqrt{2\epsilon})} + 2\sqrt{2\epsilon} \tag{3.99}$$

*and* $\eta(x) = -x \log x$*. Note, that* $\delta(\epsilon)$ *vanishes, when* $\epsilon$ *approaches zero.*

**Proof.** In this proof by $\rho_X$ we denote respective subsystem of the state $\rho_{ABA'B'}$. If it is not explicitly stated, the facts invoked in this proof can be found in Section 2.7.1. These are mostly the properties of the von Neumann entropy and quantum mutual information. Let $\rho_{AB}$ be the privacy-squeezed state of the state $\sigma_{ABA'B'}$ i.e. $\rho_{AB} = Tr_{A'B'}\rho_{ABA'B'}$ where $\rho_{ABA'B'} = U_{ps}\sigma_{ABA'B'}U_{ps}^{\dagger}$ for certain twisting $U_{ps}$. The entry $a_{0011}$ of $\rho_{AB}$ is equal to $||A_{0011}||$. By assumption we have, $a_{0011} = ||A_{0011}|| > \frac{1}{2} - \epsilon$. By lemma 3.17 (equation (3.90)) we have that

$$\mathrm{Tr}\rho_{AB}P_{+}^{(2)} > 1 - 2\epsilon. \tag{3.100}$$

We have then

$$F(\rho_{AB}, P_{+}^{(2)})^2 = \mathrm{Tr}\rho_{AB}P_{+}^{(2)} \tag{3.101}$$

which, by equivalence of norm and fidelity (lemma 2.20) gives

$$||\rho_{AB} - P_{+}^{(2)}|| \leq 2\sqrt{2\epsilon}. \tag{3.102}$$

Let us now consider the state $\rho_{ABA'B'} = U_{ps}\sigma_{ABA'B'}U_{ps}^{\dagger}$ and its purification to Eve's subsystem $\psi_{ABA'B'E}$ so that we have:

$$\rho_{AB} = \mathrm{Tr}_{A'B'E}(\psi_{ABA'B'E}) \tag{3.103}$$

By the Fannes inequality (see Eq. (2.24) in Sec. 2.7.1) we have that

$$S(\rho_{AB}) = S(\rho_{A'B'E}) \leq 2\sqrt{2\epsilon}\log d_{AB} + \eta(2\sqrt{2\epsilon}). \tag{3.104}$$

From this we will get that $||\psi_{ABA'B'E} - \rho_{AB} \otimes \rho_{A'B'E}||$ vanishes with $\epsilon$ approaching zero. We prove this as follows. Since norm distance is bounded by relative entropy as follows (see Eq. (2.93), Section 2.7.1)

$$\frac{1}{2}||\rho_1 - \rho_2||^2 \leq S(\rho_1|\rho_2) \tag{3.105}$$

one gets:

$$||\psi_{ABA'B'E} - \rho_{AB} \otimes \rho_{A'B'E}|| \leq \sqrt{2S(\psi_{ABA'B'E}||\rho_{AB} \otimes \rho_{A'B'E})}.$$

We use now the fact, that the relative entropy distance of the state to its subsystems is equal to quantum mutual information, which gives

$$||\psi_{ABA'B'E} - \rho_{AB} \otimes \rho_{A'B'E}|| \leq \sqrt{2I(AB : A'B'E)_{\psi}}.$$

Since the entropies of subsystems of a pure bipartite state are equal, and the entropy of the pure state is zero, we have:

$$I(AB:A'B'E)_\psi = 2S(AB)_\psi \leq 2(2\sqrt{2\epsilon}\log d_{AB} + \eta(2\sqrt{2\epsilon})), \tag{3.106}$$

where last inequality comes from Eq. (3.104). Coming back to inequality (3.106) we obtain

$$||\psi_{ABA'B'E} - \rho_{AB}\otimes\rho_{A'B'E}|| \leq \sqrt{2I(AB:A'B'E)} \leq 2\sqrt{2\sqrt{2\epsilon}\log d_{AB} + \eta(2\sqrt{2\epsilon})}. \tag{3.107}$$

If we trace out the subsystem $E$ the inequality is preserved:

$$||\rho_{ABA'B'} - \rho_{AB}\otimes\rho_{A'B'}|| \leq 2\sqrt{4\sqrt{\epsilon} + \eta(2\sqrt{\epsilon})} \tag{3.108}$$

where we have put $d_{AB} = 4$, as we deal with pbits. Now by triangle inequality one has:

$$||\rho_{ABA'B'} - P_+^{(2)}\otimes\rho_{A'B'}|| \leq ||\rho_{ABA'B'} - \rho_{AB}\otimes\rho_{A'B'}|| + ||\rho_{AB}\otimes\rho_{A'B'} - P_+^{(2)}\otimes\rho_{A'B'}||. \tag{3.109}$$

We can apply now the bounds (3.102) and (3.108) to the above inequality obtaining

$$||\rho_{ABA'B'} - P_+^{(2)}\otimes\rho_{A'B'}|| \leq 2\sqrt{4\sqrt{2\epsilon} + \eta(2\sqrt{2\epsilon})} + 2\sqrt{2\epsilon}. \tag{3.110}$$

Let us now apply the twisting $U_{ps}^\dagger$ (transformation which is inverse to twisting $U_{ps}$) to both states on left-hand-side of the above inequality. Since $\rho_{ABA'B'}$ is defined as $U_{ps}\sigma_{ABA'B'}U_{ps}^\dagger$ we get that:

$$||\sigma_{ABA'B'} - U_{ps}^\dagger P_+^{(2)}\otimes\rho_{A'B'}U_{ps}|| \leq 2\sqrt{4\sqrt{2\epsilon} + \eta(2\sqrt{2\epsilon})} + 2\sqrt{2\epsilon}, \tag{3.111}$$

i.e. our state is close to pbit $\gamma = U_{ps}^\dagger P_+^{(2)}\otimes\rho_{A'B'}U_{ps}$. Then the theorem follows with $\delta(\epsilon) = 2\sqrt{4\sqrt{2\epsilon} + \eta(2\sqrt{2\epsilon})} + 2\sqrt{2\epsilon}$. ∎

**Remark 3.20** *The above propositions establish the norm of upper-right block of matrix (written in computational basis according to ABA'B' order of subsystems), as a parameter that measures closeness to pbit, and in this sense it measures security of the bit obtained from the key part. The state of form (3.38) is close to a pbit if and only if the norm of this block is close to $\frac{1}{2}$. This property has been recently shown to have analogue for pdits with $d \geq 3$ [Aug08].*

## 3.8 Other possible definitions of quantum states that have secure key yields equivalent results.

In Section 3.1 we have studied security content of a bipartite quantum state. To this end we first said, that a state 'have key' if it has 'directly accessible' (ideally secure) 'classical key'. Specifying in some way the 'direct accessibility', we have provided Definition 3.1 of states that have key (we will call them in this section states from class $C_1$). This definition is both simple, and restrictive. Due to simplicity, the states from $C_1$ are in relatively easy way characterized as the private states, so that $C_1{=}PS$. However, due to restriction, the states from $C_1$ are bipartite states with subsystems of dimensions $\dim AA'$ and $\dim BB'$ dividable by some number $d = \dim A = \dim B$.

In this Section we first ask about security content of an *arbitrary bipartite state*. Since arbitrary bipartite state may have subsystems dimension of which do not have common divisor $\geq 1$, we have to consider other interpretations of 'direct accessibility' than via measuring of some predefined subsystem (the $AB$ subsystem called main part), as in case of the $C_1$. We also address the issue of which accessibility is the most 'direct'. If the state is key distillable ($K_D > 0$), it has in some sense accessible key, but the very fact of key distillability does not implies, 'how easy' it is to obtain the key. In other words: how much the information about the key is encoded into operation which gains it, versus how much it is encoded into explicit structure of the state.

Motivated by this issues, we consider two other interpretations of direct accessibility which give rise to definitions Def. 3.9 and Def. 3.10. The states that have directly accessible key according to these definitions, are called states from class $C_2$ and $C_3$ respectively. We demonstrate, that they lead to similar results as we have already obtained basing on class $C_1$. More precisely, the states from class $C_2$ and $C_3$ can be transformed via local LOCC operations into states from $PS$, and vice versa. The class $C_2$, and the fact that it is equivalent to $PS$, we attribute to Renes and Smith [RS07], since, although in different formulation, they first used this class, and argued about its security, which clearly implies the equivalence.

To this end, we first say that two bipartite states $\rho_1$ and $\rho_2$ are *locally equivalent* ($\rho_1 \sim \rho_2$), when they are transformable one into another by means of the local operations. Second, we define the relation of equivalence on the family of classes of states. The two classes $C$ and $D$ are equivalent ($C \sim D$), if and only if:

$$\forall_{\rho\in C}\, \exists_{\sigma\in D}\, \sigma \sim \rho \;\&\; \forall_{\sigma\in D}\, \exists_{\rho\in C}\, \rho \sim \sigma. \tag{3.112}$$

Finally we show, that classes $C_2$ and $C_3$ are equivalent to the class of all private states $PS$:

$$C_2 \sim C_3 \sim PS. \tag{3.113}$$

In Section 3.9.1 we observe, that this equivalence has a good property in context of the so called *distillable key*, that will be presented in Chapter 4. Namely, replacing classes $PS$, $C_2$ and $C_3$ in definition of distillable key gives the same quantity $K_D$.

Finally in Section 3.9.1 we compare the classes $PS$, the $C_2$ and $C_3$.

### 3.8.1 Two other interpretations of 'direct accessibility'

**Definition 3.7** *Two bipartite states $\rho$ and $\sigma$ are locally equivalent ($\rho \sim \sigma$) if there exist two local LOCC operations $\Lambda$ and $\Lambda'$, such that*

$$\begin{aligned} \Lambda(\rho) &= \sigma, \\ \Lambda'(\sigma) &= \rho. \end{aligned} \tag{3.114}$$

*We say then, that $\Lambda'$ is a local inverse of $\Lambda$, and vice versa.*

It is easy to check, that the relation $\sim$ on states is an equivalence relation on the set of states. Note, that there are obviously states which are not in this relation. These are states which have different values of some entanglement monotone. Basing on this relation we define the following relation on classes of states.

**Definition 3.8** *For any two nonempty classes of states $C$ and $D$ we say that $D$ is reachable from $C$ ($D \leftarrow C$) iff there holds:*

$$\forall_{\rho \in C} \exists_{\sigma \in D} \rho \sim \sigma. \tag{3.115}$$

*$C$ and $D$ are called locally equivalent (denoted as $C \sim D$) iff $D \leftarrow C$ and $C \leftarrow D$.*

#### First alternative definition of quantum states that have key

In this section we provide the definition of the class $C_2$ - the first alternative definition of quantum states that have key. This definition involves the notion of a quantum measurement (see Section 2.3.4).

**Definition 3.9** *(adapted from [RS07]) A quantum state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ is in class $C_2$ if there exist quantum measurements $Q_A$ and $Q_B$ on Alice's and Bob's sites respectively, such that the state of their classical results on system $\bar{A}\bar{B}$, together with the purifying system $E$ of $\rho_{AB}$ has form:*

$$\left( \sum_{i=0}^{d-1} \frac{1}{d} |ii\rangle\langle ii|_{\bar{A}\bar{B}} \right) \otimes \rho_E. \tag{3.116}$$

*for some state $\rho_E$ of $E$.*

According to the above definition we does not demand the state to have a structure of four subsystems: two on Alice's and two on Bob's site, as it is in case of states from $PS$. Moreover, the key is obtained only in standard basis. Nevertheless, we have the following theorem:

**Proposition 3.21** *(adapted from [RS07]) There holds* $C_2 \sim PS$.

**Proof.**

($C_2 \leftarrow PS$). To prove this relation, consider a state $\rho_{ABA'B'}$ from $PS$. It follows, that after measuring the $AB$ subsystem in a basis $\mathcal{B}$ of the purification of this state, and tracing out $A'B'$ we obtain an ideal ccq state.

Basing on this fact, we define the local operations which output the locally equivalent state $\rho'$, that will be from $C_2$. By Theorem 3.2, we know, that the state $\rho_{ABA'B'}$ is actually a private state. If we apply to this state on $A$ ($B$) the operation which copies $A$ into $\bar{A}$ ($B$ into $\bar{B}$) which is initially taken in pure state $|0\rangle_{\bar{A}}$ ($|0\rangle_{\bar{B}}$) defined as:

$$\forall_{e_i,j} \, |e_i\rangle_A |j\rangle_{\bar{A}} \mapsto |e_i\rangle_A |(i+j) \, mod \, d\rangle_{\bar{A}}, \tag{3.117}$$

with that for $B\bar{B}$ defined analogously, the resulting state is:

$$\rho'_{\bar{A}\bar{B}ABA'B'} = \sum_{i,j=0}^{d-1} \frac{1}{d} |ii\rangle\langle jj|_{\bar{A}\bar{B}} \otimes |e_i f_i\rangle\langle e_j f_j|_{AB} \otimes U_i \sigma_{A'B'} U_j^\dagger. \tag{3.118}$$

To see, that the above state is from $C_2$, consider the following quantum measurement on $\bar{A}AA'$ subsystem:

$$\Lambda_A(\rho') = \sum_{i=0}^{d-1} P_i \rho' P_i \tag{3.119}$$

with $P_i = |i\rangle\langle i|_{\bar{A}} \otimes \mathrm{I}_{AA'}$. Take now the purification $|\psi\rangle_{\bar{A}\bar{B}ABA'B'E}$ of the state $\Lambda_A \otimes \Lambda_B(\rho')$ with $\Lambda_B$ defined analogously on $\bar{B}BB'$. It is easy to see, that the ccq state emerging on $\bar{A}\bar{B}E$ is an ideal ccq state.

Note, that the only LOCC operations that we have used was adding locally an ancilla system in pure state and performing locally a unitary transformation. Hence, there exist also the LOCC operation which is an inverse of the latter on this particular state. It is just performing the inverse unitary operation, and tracing out the ancilla system. Moreover, the choice of basis $\mathcal{B}$ was arbitrary so that according to Definition 3.7 any private state is locally equivalent to some state from $C_2$. This ends the first part of the proof.

($PS \leftarrow C_2$) Consider a state $\rho_{\tilde{A}\tilde{B}} \in B(\mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}})$ from $C_2$. There exist quantum measurements $Q_A$ and $Q_B$ whose results are maximally correlated and are product with the purifying system of $\rho_{\tilde{A}\tilde{B}}$. Pair of these measurements results in a bipartite

state of four systems $AB\bar{A}\bar{B}$ (systems AB carries the 'quantum' results of measurements). Basing on this we easily give a locally equivalent state $\rho'$. The idea is to apply instead of the quantum measurements $Q_A$ and $Q_B$, their reversible parts (see Sections 2.3.6, and 2.3.7). Such implementation may involve additional two ancillary systems $\hat{A}$ and $\hat{B}$ that would have been traced out when $Q_A$ and $Q_B$ were implemented via basic quantum operations. Resulting state $\rho'$ will be on systems $A\bar{A}\hat{A}B\bar{B}\hat{B}$. We claim now, that it belongs to $PS$. Consider a purification $|\psi_{\rho'}\rangle$ of $\rho'$, to system $E$. It is clear, that if we measure it on $\bar{A}\bar{B}$ in standard product basis, and trace out the system $A\hat{A}B\hat{B}$, we obtain an ideal ccq state. Indeed, we see this by performing partial trace over systems one by one. If we first trace out $\hat{A}\hat{B}$, we obtain by construction a state which is from class $C_2$ , already being measured on $\bar{A}\bar{B}$. By definition of $C_2$, if we trace out further systems $AB$, the state of $\bar{A}\bar{B}$ together with the purifying system $E$ of the state $|\psi_{\rho'}\rangle$ is an ideal ccq state.

It follows then, that $\rho'$ is from $C_1$. Hence by Theorem 3.2, the state $\rho'$ is a private state. The operations that we have used to transform $\rho_{\tilde{A}\tilde{B}}$ into $\rho'$ can be easily inverted on $\rho'$, by means of LOCC operations as it follows from definition of reversible part of operation (Def. 2.4), which is invertible on the image. Thus, any state $\rho_{\tilde{A}\tilde{B}}$ from $C_2$ is in relation $\sim$ with some private state, hence the assertion follows.

### Second alternative definition of states that have key

We present now yet another alternative definition of states that have key. We call them the states from class $C_3$.

**Definition 3.10** *A quantum state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ is from $C_3$ if it has subsystem $ab$, such that the subsystem $abE$ of its purification $|\psi_\rho\rangle_{ABE}$ is a ccq state of the form:*

$$\Big(\sum_{i=0}^{d-1} \frac{1}{d} |ii\rangle\langle ii|_{ab}\Big) \otimes \rho_E. \tag{3.120}$$

We have now the theorem analogous to Theorem 3.21:

**Proposition 3.22** *There holds $C_3 \sim PS$.*

**Proof.** ($C_3 \leftarrow PS$) Consider a state $\rho_{ABA'B'}$ from $PS$. We construct the locally equivalent state, in similar way as in the proof ($C_2 \leftarrow PS$), via adding appropriate ancilla in state $|0\rangle$ on $\mathcal{H}_a$ and $\mathcal{H}_b$ and performing (local) control unitary operations, which copies the state of system $A$ into system $a$ and system $B$ into system $b$ respectively performing also appropriate change of basis. Such transformation on systems $A$ and $a$ is defined as:

$$\forall_{e_i,j} \; |e_i\rangle_A |j\rangle_{\bar{A}} \mapsto |e_i\rangle_A |f_{(i+j) \bmod d}\rangle_{\bar{A}}. \tag{3.121}$$

with an analogous definition for a such unitary operation on system $Bb$.

By Theorem 3.2, we know, that the state $\rho_{ABA'B'}$ is actually a private state. Hence, after applying the above operations , the resulting state is:

$$\rho'_{\bar{A}\bar{B}ABA'B'} = \sum_{i,j=0}^{d-1,d-1} \frac{1}{d} |e_i f_i\rangle\langle e_j f_j|_{\bar{A}\bar{B}} \otimes |e_i f_i\rangle\langle e_j f_j|_{AB} \otimes U_i \sigma_{A'B'} U_j^\dagger. \tag{3.122}$$

To see, that the above state is from $C_3$, consider its purification:

$$|\psi_\rho\rangle = \sum_{ij} |e_i f_i\rangle_{\bar{A}\bar{B}} |e_i f_i\rangle_{AB} \otimes (U_i^{A'B'} \otimes \mathrm{I}_E) |\psi_\sigma\rangle^{A'B'E}, \tag{3.123}$$

where $|\psi_\sigma\rangle$ is any purification of the state $\sigma_{A'B'}$. It is now easy to see, that if we trace out the systems $ABA'B'$, the resulting state will have a form of an ideal $\mathcal{B}$-ccq state, hence the assertion follows.

($PS \leftarrow C_3$) This part of the proof is straightforward. Consider a state $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ such that there is a subsystem $ab$ which is in an ideal $\mathcal{B}$-ccq state with a purifying system $\rho_E$ of $\rho_{AB}$. Here $\mathcal{B}$ is a standard product basis. Analogously as in proof $C_2 \rightarrow PS$, we can create via local operations that have local inverse a copy of the system $ab$ in arbitrary product basis. It is easy to see that resulting state is from $C_1$, and thanks to Theorem 3.2, it is a private state.

## 3.9 Comparison of definitions of quantum states that have key

In this section we deliberate on to what extent the three proposed definitions are equivalent, and further argue why the first is distinguished among the others.

### 3.9.1 On equivalence of definitions

It is a well known fact, that two states $\rho$ and $\sigma$ which are locally equivalent, have the same amount of entanglement measured by any monotone $E$. To give example, let us check this fact for $E$ which does not increase under LOCC operations (see Section 2.8.1). Consider the operations giving $\Lambda(\rho) = \sigma$ and $\Lambda'(\sigma) = \rho$. Neither of them can decrease the value of $E$ on its argument, for the other would then increase it, which is impossible for $E$, hence $E(\rho) = E(\sigma)$.

In particular, locally equivalent state have the same amount of key, which is measured by the so called *distillable key* $K_D$ introduced in the next chapter. This is the main reason, for which we consider the three proposed definition as essentially equivalent. We will discuss this fact in detail in next chapter.

This fact shows, that at the first sight there is no a priori reason to distinguish one of these definitions, as they indicate quantitatively the same amount of secrecy in quantum states. However in the following subsection we show that there are practical reasons for distinguishing the first definition, which is via Theorem 3.2 equivalent to definition of private states.

### Comparing the classes $C_1$ (consisting of private states), the $C_2$ and $C_3$

Having provided two other definitions of states that have key, we compare resulting classes of states to the very first (Def 3.1) giving rise to $C_1$, which due to characterization is just the class of private states.

As it is indicated by results of [RS07], class $C_2$ can be useful for proving security of some quantum key distribution protocols. However, the class $C_2$ is in a sense less 'basic' than the $C_1$ in that it the 'access' is 'less direct' as involving a more general operations of arbitrary quantum measurements than the complete von Neumann measurement, on a previously specified subsystem. Such general operation can be viewed as already a kind of distillation of key.

The most 'basic' class of states that have key, in a sense, that the access to the key is the most 'direct' is given by the third definition 3.10 (of $C_3$). It has yet an apparent disadvantage in comparison to the $C_1$ in that it excludes the maximally entangled states. This is because the maximally entangled state does not have a subsystem which is in the same state as the $AB$ subsystem of an ideal ccq state. It becomes so, after measurement in some product basis.

**Remark 3.23** *(natural definition based on local incomplete von Neumann measurements) In a sense more intuitive than class $C_1$ is the following, considered in [BHH+ 08]. Two incomplete von Nemuann measurements on the whole systems A and B respectively are performed, with the security constrained imposed that the resulting state can be transformed via controlled unitary operation into the state secure according to Def. 3.9. By Theorem 3.21, the class of such states is also locally equivalent to the class of private states*[6].

**Remark 3.24** *(on the states from $C_3$) One can obtain a structure of states from $C_3$ with a natural division into main part ab and side part $A'B'$ similarly as we have 'deriven' it for $C_1$ from the example of singlet states. To this end one can consider states that have ideally secure classical key. They satisfy two conditions: (i) are mixed, (ii) the state $\rho_E$ represents all knowledge that is accessible to Eve. Due to (i) there exist somewhere the system which purifies $\rho_{ccq}^{ideal}$ (call it here P), while due to (ii), this system P can not be in power of Eve. Since we assumed at the beginning*

[6] We acknowledge M. Horodecki for discussion on this definition.

*the worst-case senario, this system must be somewhat accessible to Alice and Bob. The most general way it can be made accessible to them, is to split it into two parts: $P = A'B'$, one of which is on Alice's and the other on Bob's site.*

**Remark 3.25** *(subclass of private states) We note also, that one could perform a modification of Def 3.1 basing on the simplification taken in original paper [HHHO05c]. Namely one could consider only the standard product basis in place of a general product basis $\mathcal{B} = \{|e_i\rangle|f_j\rangle\}_{i,j=0}^{d-1}$. Such modified definition would be obviously equivalent in the sense of the already presented equivalence, as it is in case of $C_2$ and $C_3$. However, in turn some of maximally entangled states would not be included, and hence they would not be private states. For this reason, in [HHHO05a], we do not follow this simplification. Instead we use this fact (as e.g. in previous sections) showing some properties for private states with the use of standard product basis, just mentioning that the same holds for arbitrary product basis $\mathcal{B}$. It is relatively easy to check, but we do not prove it so that taking this subclass of private states as the target states in key distillation protocol in Def 4.1, gives the same quantity - $K_D$.*

The private states form a class of states that after complete von Neumann measurement on the key part (which reads incomplete von Neumann measurement on both the key part and shield), leads to an ideal ccq state i.e. maximally correlated state which is uncorrelated from the eavesdropper. Thus these states gives us an insight into the origin of quantum security that is realized by the ideal ccq states, while the latter states in a sense 'do not remember' this origin. For this reason, instead of ideal ccq states (that have key according to definition 3.1 i.e. from $C_1$) we will use equivalent notion of private states. An advantage of this approach, opposite to using the notion of $C_1$ is that private states are *bipartite*, i.e. do not invoke explicitly the Eve's subsystem of their purification. How useful is this fact, will appear in next chapters. In particular, it allows for introducing the amount of key that can be obtained from many copies of a quantum state shared between distant laboratories as entanglement measure. This removes Eve from description of the protocol of key distillation.

## 3.10 Further development and open problems

Private states were studied further in [HA06] in context of entanglement. It is shown there, that all private states $\gamma$ have $E_D(\gamma) > 0$. One can find there also a simple proof of the fact, that $E_C(\gamma) \geq \log d$, by observing, that pure ensambles of private states are of special form. Each member of such ensamble has the $AB$ subsystem in a pure maximally entangled state. The latter fact follows also already from [HHHO05c, HHHO05a], yet one needs two strong results to show it: Theorem 4.18 presented in Section 4.5, and Theorem 2.26 (see Section 2.8.1).

In [RS07], the twisting operator with izometries in place of unitary transformations was used. We note, that such twisting can be performed via local embeddings (adding locally pure states), and performing suitable unitary twisting on this new state. In particular, the states whose privacy is proved via twisting operator, are locally equivalent to private states.

### 3.10.1 Development on the subject of locking entanglement with private states

In [CW05] it was shown, that the so called *squashed entanglement* $I_{sq}$ and quantity called *entanglement of purification* $E_P$ are lockable. Also, the locking effect for flower states has been strengthen there: a generalized family of flower states given there, for any $\epsilon > 0$ reveals $(\log(1 + (\log d)^3) \downarrow (1 - \epsilon) \log d + 3 \log\log d - 3) -$ Tr-locking of $E_C$, for $d$ large enough. Special kind of entanglement locking in terms of an entanglement measure satisfying some axioms has been studied in [Gou07]. Upper bound on the amount of unlocked entanglement has been shown, excluding some states from that which reveal locking of $E_D$.

There is also the following interesting connection between private states and locking, that has been to some extent a motivation for locking of entanglement, yet was not made explicit in such generality in [HHHO05b]:

**Theorem 3.26** *[HH06] Existence of PPT states with $K_D > 0$, is sufficient condition for lockability of $\mathcal{N}$ and $E_N$.* Moreover, the lockability of $\mathcal{N}$ and $E_N$ is revealed by some private bits which are approximated by PPT states. Since we show in Chapter 5, that there are PPT key distillable states, this theorem provides a way to construct examples of states which reveal this effect.

In [HHH$^+$05], it is noted, that Non Lock has the relative entropy of entanglement from any set of bipartite states, which is closed under product unitary transformations $U_A \otimes U_B$.

### 3.10.2 Private states and quantum key distribution protocols

As it will be shown in Theorem 4.11, any LOCC operation that leads to secure key in terms of ideal ccq states can be performed in a way which results in private states [HHHO05a]. This fact was used in context of coherent attacks in [RS07]. There, although implicitly, Definition 3.9 was used for the first time. This approach resulted in simple proof of security of the BB84 protocol at higher error level [RGK05], similarly as the Shor-Preskill method gave proof for security of BB84 protocol at certain (lower) error level. The link between private states and uncertainty principle has been found in [Koa07] (see also [CW05]). It was then developed to full extent in [RB07, RB08], where the system of shield is treated as a single one.

### 3.10.3 Open problems

There are plenty of open problems concerning properties of private states. We give below exemplary list:

1. Characterization of irreducible private states.
2. Characterization of $K_D = E_r$ (or $K_D = E_r^\infty$) private states
3. (Entanglement properties of private states with constraints) Given a fixed value of $E_C$ (or other entanglement measure), what are private states with this entanglement measure ?
4. (General transformations within class of private states) Which private states are transformable one into another via LOCC ?
5. (minimal private states) Given some constraints for private states, such as fixed entropy, or entanglement measure what is minimal dimension of the shield ? or in general what is the minimal dimension of private states satisfying the constraints ?

There is still pending problem concerning the locking effect:

1. [Wer99] is $E_D$ lockable ? Partial results on this has been given in [Gou07, GH08]

# Chapter 4

# Distillable key as an entanglement measure

In this Chapter we present a slightly improved and extended version of the material, that can be found in [HHHO05a], Sections VIII-IX and XI, and [HPHH05]. We provide a definition of the so called distillable key $K_D$, - a function of a bipartite state $\rho$ that reports its security content. Similarly as distillable entanglement, $K_D$ is an operational measure of entanglement, however instead of maximally entangled states only, the private states are distilled by means of local operations and classical communication. We introduce also the definition of classical distillable key $C_D$, and show that in the most important case of the *worst case LOPC scenario*, it is equal to distillable key. The relative entropy of entanglement is shown to be an upper bound on distillable key.

In Section 4.1, we define distillable key in terms of private states. In Section 4.2, we define the classical distillable key. Following the results of [DW05, DW04] and the scheme already known in classical cryptography called *classical key agreement* [Mau93] we give a definition of the so called Local Operations and Public Communication (LOPC operations), introducing the LOPC scenario.

In Section 4.3, Theorem 4.12 we show that the two introduced quantities are *equal* to each other:

$$K_D(\rho_{AB}) = C_D(\rho_{AB}). \tag{4.1}$$

To show the equality (4.1), in Section 4.3.1 we introduce the so called *coherent LOPC* (CLOPC) operations. More concretely, we use the CLOPC operations to specify for a given LOPC operation which outputs ideal ccq state, the LOCC operation which outputs a private bit. The shield of this private state emerges out of the CLOPC protocol as the joined state of Alice's and Bob's local trash bins. The CLOPC operation is then easily turned into demanded LOCC operation.

Since the case where an eavesdropper holds a purifying system of a bipartite state is the worst from cryptographic point of view, we can safely focus on the distillable key $K_D$.

In Section 4.4, we argue that $K_D$ is an operational entanglement measure. We invoke the axioms that $K_D$ might satisfy, that were collected or proved in [Chr06], and present partial results on convexity and asymptotic continuity of $K_D$.

In Section 4.5 we provide the second main result of this Chapter, which is an application of the fact, that $K_D$ is entanglement measure. Namely, we show that the relative entropy of entanglement is an upper bound on distillable key.

In Section 4.6 we show preliminaries results on key distillability of some bipartite states. In particular, Section 4.6.2 is devoted to exploit the results of Devetak and Winter on *one-way distillable key*. We show that their approach fits into our context, so that the lower bounds on the one-way distillable key according to their definition, is also a lower bound for $K_D$. We then give various simplified lower bounds on distillable key using notion of privacy squeezing introduced in Chapter 3. In particular it is shown, that $K_D(\rho_{ABA'B'}) \geq C_D([\rho^{ps}_{AB}]^{ccq})$ where $[\rho^{ps}_{AB}]^{ccq}$ is a ccq state of the privacy squeezed state $\rho_{ABA'B'}$.

Finally in Section 4.7 we discuss further development of this paradigm. In particular the main result of [CEH$^+$07] which is that an entanglement monotone satisfying some reasonable axioms is an upper bound on distillable key. Its other properties, has been investigated in context of other entanglement measure in [Chr06].

## 4.1 Distillation of private states - the LOCC scenario

In previous chapter we have established a family of states - pdits - which have the following property: after measurement in some product basis $\mathcal{B}$, they give a perfect dit of key. As we have noted in Section 2.3.2, in entanglement theory one of the important aims is to distill singlets (maximally entangled states) which leads to operational measure of distillable entanglement [BBP$^+$96]. We will pose now an analogous task namely distilling pdits (private states) which are of the form (3.8):

$$\gamma^{(d)} = \frac{1}{d} \sum_{i,j=0}^{d-1} |e_i f_i\rangle\langle e_j f_j|_{AB} \otimes U_i \sigma_{A'B'} U_j^\dagger. \tag{4.2}$$

This will give rise to a definition of distillable key i.e. maximal achievable rate of distillation of pdits. Similarly as in the case of distillation of singlet, it is usually not possible to distill exact pdits. Therefore the formal definition of distillable key $K_D$ will be a bit more involved.

**Definition 4.1** *For any state $\rho_{AB} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ let us consider sequence $P_n$ of LOCC operations such that $P_n(\rho_{AB}^{\otimes n}) = \sigma_n$, where $\sigma_n \in B(\mathcal{H}_A^{(n)} \otimes \mathcal{H}_B^{(n)})$. A set of operations $\mathcal{P} \equiv \cup_{n=1}^{\infty}\{P_n\}$ is called pdit distillation protocol of state $\rho_{AB}$ if there holds*

$$\lim_{n\to\infty} ||\sigma_n - \gamma_{d_n}|| = 0, \tag{4.3}$$

*where $\gamma_{d_n}$ is a pdit whose key part is of dimension $d_n \times d_n$.*

*For a pdit distillation protocol $\mathcal{P}$, its rate is given by*

$$\mathcal{R}(\mathcal{P}) = \limsup_{n\to\infty} \frac{\log d_n}{n} \tag{4.4}$$

*The distillable key of state $\rho_{AB}$ is given by*

$$K_D(\rho_{AB}) = \sup_{\mathcal{P}} \mathcal{R}(\mathcal{P}). \tag{4.5}$$

Due to this definition, Alice and Bob given $n$ copies of state $\rho_{AB}$ try to get a state $\sigma_n$, which is close to some pdit $\gamma_{d_n}$ with $d = d_n$. Their task is to maximize $d_n$ with respect to $n$, over all possible LOCC operations. Thus the above definition is an example of the well known scheme called an LOCC scenario. According to this scenario, Alice and Bob transform many copies of an input state via LOCC operations to obtain a state with special properties.

**Remark 4.1** *Unlike so far in entanglement theory, an effect of distillation of quantum key depends not only on initial state, but also on the choice of the output state. This is because private dits are not reversibly transformable with each other by means of LOCC operations, as it is in case of maximally entangled states (see Eq. (2.45)) in LOCC entanglement distillation. It can be seen from the example given in Section 3.4.3. There we showed a private state, which has a gap between distillable entanglement and entanglement cost. It is obvious then, that such a pdit can not be transformed reversibly via LOCC into a singlet state, who has these entanglement measures equal. Thus the quantity $K_D$ is a rate of distillation to the large class of states. (Of course, since the definition involves optimization, $K_D$ is well defined; in particular the expensive pdits will be suppressed).*

One can be interested now if this new parameter of states $K_D(\rho)$ has an operational meaning for quantum cryptography. One connection is obvious: given $n$ copies of a quantum state $\rho_{AB}$, Alice and Bob may try to distill some pdit state, and hence get (according to the above definition) $\lfloor nK_D(\rho_{AB})\rfloor$ bits of classical key if such distillation has nonzero rate. They can finally get rid of the shield and measure the key part in an appropriate product basis to yield an ideal ccq state. However the following question arises:

- Is distillation of private states an optimal way of extraction of a classical key from a quantum state?

To answer this question one needs a formal definition of *classical distillable key*, which we provide in next section. Having done this, we will give a positive answer to this question: distilling private dits is the best way of distilling classical key from a quantum state.

## 4.2 Distillable classical key- LOPC scenario

In this section, we define the so called classical key, within the LOPC scenario. The LOPC scenario scenario, being generalization of the classical cryptographic concept of secure key agreement [CK78, Mau93, AC93] (see also [Chr02, CEH$^+$07]) was first used in [DW05, DW04]. In the form, which we introduce here, it is analogous to the LOCC scenario shown in Chapter 2. This scenario, was first studied in [DW05, DW04]. We impose simpler (although slightly weaker) security condition in this scenario, from those considered there, and provide more detail description of the LOPC operations (see also [Chr02]). We require secure states to be close in trace norm to ideal ccq states. This condition is widely used as proved to be *composable* in [BOHL$^+$05b] (See [Ren05] for discussion of this issue, and Remark 4.2).

Let us introduce formally the LOPC scenario. In analogy to classical key agreement scenario, Alice, Bob and Eve are given many systems in the same tripartite state $\rho_{ABE}$, so that each party holds its corresponding subsystem $A$, $B$ and $E$ respectively. On the input states, Alice and Bob are able to perform certain operations. They can process states via quantum operations each in her/his laboratory, and they can communicate publicly, that is send 'classical' messages, whose copies are send also to the eavesdropper Eve. Formally these operations called LOPC are defined as:

**Definition 4.2** *An operation $\Lambda$ belongs to local operations and public communication (LOPC) class if it is a composition of finite number of the following operations:*

*(i) Local Alice (Bob) operations, i.e. operations of the form $\Lambda_A \otimes I_{BE}$ (or $\Lambda_B \otimes I_{AE}$).*

*(ii) Public communication from Alice to Bob (or from Bob to Alice). The process of public communication from Alice to Bob is described by the following map*

$$\Lambda(\rho_{aABE}) = \sum_i P_i \rho_{aABE} P_i \otimes |i\rangle_b\langle i| \otimes |i\rangle_e\langle i| \tag{4.6}$$

*where $P_i = |i\rangle_a\langle i| \otimes \mathrm{I}_{ABE}$, with that from Bob to Alice defined in analogous way.*

In the above definition, the subsystem $a$ carries the message to be sent, and the subsystems $b$ and $e$ of Bob and Eve represent the received message. The state of $AB$ subsystem of an LOPC operation we call its *bipartite output* .

Having provided allowed class of operations, we can describe the goal of the LOPC scenario. The task of Alice and Bob is to distill the maximal possible amount of classical key. More formally, via LOPC operations they try to transform the input state into ideal ccq states $\rho_{ideal}^{ccq}$ with the largest possible subsystem $AB$. Similarly as it is in case of distillation of private states, we will tolerate inaccuracies in this process. More concretely, we will allow to obtain instead of an $\rho_{ideal}^{ccq}$ state, the one which is close in trace norm distance to the latter. Note, that the cryptographical issue is hidden in definition of the LOPC operations: these are operations which gives to Eve a copy of each classical communicate which is exchanged between the honest parties.

Consequently, we adopt the following measure of distillable classical key from a quantum tripartite state:

**Definition 4.3** *For any state $\rho_{ABE} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ let us consider sequence $P_n$ of LOPC protocols such that $P_n(\rho_{ABE}^{\otimes n}) = \beta'_n$, where $\beta'_n$ is ccq state*

$$\beta'_n = \sum_{i,j=0}^{d_n-1} p_{ij} |ij\rangle\langle ij|_{AB} \otimes \rho_{ij}^E \tag{4.7}$$

*from $\mathcal{B}(\mathcal{H}^{(n)}) = B(\mathcal{H}_A^{(n)} \otimes \mathcal{H}_B^{(n)} \otimes \mathcal{H}_E^{(n)})$ with $\dim\mathcal{H}_A^{(n)} = \dim\mathcal{H}_B^{(n)} = d_n$. A set of operations $\mathcal{P} \equiv \cup_{n=1}^{\infty}\{P_n\}$ is called classical key distillation protocol of state $\rho_{ABE}$ if there holds*

$$\lim_{n\to\infty} ||\beta'_n - \beta_{d_n}|| = 0, \tag{4.8}$$

*where $\beta_{d_n} \in B(\mathcal{H}^{(n)})$ is of the form*

$$\beta_{d_n} = \frac{1}{d_n}\left(\sum_{i=0}^{d_n-1} |ii\rangle_{AB}\langle ii|\right) \otimes \rho_n^E, \tag{4.9}$$

*$\rho_n^E$ are arbitrary states from $B(\mathcal{H}_E^{(n)})$. The rate of a protocol $\mathcal{P}$ is given by*

$$\mathcal{R}(\mathcal{P}) = \limsup_{n\to\infty} \frac{\log d_n}{n} \tag{4.10}$$

*Then the distillable classical key of state $\rho_{ABE}$ is defined as supremum of rates*

$$C_D(\rho_{ABE}) = \sup_{\mathcal{P}} \mathcal{R}(\mathcal{P}). \tag{4.11}$$

**Remark 4.2** *Let us note here, that the condition (4.8) which measures an inaccuracy of the output of distillation protocol which we have adopted, is in principle arbitrary. However it has to capture two issues. First, Alice and Bob should have finally almost perfect correlations, that is Bob should have almost the same system as Alice. Second, the final Eve's state should have small correlations with state of Alice and Bob systems so that they would hold a possibly inaccurate but 'almost' secure key. The first condition refers to uniformity, the second one to security. There are several ways of quantifying the correlations between Alice's and Bob's final systems, and some of them are equivalent. In particular, the uniformity condition can be of the following form*

$$|| \sum_{i,j=0}^{d-1} p_{ij}|ij\rangle\langle ij| - \frac{1}{d}\sum_{i=0}^{d-1}|ii\rangle\langle ii||| \leq \epsilon \tag{4.12}$$

*with vanishing $\epsilon$. We focus in this remark on the possible security conditions.*

*To quantify security one can use Holevo function of distilled ccq state [BOHL$^+$05a], namely:*

$$\chi(\rho_{ccq}) \equiv S(\rho_E) - \sum_{i,j=0}^{d-1} p_{ij}S(\rho_{ij}) \leq \epsilon \tag{4.13}$$

*where $S(\rho) = \mathrm{Tr}\rho\log\rho$ denotes von Neumann entropy, and $\rho_E = \sum_{i,j=0}^{d-1} p_{ij}\rho_{ij}$. Alternatively, one can use similar condition based on norm*

$$\sum_{i,j=0}^{d-1} p_{ij}\|\rho_E - \rho_{ij}^E\| \leq \epsilon \tag{4.14}$$

*Relations between the condition from definition above, and security criteria (4.13) and (4.14) as well as with uniformity criterion (4.12) has been established in [HHHO05a], which we will not invoke here.*

### 4.2.1 The worst-case LOPC scenario

The Definition 4.3 works for any input tripartite state $\rho_{ABE}$. However in what follows we will mostly deal with the case were the state $\rho_{ABE} = |\psi\rangle_{ABE}$ is pure, according to the worst case scenario assumed for definition of secure key in Section 3.1.1. As noted in [DW05, DW04], this is the worst case, because having access to the purifying system Eve can transform it into any other *extension* of Alice's and Bob's state $\rho_{AB} = \mathrm{Tr}_E\rho_{ABE}$, which they share for sure, since we assume, that Eve can not have access to their sites. Hence, we call it *worst-case LOPC scenario*.

Being the most important scenario from cryptographic point of view, the worst-case LOPC scenario is at the same time the simplest, as can be described by

means of only *bipartite* states. Indeed, a pure state $|\psi\rangle_{ABE}$ is determined by state $\rho_{AB} = \mathrm{Tr}_E|\psi\rangle_{ABE}$ up to a partial isometry on Eve's system (see Lemma 2.6). We show below (Corollary 4.5), that implementation of partial isometry via quantum operations (see Corollary A.2) does not change the quantity $C_D(\psi\rangle_{ABE})$, hence the latter freedom is not an issue. That is, in context of key distillation, we can consider the state $\rho_{AB}$ as completely determining its purification $|\psi_\rho\rangle_{ABE}$. This allows us to define distillable classical secure key from *bipartite* state $\rho_{AB}$:

**Definition 4.4** *For a bipartite state $\rho_{AB}$, the distillable classical key is given by*

$$C_D(\rho_{AB}) \equiv C_D(|\psi_\rho\rangle_{ABE}), \tag{4.15}$$

*where $|\psi_\rho\rangle_{ABE}$ is a purification of $\rho_{AB}$.*

We show now a general result, that $C_D$ does not decrease under quantum operation on Eve's subsystem. This property is one of the axioms of the so called *secrecy monotones* defined in [CMS02]. We begin with a lemma, which shows that one can in a sense 'commute' the operation on Eve's subsystem through an LOPC operation, getting some new LOPC operation, and new operation on Eve's subsystem.

**Lemma 4.3** *For any tripartite state $\rho_{ABE}$, quantum operation $\Lambda_E$, $\rho'_{ABE'} = \mathrm{I}_{AB} \otimes \Lambda_E(\rho_{ABE})$, and any LOPC operation $P : B(\mathcal{H}_{ABE}) \to B(\mathcal{H}_{\tilde{A}\tilde{B}\tilde{E}})$, there is an LOPC operation $P' : B(\mathcal{H}_{ABE'}) \to B(\mathcal{H}_{\tilde{A}\tilde{B}E''})$ which staisfies:*

$$P'(\rho'_{ABE'}) = \mathrm{I}_{\tilde{A}\tilde{B}e_1\ldots e_m} \otimes \Lambda_E[P(\rho_{ABE})], \tag{4.16}$$

*where $\tilde{E} = e_1 \ldots e_m E$, and $m$ is the number of operations of public communication in some decomposition of $P$ into basic LOPC operations.*

**Proof.** We will define $P'$ as the operation $P$, suitably adapted to system $ABE'$. Operation $P$ is a composition of some local operations and public communication operations. Let $K$ denote the total number of basic operations in its composition, and $m$ the number of operations of public communication. We naturally define $P'$ as a composition of their counterparts defined as follows. Any local operation of $P$ which has form $L \otimes \mathrm{I}_{AE}$ or $L \otimes \mathrm{I}_{BE}$ becomes $L' = L \otimes \mathrm{I}_{AE'}$ and $L' = L \otimes \mathrm{I}_{BE'}$ respectively. The $j$-th operation of public communication becomes $[L^{(c)}]'(\rho_{aABE'}) = \sum_i P_i \rho_{aABE'} P_i \otimes |i\rangle\langle i|_{b_j} \otimes |i\rangle\langle i|_{e_j}$ with $P_i = |i\rangle\langle i|_a \otimes \mathrm{I}_{ABE'e_1\ldots e_{j-1}}$.

To see, that the composition of these operations satisfy (4.16), we apply in parallel basic operations of $P$ and $P'$. After composing first $k$ of them, assuming that $l$ of these $k$ were operations of public communication we see by induction, that:

$$\mathrm{I}_{A_kB_ke_1\ldots e_l} \otimes \Lambda_E[Q_k \circ \ldots \circ Q_1(\rho_{ABE})] = Q'_k \circ \ldots \circ Q'_1[(\mathrm{I}_{AB} \otimes \Lambda_E(\rho_{ABE}))] \tag{4.17}$$

where $0 \leq l \leq k$ and $A_k B_k$ is the system of bipartite output of a composition of $Q_k \circ \ldots \circ Q_1$. We obtain (4.16) for $k = K$.

∎

Using the above lemma we can prove desired theorem which shows that acting on Eve's subsystem can not decrease classical distillable key.

**Theorem 4.4** *For any tripartite state $\rho_{ABE}$, quantum operation $\Lambda_E$ and $\rho'_{ABE'} = \mathrm{I}_{AB} \otimes \Lambda_E(\rho_{ABE})$ there holds:*

$$C_D(\rho_{ABE}) \leq C_D(\rho'_{ABE'}). \tag{4.18}$$

*If additionally there exists $\Lambda'_{E'}$ such that $\mathrm{I}_{AB} \otimes \Lambda'_{E'}(\rho'_{ABE'}) = \rho_{ABE}$, we have $C_D(\rho_{ABE}) = C_D(\rho'_{ABE'})$.*

**Proof.** The idea of the proof is as follows. For any protocol $P$ of distilling classical key from $\rho_{ABE}$ we find its counterpart $P'$ that distills the same amount of classical key from $\rho'_{ABE'}$. $P'$ is an easy adaptation of $P$. It merely differs by the fact, that acts as identity not on $E$ but on system $E'$. Acting on the output $\rho^{out}$ of $P$ with operation $\Lambda_E$ we observe, that such modified output $\rho_1^{out}$ is still secure. Thanks to the fact that operation $\Lambda_E$ commutes with any LOPC protocol, we observe that $P'$ applied to $\rho'_{ABE'}$ (when we first apply $\Lambda_E$ to $\rho_{ABE}$) equals $\rho_1^{out}$ (when we apply first P, and then $\Lambda_E$ to $\rho_1^{out}$). This will give the proof, since $\rho_1^{out}$ is secure. In what follows, we show the main arguments for operations, with that for protocols following the same, yet with the input state $\rho^{\otimes n}$.

Consider any operation $P$ which on $\rho_{ABE}$ gives some $\rho^{out}_{\tilde{A}\tilde{B}\tilde{E}}$ wich satisfies:

$$||\rho^{out}_{\tilde{A}\tilde{B}\tilde{E}} - \sigma^{ccq}_{ideal}|| \leq \epsilon, \tag{4.19}$$

for some ideal ccq state $\sigma^{ccq}_{ideal} = \frac{1}{d}\sum_{i=0}^{d-1} |ii\rangle\langle ii| \otimes \rho_{\tilde{E}}$. By Lemma 4.3, there is an operation $P'$ which satisfies

$$P'(\rho') = \Lambda'(\rho^{out}). \tag{4.20}$$

with $\Lambda'$ acting on $\tilde{A}\tilde{B}$ as identity operation. Let us apply then $\Lambda'$ to both states in (4.19). Since trace norm does not increase under quantum operations, resulting states satisfy:

$$||\rho_1^{out} - \hat{\sigma}^{ccq}_{ideal}|| \leq \epsilon. \tag{4.21}$$

where $\rho_1^{out} = \Lambda'(\rho^{out})$ and $\hat{\sigma}^{ccq}_{ideal}$ is some other ideal ccq state.

From (4.20), and the above inequality we have:

$$||P'(\rho') - \hat{\sigma}^{ccq}_{ideal}|| \leq \epsilon. \tag{4.22}$$

Now, since $\Lambda'$ does not change a state of $\tilde{A}\tilde{B}$ system, $\hat{\sigma}^{ccq}_{ideal} = \frac{1}{d}\sum_{i=0}^{d-1} |ii\rangle\langle ii| \otimes \rho'_{\tilde{E}}$ for some state $\rho'_{\tilde{E}}$ on Eve's site. This means, that there is an LOPC operation $P'$ which acting on $\rho'$ yields an output state with the same amount of security.

To summarise, for any operation $P$ which on $\rho$ outputs a state close to an ideal *ccq* state with $d \times d$ dimensional $AB$ subsystem, there is an operation $P'$ which on $\rho'$ outputs a state close to some other ideal *ccq* with $AB$ subsystem of the same dimension. Using this fact and the method shown in proof of Theorem 4.12, one easily obtains the same for protocols of key distillation and in turn that $C_D(\rho_{ABE}) \leq C_D(\rho'_{ABE'})$.

The second thesis of this theorem is now immediate. If there exists an inverse operation $\mathrm{I}_{AB} \otimes \Lambda'_{E'}$, we can repeat the above reasoning starting from $\rho'_{ABE'}$ and with $\Lambda'_{E'}$ in place of $\Lambda_E$. This gives $C_D(\rho_{ABE}) \geq C_D(\rho'_{ABE'})$, which together with the converse inequality that holds due to the above considerations, gives desired equality. ∎

From the above theorem we have immediate corollary, which justifies Definition 4.4.

**Corollary 4.5** *For any two purifications $|\psi_\rho\rangle \in \mathcal{H}_{ABE}$ and $|\phi_\rho\rangle \in \mathcal{H}_{ABE'}$ of a bipartite state $\rho_{AB}$ there is*

$$C_D(|\psi_\rho\rangle) = C_D(|\phi_\rho\rangle) \tag{4.23}$$

**Proof.** By Lemma 2.6, there exist a partial isometry $F : \mathcal{H}_E \to \mathcal{H}'_E$ which transforms $|\psi_\rho\rangle_{ABE}$ into $|\phi_\rho\rangle_{ABE'}$. Let w.l.g. $F$ be an isometry (assuming partial isometry uses similar argument). There is then a partial isometry $G : \mathcal{H}'_E \to \mathcal{H}_E$ which transforms $|\phi_\rho\rangle_{ABE'}$ in to $|\psi_\rho\rangle_{ABE}$, hence we can apply Theorem 4.4 with $F = \Lambda$ and $G = \Lambda'$.

## 4.3 Equality of key rates in LOCC and worst-case LOPC scenarios

In this section we will show that Definitions 4.1 and 4.4 give rise to the same quantities. In this way the problem of drawing key within worst-case LOPC scenario is recast in terms of transition to a desired state by LOCC, that is within LOCC scenario.

We show this proving two relations. First, if Alice and Bob can get via LOPC operation an ideal ccq state, there is an LOCC operation which would give them a private state with the same amount of security. Second, if Alice and Bob can obtain via some LOCC operation a private state, there is an LOPC operation which would give them an ideal ccq state with the same amount of security.

As described in Section 4.3.2, it is relatively easy to achieve the first relation. To achieve the second, in Section 4.3.1, we first need to consider *coherent* LOPC operations (CLOPC)(cf. [HHH01, DW05]). Basing on the coherent version of an LOPC operation, we build a desired LOCC operation. The coherent LOPC operation will be a composition of coherent basic LOPC operations. Whenever the LOPC operation would trace out some system when implemented via basic quantum operations, its coherent counterpart just *puts* such system *aside*. All systems that are put aside in such implementation of coherent LOPC operation, contribute to systems of *local trash bins*. These local trash bins will form a shield of a private state, in desired LOCC operation (Section 4.3.2).

The relations between the LOCC and LOPC operations induces natural relations between the LOCC and LOPC key distillation protocols respectively. This enables us to derive in Section 4.3.3 the equivalence in exact case (where protocols produce as an output exactly ideal ccq states or exactly pdits). Subsequently, in Section 4.3.3 we will turn to the general case where inexact transformations are allowed. We sketch here briefly the idea of the main result of this section.

### 4.3.1 Coherent LOPC operations

In what follows by $R_{\mathcal{A}}$ and $R_{\mathcal{B}}$ we mean the trash bin systems on Alice's and Bob's site respectively. We recall also, that by convention (see Section 2.3.7), the CLOPC operations will act on states $\rho_{ABR_AR_BE}$. Each basic LOPC operation will (instead of tracing out) put some system aside enlarging the system $R_{\mathcal{A}}$ or $R_{\mathcal{B}}$ depending on which site it is realized in case of local operations, or from which site the public communication operation is performed.

We now define basic coherent LOPC operations.

**Coherent local operations**

For any input state $\rho_{ABR_{\mathcal{A}}R_{\mathcal{B}}E}$, a local operation $\Lambda_{AR_{\mathcal{A}}} \otimes \mathrm{I}_{BR_{\mathcal{B}}E}$ on Alice's site, the coherent local operation $\Lambda_{AR_{\mathcal{A}}}$, has form:

$$(\Lambda_{AR_{\mathcal{A}}} \otimes \mathrm{I}_{BR_{\mathcal{B}}E})^{coh}, \tag{4.24}$$

according to Example 2.13 and Definition 2.5. That is when $\Lambda_{AR_{\mathcal{A}}}$ is implemented via adding ancillary state $|0\rangle\langle 0|_S$, performing $U_{AS}$ and tracing out subsystem $R'$ of $AR$, the operation (4.24) acts on state $\rho$ of systems $ABR_{\mathcal{A}}R_{\mathcal{B}}E$ as

$$PA_{R'}[U_{AS} \otimes \mathrm{I}\,(\rho \otimes |0\rangle\langle 0|_S)\, U_{AS}^{\dagger} \otimes \mathrm{I}], \tag{4.25}$$

where $PA$ means putting the system $R'$ aside, so that it becomes subsystem of $R_{\mathcal{A}}$, and identity operation is performed on systems $R_{\mathcal{A}}BR_{\mathcal{B}}E$.

**Coherent public communication**

Coherent version of process of public communication from Alice to Bob is performing special operation $\Lambda$ and putting aside appropriate system: $\Lambda$ acts on $\rho_{aABR_AR_BE} \in B(\mathcal{H}_a \otimes \mathcal{H}_{AB} \otimes \mathcal{H}_{R_AR_B} \otimes \mathcal{H}_E)$ as follows:

$$\Lambda(\rho_{aAR_ABR_BE}) = U(\rho_{aABR_AR_BE} \otimes |0\rangle\langle 0|_{Anc} \otimes |0\rangle_b\langle 0| \otimes |0\rangle_e\langle 0|)U^\dagger \tag{4.26}$$

where

$$U = I_{ABR_AR_BE} \otimes \sum_i |i\rangle_a\langle i| \otimes U^{(i)}_{Anc} \otimes U^{(i)}_b \otimes U^{(i)}_e \tag{4.27}$$

with unitary transformation $U^{(i)}_x$ satisfying $U^{(i)}_x|0\rangle = |i\rangle_x$ for $x \in \{Anc, b, e\}$. The system $Anc$ is put aside, that is put to Alice's trash bin $R_A$. The coherent operation of classical communication from Bob to Alice we define in analogous way.

**Coherent LOPC operation**

Similarly as for LOPC operations, the CLOPC operation is a composition of basic coherent LOPC operations, according to the rule of composing coherent operations. As for general operations, relating a CLOPC operation with the LOPC operation $\Lambda$ from which it originates, we will denote it as $\Lambda^{coh}$. If the output of $\Lambda^{coh}$ is $\rho'_{ABR_\mathcal{A}R_\mathcal{B}E}$, then the state of the subsystem $ABR_\mathcal{A}R_\mathcal{B}$ we call the *bipartite output of coherent LOPC operation*.

Applying now Observation 2.12 we have the following corollary:

**Corollary 4.6** *The CLOPC operation $\Lambda^{coh} : B(\mathcal{H}_{AB} \otimes \mathcal{H}_{R_\mathcal{A}R_\mathcal{B}} \otimes \mathcal{H}_{\tilde{E}}) \to B(\mathcal{H}_{\tilde{A}\tilde{B}} \otimes \mathcal{H}_{R_\mathcal{A}R_\mathcal{B}} \otimes \mathcal{H}_E)$ has the following two features:*

*(i) On input pure state, outputs a pure state.*

*(ii) For any tripartite state $\rho_{ABE}$, $\mathrm{Tr}_{R_\mathcal{A}R_\mathcal{B}}\Lambda^{coh}(\rho_{ABE}) = \Lambda(\rho_{ABE})$, where by convention (see Section 2.3.7), $\rho_{ABE} = \rho_{ABR_\mathcal{A}R_\mathcal{B}E}$ where systems $R_\mathcal{A}$ and $R_\mathcal{B}$ are Alice's and Bob's trash bins initially empty.*

∎

### 4.3.2 Switching between LOCC and (coherent) LOPC operations

In this section, in Theorem 4.7 we show that for any CLOPC operation there is an LOCC one with the same (bipartite) output. We then prove, also in Theorem 4.8, that for any LOCC operation there is an LOPC operation with the same bipartite output as that of LOCC.

**From coherent LOPC to LOCC operations**

To link the LOCC operation with a given CLOPC one, we define the basic LOCC operations that will correspond to coherent LOPC operations.

We first provide a general fact, that links basic coherent LOPC with LOCC operations. Owing to this fact, the relation of LOCC operations with coherent LOPC operations is straightforward.

**Lemma 4.7** *For any coherent basic LOPC operation* $\Lambda_P : B(\mathcal{H}_{AB}\otimes\mathcal{H}_{R_\mathcal{A}R_\mathcal{B}}\otimes\mathcal{H}_E) \to B(\mathcal{H}_{\tilde{A}\tilde{B}} \otimes \mathcal{H}_{R_\mathcal{A}R_\mathcal{B}} \otimes \mathcal{H}_{\tilde{E}})$*, there is an LOCC operation* $\Lambda_Q : B(\mathcal{H}_{AB} \otimes \mathcal{H}_{R_\mathcal{A}R_\mathcal{B}}) \to B(\mathcal{H}_{\tilde{A}\tilde{B}} \otimes \mathcal{H}_{R_\mathcal{A}R_\mathcal{B}})$*, such that for any state* $\rho_{ABR_\mathcal{A}R_\mathcal{B}} \in B(\mathcal{H}_{AB} \otimes \mathcal{H}_{R_\mathcal{A}R_\mathcal{B}})$ *and its any purification* $|\psi_\rho\rangle_{ABR_\mathcal{A}R_\mathcal{B}E} \in \mathcal{H}_{AB} \otimes \mathcal{H}_{R_\mathcal{A}R_\mathcal{B}} \otimes \mathcal{H}_E$*, there holds:*

$$\mathrm{Tr}_{\tilde{E}}\Lambda_P(|\psi_\rho\rangle) = \Lambda_Q(\rho). \tag{4.28}$$

**Proof.** Consider the first coherent local operation, on Alice's site. It is of the form:

$$\Lambda_P = (\Lambda_{AR_\mathcal{A}} \otimes \mathrm{I}_{BR_\mathcal{B}} \otimes \mathrm{I}_E)^{coh}, \tag{4.29}$$

specified in (4.25). With this operation we associate the LOCC operation of the form:

$$\Lambda_Q = (\Lambda_{AR_\mathcal{A}} \otimes \mathrm{I}_{BR_\mathcal{B}})^{coh}, \tag{4.30}$$

which we specify in analogy to (4.25), according to rule given in Example (2.13).

Since $\Lambda_P$ acts on the system $E$ as identity, by Observation 2.11, the dependence (4.28) holds in this case, with the same for $\Lambda_Q$ on Bob's site defined analogously.

Consider now the operation of coherent public communication from Alice to Bob $\Lambda_P^{(c)}$, which acts as:

$$\Lambda_P^{(c)}(|\psi_\rho\rangle_{aABR_\mathcal{A}R_\mathcal{B}E}) = U(|\psi_\rho\rangle_{aABR_\mathcal{A}R_\mathcal{B}E} \otimes |0\rangle\langle 0|_{Anc} \otimes |0\rangle_b\langle 0| \otimes |0\rangle_e\langle 0|)U^\dagger \tag{4.31}$$

where

$$U = I_{ABR_\mathcal{A}R_\mathcal{B}E} \otimes \sum_{i=0}^{\dim\mathcal{H}_a-1} |i\rangle_a\langle i| \otimes U_{Anc}^{(i)} \otimes U_b^{(i)} \otimes U_e^{(i)} \tag{4.32}$$

with unitary transformation $U_x^{(i)}$ satisfying $U_x^{(i)}|0\rangle = |i\rangle_x$ for $x \in \{Anc, e, b\}$, so that $U$ copies the state of system $a$ into systems $x$. It also putts $Anc$ aside, forming Alice's trash bin i.e. makes $Anc$ to be subsystem of a trash bin $R_\mathcal{A}$. Hence, the output of $\Lambda_P^{(c)}$ yields equivalently:

$$\Lambda_P^{(c)}(|\psi_\rho\rangle_{aABR_\mathcal{A}R_\mathcal{B}E}) = U(|\rho\rangle_{aABR_\mathcal{A}R_\mathcal{B}E} \otimes |0\rangle\langle 0|_{R_\mathcal{A}} \otimes |0\rangle_b\langle 0| \otimes |0\rangle_e\langle 0|)U^\dagger. \tag{4.33}$$

For this operation, we define the LOCC operation $\Lambda_Q^{(c)}$, which acts as:

$$\Lambda_Q^{(c)}(\rho_{aABR_{\mathcal{A}}R_{\mathcal{B}}}) = \sum_{i=0}^{\dim\mathcal{H}_a-1} P_i(\rho_{aABR_{\mathcal{A}}R_{\mathcal{A}}})P_i \otimes |i\rangle\langle i|_b \otimes |i\rangle\langle i|_{Anc}, \tag{4.34}$$

with $P_i = |i\rangle\langle i|_a \otimes \mathrm{I}_{AB}$, where, by $\rho_{aABR_{\mathcal{A}}R_{\mathcal{B}}}$ we mean the $\mathrm{Tr}_E|\psi_\rho\rangle\langle\psi_\rho|_{aABR_{\mathcal{A}}R_{\mathcal{B}}E}$. Following coherent operation, $\Lambda_Q^{(c)}$ puts the system *Anc* aside. Note, that $\Lambda^{(c)}$ is operation of classical communication, composed with local operation which copies the result of measurement performed on $a$ to system *Anc*.

Taking general input state, and performing partial trace over $\tilde{E}$ we easily obtain that $\Lambda_P^{(c)}$ and $\Lambda_Q^{(c)}$ satisfy (4.28). Analogously we obtain the result for operation of public communication from Bob to Alice, which proves the assertion ∎

The above lemma allows us to state the following theorem:

**Theorem 4.8** *For any bipartite state $\rho \in B(\mathcal{H}_{ABR_{\mathcal{A}}R_{\mathcal{B}}})$, its any purification $|\psi_\rho\rangle \in \mathcal{H}_{ABR_{\mathcal{A}}R_{\mathcal{B}}} \otimes \mathcal{H}_E$, and any CLOPC operation $P$, with output in $B(\mathcal{H}_{\tilde{A}\tilde{B}R_{\mathcal{A}}R_{\mathcal{B}}} \otimes \mathcal{H}_{\tilde{E}})$ there is an LOCC operation $Q$ with the output in $B(\mathcal{H}_{\tilde{A}\tilde{B}R_{\mathcal{A}}R_{\mathcal{B}}})$, such that*

$$Q(\rho) = \mathrm{Tr}_E P(|\psi_\rho\rangle). \tag{4.35}$$

**Proof.** $P$ is a composition of basic CLOPC operations. For each such operation $\Lambda_P$ we know by Corollary 4.6 (i), that if applied to $|\psi_\rho\rangle$ yields some tripartite pure state $|\phi\rangle_{\tilde{A}\tilde{B}R_{\mathcal{A}}R_{\mathcal{B}}\tilde{E}}$. By Lemma 4.7, this state has subsystem $\tilde{A}\tilde{B}R_{\mathcal{A}}R_{\mathcal{B}}$ equal to output of the corresponding LOCC operation $\Lambda_Q(\rho)$. Hence $|\phi\rangle_{\tilde{A}\tilde{B}R_{\mathcal{A}}R_{\mathcal{B}}\tilde{E}}$ is a purification of $\Lambda_Q(\rho)$, and we can apply to this pair of states recursively Lemma 4.7, to obtain that for a composition of basic CLOPC operations, there is corresponding LOCC operation which has the same bipartite output. By induction we obtain the thesis for general CLOPC operation. ∎

### From LOCC operations to LOPC ones

We observe now, a similar statement, that with given LOCC operation connects an LOPC one. In short, the result states, that for an LOCC operation which transforms $\rho$ into $\sigma$, there is an LOPC operation which transforms extension of $\rho$ into some extension of $\sigma$. For brevity, with a little abuse of notation, we will say that the LOPC operation has the output in $B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ instead of $B(\mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'} \otimes \mathcal{H}_E)$, that actually takes place in accordance with Def. 4.2.

**Theorem 4.9** *For any LOCC operation $Q : B(\mathcal{H}_A \otimes \mathcal{H}_B) \to B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$, there is an LOPC operation $P : B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{\tilde{E}}) \to B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes$*

$\mathcal{H}_{B'} \otimes \mathcal{H}_E$), *such that for any bipartite state* $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ *and its any extension* $\rho_{AB\tilde{E}} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{\tilde{E}})$, *there holds:*

$$Q(\rho)_{ABA'B'} = \mathrm{Tr}_E P(\rho_{AB\tilde{E}}) \tag{4.36}$$

**Proof.** We first show the thesis for basic operations. We consider the operations performed by Alice, with that for Bob along similar lines. With a local LOCC operation $\Lambda_A$ on Alice's system we associate analogous one, but defined on tripartite states via identity operation on system of Eve: $\Lambda_A \otimes \mathrm{I}_B \otimes \mathrm{I}_{\tilde{E}}$. By Observation 2.11, we have that the state on $AB$ after applying $\Lambda_A$ is the same as bipartite output of this LOPC operation.

Second, with an LOCC operation of classical communication $\Lambda_Q^{(c)}$, we associate its natural tripartite counterpart, which is acting on a state as quantum measurement with classical results on Bob's and Eve's systems:

$$\Lambda_P^{(c)}(\rho_{aAB\tilde{E}}) = \sum_i P_i \rho_{aAB\tilde{E}} P_i \otimes |i\rangle_b\langle i| \otimes |i\rangle_e\langle i| \tag{4.37}$$

where $P_i = |i\rangle_a\langle i| \otimes \mathrm{I}_{AB\tilde{E}}$. To see equality (4.36) it is straightforward to consider matrix of an arbitrary input state $\rho_{aAB\tilde{E}}$, compute $\Lambda_P^{(c)}(\rho_{aAB\tilde{E}})$ and tracing over $E = \tilde{E}e$ to obtain desired state $\Lambda_Q^{(c)}(\rho_{aAB\tilde{E}})$.

Consider now general LOCC operation. It is a finite composition of basic operations. Due to the above reasoning, output of a basic LOPC operation is an extension of the output of the corresponding basic LOCC operation. We can apply then recursively the above reasoning to these states, and obtain that composition of two basic operations also satisfy the thesis. Hence, the induction argument proves the theorem for general LOCC operation. ∎

### 4.3.3 Equality of key rates in LOCC and worst-case LOPC scenario

In this section we show that the distillable key of a quantum bipartite state $\rho_{AB}$ and classical distillable key of $\rho_{AB}$ are equal. We do this in three steps. Just to describe the idea, we prove this fact for special states which have *exactly* distillable key, that is from which one can obtain exactly a private state via LOCC operations, or exactly an ideal *ccq*-state via LOPC operations (Observation 4.10). We then show that the non-exact operations yield equivalent results (Theorem 4.11), and basing on this finally show in Theorem 4.12, that $K_D(\rho_{AB}) = C_D(\rho_{AB})$ for an arbitrary bipartite quantum state.

### The case of exact key

Here we will consider the ideal case, where the distillation of the key gives *exactly* the demanded output state. Formal definition of exactly distillable classical key, denoted as $C_D^{exact}$, is just Definition 4.3, with $\beta'_n = \beta_{d_n}$ in place of $\lim_{n\to\infty} ||\beta'_n - \beta_{d_n}|| = 0$, restricted to pure input state $\rho_{ABE}$, as in Definition 4.4. Similarly, definition of exactly distillable private states denoted as $K_D^{exact}$ is just Definition 4.1 of distillable private states with $\sigma_n = \gamma^{(d_n)}$ in place of $\lim_{n\to\infty} ||\sigma_n - \gamma_{d_n}|| = 0$. We have then the following observation:

**Observation 4.10** *For any $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ there holds:*

$$K_D^{exact}(\rho_{AB}) = C_D^{exact}(\rho_{AB}) \tag{4.38}$$

**Proof.** We give the proof for operations, with the one for protocols following directly from the latter. If after LOPC operation $\Lambda$ applied to purification of $\rho$, Alice and Bob obtain exactly $d \times d$ ccq state (4.9):

$$\beta_{d_n} = \left( \sum_{i=0}^{d_n - 1} \frac{1}{d_n} |ii\rangle_{AB}\langle ii| \right) \otimes \rho_n^E, \tag{4.39}$$

then the bipartite output of its coherent application $\Lambda^{coh}$ due to Corollary 4.6 (ii) and Theorem 3.2 will be a pdit of the same dimension of its key part. Now, by Theorem 4.8, there is an LOCC operation $Q$ with output equal to the bipartite output of $\Lambda^{coh}$. If we consider such operation acting on many copies of an input state, we get analogous result for protocols of distilling classical key and pdits, which proves $C_D(\rho)^{exact} \leq K_D^{exact}(\rho)$.

Conversely, let Alice and Bob can get from $\rho$ via LOCC operation a pdit, that is secure in some basis $\mathcal{B}$. Then by Theorem 4.9 there is an LOPC operation which applied to purification of $\rho$ ends with some extension $\rho_{ABA'B'E}$ of the pdit. Let us purify now this extension to some system $E'$. By Theorem 3.2, the state $\rho_{ABEE'}$ after von Neumann measurement in basis $\mathcal{B}$ on AB is an ideal ccq state (4.9) of the same dimension of $AB$ as the shield of a pdit. If we trace out the system $E'$, we get the state which is also an ideal ccq state. This state can be obtained by LOPC operations, as we have just argued. Hence, possibility of distilling exact pdit implies possibility of distilling a ccq state with the same dimension of the $AB$ subsystem. Applying this result for many copies we get $K_D^{exact}(\rho) \leq C_D^{exact}(\rho)$, which ends the proof of this theorem. ∎

**Distillation of classical key and distillation of pdits from bipartite states - equivalence in general (asymptotically exact) case**

We will prove in this section, that even in non exact case, distillation of pdits from initial bipartite state via LOCC operations, is equivalent to distillation of key by LOPC operations from initial pure state, which is purification of the bipartite state. We first show a general fact for operations (Theorem 4.11) and in turn argue the same for protocols in Theorem 4.12 which states that the maximal achievable rates in both scenarios are equal.

**Theorem 4.11** *Let Alice and Bob share a bipartite state $\rho$ and let Eve has it's purifying system. Then the following holds: if Alice and Bob can obtain by LOPC operation a state such that with Eve's subsystem it is of the form*

$$\rho_{ABE}^{ccq} = \sum_{i,j=1}^{d} p_{ij}|ij\rangle\langle ij|_{AB} \otimes \rho_{ij}^{E}, \tag{4.40}$$

*with $||\rho_{ABE}^{ccq} - \rho_{ideal}^{ccq}|| \leq \epsilon$, then by some LOCC operation they can obtain a state $\rho_{out}$ which is close to some pdit state $\gamma$ in trace norm:*

$$||\rho_{out} - \gamma|| \leq 2\sqrt{\epsilon}, \tag{4.41}$$

*where the key part of a pdit $\gamma$ is of dimension $d \times d$.*
*Conversely, if by LOCC they can obtain state $\rho_{out}$ satisfying $||\rho_{out} - \gamma|| \leq \epsilon$, then by LOPC operation they can obtain state $\rho_{ccq}$ satisfying $||\rho_{ABE}^{ccq} - \rho_{ideal}^{ccq}|| \leq 2\sqrt{\epsilon}$.*
**Proof.** ($\Rightarrow$) By assumption Alice and Bob are able to get by some LOPC operation $\Lambda_P$ a ccq state $\rho_{ABE}$ satisfying

$$||\rho_{ABE}^{ccq} - \rho_{ideal}^{ccq}|| \leq \epsilon. \tag{4.42}$$

Now by equivalence of norm and fidelity (Lemma (2.20)) we can rewrite this inequality as follows

$$F(\rho_{ABE}^{ccq}, \rho_{ideal}^{ccq}) > 1 - \frac{1}{2}\epsilon. \tag{4.43}$$

Consider now a purification $|\psi_\rho\rangle_{ABA'B'E}$ of $\rho_{ABE}^{ccq}$, which is the output of coherent application of the operation $\Lambda_P$, denoted as $\Lambda_P^{coh}$. In case there was $\dim A'B' < \dim ABE$ we assume without loose of generality, that the operation $\Lambda_P^{coh}$ is followed by adding a state $|0\rangle$ of proper dimension, to systems $A'$ and $B'$ to assure $\dim A'B' \geq \dim ABE$. The composition of $\Lambda_P^{coh}$ and enlarging $A'B'$ we also denote as $\Lambda_P^{coh}$. Now, by Lemma 2.22, we have:

$$F(\rho_{ABE}^{ccq}, \rho_{ideal}^{ccq}) = \max_{|\phi\rangle} |\langle\psi_\rho|\phi\rangle|, \tag{4.44}$$

where maximum is taken over purification $|\phi\rangle$ of $\rho^{ccq}_{ideal}$ to system $A'B'$. By the above equation and Eq. 4.43, there exists a purification $|\phi_{ideal}\rangle_{ABA'B'E}$ of $\rho^{ccq}_{ideal}$ such that it's fidelity with $|\psi_\rho\rangle$ is greater than $1-\frac{1}{2}\epsilon$. Since the fidelity can only increase after partial trace applied to both the states, it will be still greater than $1-\frac{1}{2}\epsilon$ once we trace over Eve's subsystem. Thus we have

$$F(\rho^{\psi}_{ABA'B'}, \sigma^{\phi}_{ABA'B'}) > 1 - \frac{1}{2}\epsilon. \tag{4.45}$$

where $\sigma^{\phi}_{ABA'B'}$ and $\rho^{\psi}_{ABA'B'}$ are partial traces over system $E$ of $|\phi_{ideal}\rangle$ and $|\psi_\rho\rangle$ respectively.

The state $\sigma^{\phi}_{ABA'B'}$ comes from purification of an ideal state, and by the very definition it is some pdit state with key part of dimension $\dim AB = d \times d$. At the same time, the state $\rho^{\psi}_{ABA'B'}$ is the one which is the output of $\Lambda^{coh}_P$. Thus by a CLOPC operation ($\Lambda^{coh}_P$ composed with adding local pure states $|0\rangle$ if needed) Alice and Bob can obtain state close to pdit.

Now, by Theorem 4.8, there exists an LOCC operation $\Lambda_Q$ which acting on $\rho$ has the same output as bipartite output of $\Lambda^{coh}_P$. In turn, by LOCC operation, Alice and Bob can obtain a state which is close to pdit in terms of fidelity. This by Lemma 2.20, implies desired formula in terms of trace norm distance, which ends the proof of the implication ($\Rightarrow$).

($\Leftarrow$) This time we assume that there exists an LOCC operation which acting on state $\rho$ ends up with a state $\rho_{out}$ with main part of $d \times d$ dimension which is close to some pdit in trace norm:

$$||\rho_{out} - \gamma|| \leq \epsilon. \tag{4.46}$$

Due to equivalence between fidelity and norm (2.20), we have

$$F(\rho_{out}, \gamma) \geq 1 - \epsilon/2 \tag{4.47}$$

By Theorem 4.9, there is an LOPC operation which acting on $|\psi_\rho\rangle$ gives an extension $\rho^{ext}_{out}$ of $\rho_{out}$ to system $E$. Let us purify this extension to system $E'$. We can assume without loss of generality[1], that $\dim EE' \geq \dim AB$. This purification is also a purification of $\rho_{out}$, which we denote as $|\psi\rangle$. By Lemma 2.22, we can find such $|\phi\rangle$, a purification of $\gamma$ to $EE'$, that $F(|\psi\rangle, |\phi\rangle) > 1 - \epsilon/2$. Now if Alice and Bob measure the key part and trace out the shield, out of $|\psi\rangle$ they get some ccq state $\rho^{ccq}_{out}$ on systems $ABEE'$. The same operation applied to $|\phi\rangle$ gives the ideal ccq state $\rho^{ccq}_{ideal}$ (4.9). Finally let us trace out system $E'$. This operation changes the state $\rho^{ccq}_{out}$ into a state $\sigma^{ccq}_{out}$ that is achievable via LOPC operation, and yields from $\rho^{ccq}_{ideal}$ another

[1]This is because if it is not the case, we can enlarge $E'$ adding a pure state $|0\rangle$ from a properly large Hilbert space.

ideal ccq state $\sigma^{ccq}_{ideal}$. All those operations (measurement and partial traces) can only increase the fidelity, so that

$$F(\sigma^{ccq}_{out}, \sigma^{ccq}_{ideal}) \geq 1 - \epsilon/2 \tag{4.48}$$

Returning to trace norm distance we get

$$||\sigma^{ccq}_{out} - \sigma^{ccq}_{ideal}|| \leq 2\sqrt{\epsilon}. \tag{4.49}$$

∎

Owing to the above theorem we can finally state the main result of this section.

**Theorem 4.12** *For every $\rho \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$, there holds $K_D(\rho) = C_D(\rho)$.*
**Proof.** The proof amounts to straightforward application of Theorem 4.11. Similarly as in case of exact distillation we need to prove two inequalities. We will show only $K_D(\rho) \geq C_D(\rho)$ with the second inequality following along similar lines.

Let us consider the value $C_D(\rho)$. By Definition 4.3, for any fixed $\delta > 0$ there is a classical key distillation protocol $\mathcal{P}_r$, with rate $r$ such that $C_D(\rho) - \delta < r$. That is, by definition of key distillation protocol, that for every $\epsilon > 0$, for every sufficiently high $n > n_0$ there is some LOPC operation $P^\delta_n$ such that:

$$||P^\delta_n(|\psi_\rho\rangle^{\otimes n}) - \beta_{d_n}|| \leq \epsilon. \tag{4.50}$$

By Theorem 4.11, there is an LOCC operation $Q^\delta_n$ such that

$$||Q^\delta_n(\rho^{\otimes n}) - \gamma^{d'_n}|| \leq 2\sqrt{\epsilon}, \tag{4.51}$$

with $d'_n = d_n$. Hence, we obtain that $Q^r_\delta := \{Q^\delta_n\}^\infty_{n=1}$ where $Q^\delta_n$ for $n \leq n_0$ are choosen w.l.g. to be an identity operations, satisfies

$$\lim_{n\to\infty} ||Q^\delta_n(\rho^{\otimes n}) - \gamma^{d'_n}|| = 0. \tag{4.52}$$

From Definition 4.3, there is also a subsequence $k(n)$, such that

$$\lim_{k(n)\to\infty} \frac{\log d_{k(n)}}{k(n)} = r. \tag{4.53}$$

Since $d'_n = d_n$, the same subsequence gives us $\limsup_{n\to\infty} \frac{\log d'_{k(n)}}{k(n)} = r$. Thus, by Definition 4.1 the set $Q^r_\delta$ is a legitimate pdit distillation protocol, with rate $r$. Since $\delta$ was fixed arbitrarily, we have

$$\forall_{\delta>0}\, \exists_{Q^r_\delta}\ r > C_D(\rho) - \delta. \tag{4.54}$$

By definition of $K_D$ and the above inequality there is

$$\forall_{\delta>0}\, K_D(\rho) \geq C_D(\rho) - \delta. \tag{4.55}$$

Taking infimum over $\delta$ we obtain $K_D(\rho) \geq C_D(\rho)$ for every input state $\rho$. This ends the proof of this theorem. ∎

## 4.4 Distillable key is an entanglement measure - advantages of entanglement approach

It is easy to see, that $K_D$ is an operational entanglement measure. From Definition of $K_D$ (Def. 4.1), it follows that $K_D$ is monotoneous in usual sense (can not be increased by LOCC operations), as well as in strong sense (see Section 2.8.1). More precisely $K_D$ can not be increased (even on average) by means of LOCC operations. It is also easy to see that $K_D$ vanishes on separable states (see the properties of $K_D$ below, and discussion in Section 4.6.1). These two features proves that according to (Def. 2.15), $K_D$ is an entanglement measure. Recall, that $K_D$ is *operational* entanglement measure, because it is defined by a task of reaching some target states (private states in this case) by means of LOCC operations in parallel to definition of $E_D$ (see introduction to Section 2.8, and in Section 2.8.2)

The main advantage for quantum cryptography which follows from the fact, that $K_D$ is entanglement measure, is that to study its properties, one can employ tools that have been worked out in domain of entanglement theory[2]. In particular, there is a list of features which entanglement measures may satisfy. Some of them we have presented in Section 2.8.1. Distillable key $K_D$ defined in [HHHO05a], it has been studied as entanglement measure by Matthias Christandl in [Chr02]. For complete presentation, we quote some of main axioms of entanglement measures which are (or not) satisfied by $K_D$. Some of them has been either proved, or just collected as easy properties in [Chr02]. Some of the axioms are formulated for all bipartite states, but till now are known to hold only for some of them. In Sections 4.4.2 and 4.4.2 we enlarge the family of states on which $K_D$ is known to be asymptotically continuous and convex.

### 4.4.1 Which axioms of entanglement measures are satisfied by distillable key ?

We quote now the list given in [Chr06]. By convention, we first quote the acronym, with added 'Not' if the property of entanglement measure does not hold, and a question mark, if it is not known weather it holds. We also append the results of [CEH$^+$07, HHHO05c], and describe then original contribution to this subject.

1. (Norm): equals $\log d$ for maximally entangled states from $MS^{(d)}$.
2. (Van Sep): $K_D(\sigma) = 0$ for $\sigma \in SEP$.

[2]Of course, the are at least that many, and seemingly even more advantages, which this fact gives for entanglement theory. The interrelation between the two domains will be presented in concluding Chapter 7.

3. (strong LOCC Mon): $K_D(\sum_i p_i\rho_i) \leq K_D(\rho)$ where $\rho$ is transformed into $\rho_i$ with probability $p_i$ by $\Lambda \in LOCC$.

4. Not(PPT Mon): not monotoneous under PPT operations

5. ?(As Cont): asymptotic continuity: is there $c, c' \geq 0$, such that for all $\rho, \sigma$ with $D(\rho, \sigma) \leq \epsilon$,
$$|K_D(\rho) - K_D(\sigma)| \leq c\epsilon \log d + c' \,? \tag{4.56}$$

6. (As Cont Pure) [Chr06]: $K_D$ is asymptotically continuous on pure bipartite states: there is $c, c' \geq 0$, such that if $D(|\psi\rangle, |\phi\rangle) \leq \epsilon$, then
$$|K_D(|\psi\rangle\langle\psi|) - K_D(|\phi\rangle\langle\phi|)| \leq c\epsilon \log d + c'. \tag{4.57}$$

7. ?(Conv) Is it that for all $\rho, \sigma$ and $p \in [0, 1]$ there holds
$$pK_D(\rho) + (1-p)K_D(\sigma) \geq K_D(p\rho + (1-p)\sigma) \,? \tag{4.58}$$

8. (Conv Pure) [Chr06]: convex on pure states: for any pure ensamble $(p_i, |\psi_i\rangle)$ of some bipartite state $\rho$,
$$\sum_i p_i K_D(|\psi_i\rangle\langle\psi_i|) \geq K_D(\rho). \tag{4.59}$$

9. (Strong Super Ad): is strongly super additive: for all $\rho_{ABA'B'}$,
$$K_D(\rho_{ABA'B'}) \geq K_D(\rho_{AB}) + K_D(\rho_{A'B'}) \tag{4.60}$$

10. ?(Add): it is not known if $K_D$ is additive, that is if for all bipartite $\rho$ and $\sigma$
$$K_D(\rho \otimes \sigma) \leq K_D(\rho) + K_D(\sigma) \tag{4.61}$$

11. ?(Add i.i.d) $K_D(\rho^{\otimes n}) = nK_D(\rho)$

12. ?(Non Lock): is there $c \geq 0$ such that for all $\rho_{AA'B}$,
$$E(\rho_{AA'B}) \geq E(\rho^{AB}) + c \log Rank(\rho'_A), \,? \tag{4.62}$$

13. Relation to other measures [HHHO05a] (see Section 4.5):
$$E_D \leq K_D \leq E_r^\infty \leq E_C. \tag{4.63}$$
as well as [Chr06]
$$E_D \leq K_D \leq E_{sq} \leq E_C \tag{4.64}$$
where $E_{sq}$ is the squashed entanglement.

We also invoke here the property that has been proved further in [CEH$^+$07], which is a generalization of property (13):

14 **Theorem 4.13** *[CEH$^+$07] (Upper bound on key via entanglement measures) For an entanglement measure $E$ which has properties: Conv, As Cont, Mon LOCC, SupNorm($\gamma$) (i.e. $E(\gamma) \geq \log d$), there is*

$$K_D(\rho) \leq E^\infty(\rho). \tag{4.65}$$

### 4.4.2 Applications of the relative entropy bound - on the Conv and As Cont properties on some states for $K_D$ and $E_D$

In this section we explore the relative entropy of entanglement bound (4.65), for the so called *Werner states* We first extend the property As Cont Pure of $K_D$ to some mixed states.

#### Continuity on separable and some other states of distillable key

Since $E_r^\infty(\sigma) = K_D(\sigma) = 0$ for separable $\sigma$, and $E_r$ is asymptotically continuous (see Proposition 4.17), we have for $\rho$ and $\sigma$, if $||\rho - \sigma|| \leq \epsilon$, then

$$K_D(\rho) \leq E_r(\rho) \leq 4\epsilon \log d + h(\epsilon), \tag{4.66}$$

which proves the continuity of $K_D$ on separable states. The same holds for $E_D$, since $E_D \leq K_D$, by property (4.63).

It is tempting to generalize property As Cont Pure to the case of private states, and in general to the pure states twisted in its Schmidt basis which seems to be generalization of pure states called here **Schmidt-twisted pure states** (see [PHHH08]). Note, that this class of states, includes some of irreducible private states, and Schmidt-twisted pure states as well. This class includes in particular a subclass of irreducible pdits constructed in Section 3.6.

We note also, that $K_D$ satisfies Cont, on states for which Devetak-Winter protocol is an optimal key distillation protocol, since its rate $C_D^{DW}(\rho)$ is asymptotically continuous (see Section 2.8.1).

#### Partial convexity of $K_D$

**Proposition 4.14** *For an entanglement measure $E$ satisfying Conv, As Cont, SupNorm($\gamma$), $K_D$ satisfies Conv on an ensamble $\{(p_i, \rho^{(i)})\}$, if $K_D(\rho^{(i)}) = E(\rho^{(i)})$.*

**Proof.** Denote $\sum_i p_i\rho_i = \rho$. We have the following chain of (in)equalities, which we comment below:

$$K_D(\rho) \leq K_D(\sum_i p_i\rho_i \otimes |ii\rangle\langle ii|) \leq E(\sum_i p_i\rho^{(i)} \otimes |ii\rangle\langle ii|) \leq$$
$$\sum_i p_i E(\rho_i \otimes |ii\rangle\langle ii|) = \sum_i p_i E(\rho_i) = \sum_i p_i K_D(\rho_i). \tag{4.67}$$

The first inequality is because for any ensamble $\{(p_i, \rho^{(i)})\}$ of $\rho$, the first action of any protocol of key distillation from $\sum_i p_i\rho^{(i)}_{AB} \otimes |ii\rangle\langle ii|_{A'B'}$ can be just tracing out system $A'B'$, ending up with $\rho$. Next two inequalities follows from Theorem 4.13, and convexity of $E$. The last but one is due to Mon LOCC property of E. The last equality is by assumption. ∎

**Remark 4.15** *The above results holds by the same argument for $E_D$, and in fact for all suitably defined operational measures (note, that we deal here with intuitive notion of 'operationality' of entanglement measure).*

### On $K_D$ of Werner states

The following example of application of the bound $K_D \leq E_r^\infty$ has been provided in [HHHO05c]. Consider the antisymmetric Werner state $\rho_a = \frac{2}{(d^2+d)}(\mathrm{I} + V)$ with $V$ the swap operator (see Section 2.2.2). It has been shown in [AEJ$^+$01], that the regularised relative entropy of entanglement is considerably small:

$$E_r^\infty(\rho_a) \geq \log(\frac{d+2}{d}) \geq K_D(\rho_a). \tag{4.68}$$

Hence we have considerably small key in that case, even for relatively 'small' Werner states. It is also important to note, that $E_C(\rho_a) = 1$ independent of the dimension $d$ [MY04].

We give now the upper bound on $K_D$ of arbitrary Werner state defined as:

$$\rho_W(p) = p\rho_a + (1-p)\rho_s \tag{4.69}$$

with $p$ the probability of mixing, and $\rho_s = \frac{2}{(d^2-d)}(\mathrm{I} - V)$ the symmetric Werner state. Now, we have:

$$K_D(\rho_W(p)) \leq E_r^\infty(\rho_W(p)) \leq pE_r^\infty(\rho_a) + (1-p)E_r^\infty(\rho_s) \tag{4.70}$$

where the second inequality follows from convexity of $E_r$. Since $\rho_s$ is separable [Wer89], from (4.68)

$$\rho_W(p) \leq p\log(1 + \frac{2}{d}). \tag{4.71}$$

## 4.5 Relative entropy of entanglement - an upper bound on distillable key

In [CEH+07] it is shown, that an entanglement monotone satisfying some axioms is an upper bound on distillable key, as described in Theorem 4.13. This general result uses the fact, that - informally speaking - each operation $P_n$ of key distillation protocols in Defs. 4.1 and 4.3, can be w.l.g. assumed to use only $m$ operations of classical communication with $m$ linear function of $n$. Prior to this result, in [HHHO05a] it has been shown, that $K_D \leq E_r^\infty$, where $E_r^\infty$ is regularized relative entropy of entanglement (see Eq. (2.115)). Since the proof of the latter fact does not use the linearity of communication, and provides methods useful in other contexts, we show it in detail now.

We need first the following technical lemma:

**Lemma 4.16** *Consider a set* $\mathcal{S}_U := \{U\rho_{ABA'B'}U^\dagger \,|\, \rho_{ABA'B'} \in SEP \cap B(\mathcal{C}^d \otimes \mathcal{C}^d \otimes \mathcal{C}^{d_{A'}} \otimes \mathcal{C}^{d_{B'}})\}$ *where* $U = \sum_{i,j=0}^{d-1} |ij\rangle\langle ij| \otimes U_{ij}$ *is* $\mathcal{B}$*-twisting with* $\mathcal{B}$ *being a standard product basis in* $\mathcal{C}^d \otimes \mathcal{C}^d$*. Let* $\sigma_{ABA'B'} \in \mathcal{S}_U$ *and* $\sigma_{AB} = \mathrm{Tr}_{A'B'}\sigma_{ABA'B'}$*. We have then*

$$S(P_+^{(d)}||\sigma_{AB}) \geq \log d, \tag{4.72}$$

*where* $P_+^{(d)} = |\Psi_+^{(d)}\rangle\langle\Psi_+^{(d)}|$ *is a projector onto maximally entangled state* $|\Psi_+^{(d)}\rangle = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}}|i\rangle|i\rangle$.

**Proof.** Let us first show, that

$$\mathrm{Tr}P_+^{(d)}\sigma_{AB} \leq \frac{1}{d} \tag{4.73}$$

for any $\sigma_{AB} \in \mathcal{S}_U$. We first show this for $\sigma_{AB}$ "derived" from some pure product states $|\psi\rangle_{AA'BB'}$ in $AA' : BB'$ cut (see Section 2.4.1):

$$\sigma_{AB} = \mathrm{Tr}_{A'B'}U^\dagger|\psi\rangle\langle\psi|U. \tag{4.74}$$

Because $\psi$ is product, it can be written as

$$\psi = (\sum a_i|i_A\rangle|\psi_i\rangle'_A) \otimes (\sum b_i|i_B\rangle|\phi_i\rangle'_B) \tag{4.75}$$

with $a_i, b_i$ normalized and $|i_A\rangle, |i_B\rangle, |\psi_i\rangle, |\phi_i\rangle$ on subsystem $A, B, A', B'$ respectively.

Now the condition (4.73) for $\sigma$ originating from pure product state is

$$\sum_{ij} a_i b_i a_j^* b_j^* \langle x_i|x_j\rangle \leq 1 \tag{4.76}$$

where $x_k$ are arbitrary vectors of norm one arising from the action of $U$ on $\psi_i$ and $\phi_i$. Since the $x_k$ are arbitrary they can incorporate the phases of $a_i, b_i$ so that we require now $\sum_{ij}\sqrt{p_i q_i p_j q_j}\langle x_i|x_j\rangle \leq 1$. where $p_i$ and $q_i$ are probabilities. Now, the right hand side will not decrease if we assume $\langle x_i|x_j\rangle = 1$ so we require $[\sum_i \sqrt{p_i q_i}]^2 \leq 1$ which is satisfied by any probability distribution, which gives the proof of (4.73) for special $\sigma_{AB}$.

Now we observe, that since (4.73) holds for $\sigma_{AB}$ derived from pure product state, by averaging over probabilities, we will have (4.73) for an arbitrary $\sigma_{AB}$ from the set $\mathcal{S}_U$. Indeed we have:

$$\begin{aligned}\mathrm{Tr}P_+^{(d)}\mathrm{Tr}_{A'B'}U^\dagger \sum_k p_k|\psi_k\rangle\langle\psi_k|U = \\ \sum_k p_k \mathrm{Tr}P_+^{(d)}\mathrm{Tr}_{A'B'}U^\dagger|\psi_k\rangle\langle\psi_k|U.\end{aligned} \tag{4.77}$$

Now by concavity of logarithm, we have for any states $\rho$ and $\sigma$:

$$\begin{aligned}S(\rho||\sigma) = -S(\rho) - \mathrm{Tr}(\rho\log\sigma) \geq \\ -S(\rho) - \log(\mathrm{Tr}\rho\sigma)\end{aligned} \tag{4.78}$$

Applying inequality (4.73) we have that

$$-\log(\mathrm{Tr}\rho\sigma) \geq \log d. \tag{4.79}$$

Finally, using (4.78) we obtain

$$S(P_+^{(d)}||\sigma_{AB}) \geq \log d, \tag{4.80}$$

which is a desired bound.∎

We will also need the following proposition obtained in [DHR02, SRH06].

**Proposition 4.17** *[DHR02, SRH06] For any convex set of state $\mathcal{S} \subset B(\mathcal{C}^d)$ that contains the maximally mixed state, the relative entropy distance from this set given by*

$$E_r^{\mathcal{S}}(\rho) = \inf_{\sigma\in\mathcal{S}} S(\rho||\sigma), \tag{4.81}$$

*is asymptotically continuous i.e. it satisfies*

$$|E_r^{\mathcal{S}}(\rho_1) - E_r^{\mathcal{S}}(\rho_2)| < 4\epsilon\log d + h(\epsilon) \tag{4.82}$$

*for any states $\rho_1$, $\rho_2 \in B(\mathcal{C}^d)$ with $\epsilon = \|\rho_1 - \rho_2\| \leq 1$, and the binary entropy function $h(\epsilon) = -\epsilon\log\epsilon - (1-\epsilon)\log(1-\epsilon)$.*

We are now in position to formulate and prove the main result of this section.

**Theorem 4.18** *For any bipartite state $\rho_{AB} \in B(\mathcal{C}^{d_A} \otimes \mathcal{C}^{d_B})$ there holds*

$$K_D(\rho_{AB}) \leq E_r^{\infty}(\rho_{AB}). \tag{4.83}$$

**Proof.** Let us fix $\delta > 0$. By definition of $K_D(\rho_{AB})$ there exists protocol $P_\delta$ (i.e. sequence of maps $\Lambda_n$), such that

$$\Lambda_n(\rho^{\otimes n}) = \tilde{\gamma}^{(d)} \tag{4.84}$$

where

$$\limsup_{n\to\infty} \frac{\log d}{n} = K_D(\rho_{AB}) - \delta \tag{4.85}$$

and

$$\lim_{n\to\infty} \|\tilde{\gamma}^{(d)} - \gamma^{(d)}\| \equiv \lim_{n\to\infty} \epsilon_n = 0 \tag{4.86}$$

with $\gamma^{(d)}$ being pdit with $d \times d$-dimensional key part (for simpler notation we omit the dependence of d from $n$) on systems $ABA'B'$.

Let $\tilde{\sigma_{sep}}$ be a separable state on $(\mathcal{C}^{d_A} \otimes \mathcal{C}^{d_B})^{\otimes n}$. We will present now the chain of (in)equalities, and comment it below.

$$\begin{aligned}
& S(\rho_{AB}^{\otimes n}||\tilde{\sigma}_{sep}) \geq S(\tilde{\gamma}^{(d)}_{ABA'B'}||\sigma_{sep}) = && (4.87)\\
= \;& S(U_\gamma \tilde{\gamma}^{(d)}_{ABA'B'} U_\gamma^\dagger || U_\gamma \sigma_{sep} U_\gamma^\dagger) \geq && (4.88)\\
\geq \;& S(\mathrm{Tr}_{A'B'}[U_\gamma \tilde{\gamma}^{(d)}_{ABA'B'} U_\gamma^\dagger] || \mathrm{Tr}_{A'B'}[U_\gamma \sigma_{sep} U_\gamma^\dagger]) && (4.89)\\
=: \;& S(\tilde{P}_+^{(d)}||\sigma) \geq && (4.90)\\
\geq \;& \inf_{\sigma\in T} S(\tilde{P}_+^{(d)}||\sigma) =: E_r^T(\tilde{P}_+^{(d)}) \geq && (4.91)\\
\geq \;& E_r^T(P_+^{(d)}) - 4||\tilde{P}_+^{(d)} - P_+^{(d)}|| \log d - h(||\tilde{P}_+^{(d)} - P_+^{(d)}||) \geq && (4.92)\\
\geq \;& (1 - 4\epsilon_n)\log d - h(\epsilon_n) && (4.93)
\end{aligned}$$

Inequality (4.87) is due to the fact, that relative entropy does not increase under completely positive maps; in particular it can not increase under LOCC action of operation which distills key, applied to it's both arguments. The second argument becomes other separable state $\sigma_{sep}$, due to Theorem 2.14. Note, that subsystems $AB$ of $\tilde{\gamma}^{(d)}_{ABA'B'}$ are not to be identified with that of $\rho$.

In Eq. (4.88) we perform twisting $U_\gamma$ controlled by the basis in which $\gamma^{(d)}_{ABA'B'}$ is secure (without loss of generality we can assume it is standard basis). The equality follows from the fact that unitary transformation does not change the relative entropy when applied to its both arguments. Next (4.89) we trace out $A'B'$ subsystem of

both states which only decreases the relative entropy. After this operation, the first argument is $\tilde{P}_+^{(d)}$, which is a state close to the EPR state $P_+^{(d)}$. ($\tilde{P}_+^{(d)}$ would be equal to the EPR state if $\tilde{\gamma}_{ABA'B'}^{(d)}$ were exactly pdit) while second argument becomes some – not necessarily separable – state $\sigma$. The state belongs to the set $T$, constructed as follows. We take set of separable states on system $ABA'B'$ subject to twisting $U_\gamma$ and subsequently trace out the $A'B'$ subsystem.

The inequality (4.90) holds, because we take infimum over all states from the set $T$ of the function $S(\tilde{P}_+^{(d)}||\sigma)$. This minimised version is named there $E_r^T(\tilde{P}_+^{(d)})$ as it is relative entropy distance of $P'_+$ from the set $T$.

Let us check now, that set $T$ fulfills the conditions of proposition 4.17. Convexity of this set is obvious, since (for fixed unitary $U_\gamma$) by linearity it is due to convexity of the set of separable states. This set contains the identity state, since it contains maximally mixed state which is separable, unitarily invariant (i.e. invariant under $U_\gamma$ ) and whose subsystem $AB$ by definition is the maximally mixed state as well. Thus by proposition 4.17 we have that $E_r^T$ is asymptotically continuous

$$|E_r^T(\tilde{P}_+^{(d)}) - E_r^T(P_+^{(d)})| < ||\tilde{P}_+^{(d)} - P_+^{(d)}||4\log d + h(||\tilde{P}_+^{(d)} - P_+^{(d)}||). \tag{4.94}$$

Since $\tilde{P}_+^{(d)}$ and $P_+^{(d)}$ come out of $\tilde{\gamma}_{ABA'B'}^{(d)}$ and $\gamma_{ABA'B'}^{(d)}$ by the same transformation described above (twisting, and partial trace) which does not increase the trace norm distance, by (4.86) we have that $||\tilde{P}_+^{(d)} - P_+^{(d)}|| \leq \epsilon_n$. This, together with asymptotic continuity (4.94) implies (4.91) if only $\epsilon_n \leq 1/2$, which we can assume, as $\epsilon_n$ approaches zero for large $n$ by (4.86). Now by Lemma 4.16 we have

$$E_r^T(P_+^{(d)}) \geq \log d, \tag{4.95}$$

which by (4.94) gives the last inequality. Summarizing this chain of inequalities (4.87)-(4.92), we have that for any separable state $\tilde{\sigma}_{sep}$:

$$S(\rho_{AB}^{\otimes n}||\tilde{\sigma}_{sep}) \geq (1 - 4\epsilon_n)\log d - h(\epsilon_n) \tag{4.96}$$

Taking now infimum over all separable states $\tilde{\sigma}_{sep}$ we get

$$E_r(\rho_{AB}^{\otimes n}) \geq (1 - 4\epsilon_n)\log d - h(\epsilon_n). \tag{4.97}$$

Now we divide both sides by $n$ and take the limit. Then the left-hand-side converges to $E_r^\infty$. Thanks to (4.86), $\epsilon_n$ approaches zero for large $n$, and due to (4.85), $\log d/n$ converges to $K_D(\rho_{AB})$. Thus owing to the continuity of $h$, we obtain

$$E_r^\infty \geq K_D - \delta. \tag{4.98}$$

Since $\delta$ was fixed arbitrarily, this ends the proof of Theorem 4.18. ∎

## 4.6 Which states are key distillable ? - preliminaries

In this section we consider special cases of key (un)distillability of bipartite states [HHHH07]. We first focus on two cases when it is easy to say if a given bipartite state is key distillable. We present then the lower bound on distillable key given by Devetak and Winter [DW05]. Their protocol of key distillation is formulated in slightly different way, but can be used in our context, as it is shown below explicitly. Thanks to this fact, we observe, that states which are close in trace norm to pdits have nonzero distillable key. We also note, that PPT states are bounded away from private states by a positive constant in trace norm distance, yet this constant can vanish for some PPT states from properly large dimension.

### 4.6.1 Separable and distillable states

**Observation 4.19** *[GW00, GW99, CLL04b] For any bipartite state $\rho$ there holds:*

1. *$E_D(\rho) > 0 \Rightarrow K_D(\rho) > 0$, in particular, if $\rho$ is pure,*

$$K_D(\rho_{AB}) = E_D(\rho_{AB}) = S(\rho_A). \tag{4.99}$$

2. *$\rho \in SEP \Rightarrow K_D(\rho) = 0$.*

The first fact has been noticed already in context of the so called *unconditional quantum key distribution* in [DEJ$^+$96]. There the protocol of distillation of entanglement has been proposed in order to obtain secure bits and called quantum privacy amplification. In present context, this fact follows from the very definition of private states: maximally entangled states are also private states. Hence distillation of entanglement is one of ways to distill key. Concerning equalities (4.99), the second equality is a well known property of pure states [BDSW96], and the first follows from Theorems 4.18 and 2.26 (cf. [Chr06]).

In particular, as it is noted in [AH06], all entangled states $\rho \in B(\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes n})$ for $n = 2, 3$ there is also $K_D(\rho) > 0$ for these states, because these states have $E_D > 0$ [HHH97].

The second fact can be found (in different formulation) in [GW00, GW99, CLL04b]. Another immediate proof of the latter, follows from Theorem 4.18. This is because by definition of regularized relative entropy of entanglement, $E_r^\infty(\sigma) = 0$ for any separable state $\sigma$, which is an upper bound on distillable key.

**Observation 4.20** *For every pair $\sigma, \gamma$ with $\sigma \in SEP^{(d,d')}$ and $\gamma \in PS^{(d,d')}$, there holds*

$$||\sigma - \gamma|| \geq 1 - \frac{1}{d}. \tag{4.100}$$

*where* $SEP^{(d,d')}$ *denotes the set of separable states acting on* $\mathcal{H}_{ABA'B'}$ *with* $\dim A = \dim B = d$ *and* $\dim A' = \dim B' = d'$.

**Proof.** Applying the privacy squeezing of $\gamma$, to both $\gamma$ and $\sigma$, we obtain:

$$||\sigma - \gamma|| \geq ||\rho^{(ps)} - P_+^{(d)}||, \tag{4.101}$$

as the norm does not increase under quantum operations (in this case the operation of privacy squeezing). From the proof of Lemma 4.16, Eq. (4.73), we know that fidelity of a privacy squeezed separable state with the maximally entangled state $|\Psi_+^{(d)}\rangle = \sum_i \frac{1}{\sqrt{d}}|ii\rangle$ is bounded from above by $\frac{1}{d}$. By equivalence of norm and fidelity given in Lemma 2.20, we have that the trace norm distance between the two is bounded from below by $1 - \frac{1}{d}$. ∎

Since the smallest $d$ equals 2, we have that the set of separable states is bounded away by $\frac{1}{2}$ from the set of private states independently of the dimension.

### 4.6.2 Devetak and Winter approach - lower bound on one way distillable key

In this section we present the result of Devetak and Winter [DW05] in our context. We invoke their definition of one-way protocol of key distillation, that is a protocol which uses only communication from Alice to Bob. This protocol (in short DW) can be easily turned into classical key distillation protocol, as we show below. This enable us to use the lower bound on the rate of one-way distillable key that has been worked out in [DW05]. In consequence, we show the main result of this section that states close enough to pbit in trace norm, have nonzero distillable key.

The one-way key distillation protocol is defined for the following input states, called *cqq states* $\rho_{ABE}^{(cqq)}$ of the form:

$$\rho_{ABE}^{(cqq)} = \sum_{i=0}^{dimA-1} p_i |i\rangle\langle i|_A \otimes \rho_{BE}^{(i)}, \tag{4.102}$$

where $p_i$ is the probability that system $A$ is in state $|i\rangle\langle i|_A$. In what follows, the symbol $Y = y$ will denote, that system labeled as $Y$ is in state $|y\rangle\langle y|$. Consequently we will write explicitly $P(A = i)$ instead of $p_i$. $n$ copies of the cqq state can be written as

$$\left(\rho_{ABE}^{(cqq)}\right)^{\otimes n} = \sum_{i_n} P(A_{(n)} = i_n)|i_n\rangle\langle i_n|^{A_{(n)}} \otimes \rho_{BE_{(n)}}^{i_n}, \tag{4.103}$$

with $i_n = i_n^{(1)} \dots i_n^{(n)}$ and

$$|i^n\rangle = |i_1\rangle \otimes \cdots \otimes |i_n\rangle, \tag{4.104}$$

$$\rho_{BE_{(n)}}^{i_n} = \rho_{BE}^{i_1} \otimes \cdots \otimes \rho_{BE}^{i_n}. \tag{4.105}$$

The subscript $(n)$ recalls that system under consideration consists of the $n$ systems in identical state.

A *one–way key distillation protocol* consists of:

- An operation $T$ defined as

$$T(\rho_{A_{(n)}}) = \sum_{i_n} P(C = l, K = m | A_{(n)} = i_n) |\ell\rangle\langle\ell|_C \otimes |m\rangle\langle m|_K, \tag{4.106}$$

  with range $\ell \in \{1, \ldots, L\}$ and $m \in \{1, \ldots, M\}$.

- A POVM

$$D^{(\ell)} = \{D_m^{(\ell)}\}_{m=1}^M \tag{4.107}$$

  on $B_{(n)}$ for every $\ell$.

The idea is that Alice performs $T$ on her subsystem $\rho_{A_{(n)}}$ of the state (4.103). She then treats state of system $K$ as the key, and sends $C = \ell$ to Bob.

Bob obtains his version of the key - $K'$ by measuring his system $B$ using $\{D^{(\ell)}\}$:

$$P(K' = m | C = \ell, A_{(n)} = i_n) = \mathrm{Tr}\big(D_m^{(\ell)} \rho_{B_{(n)}}^{i_n}\big).$$

For technical reasons it is assumed that the number of possible messages send by Alice is bounded from above: $L \leq 2^{nF}$, for some constant $F$.

The one-way key distillation protocol is called an $(n, \epsilon)$–*protocol* if

1.
$$P(K \neq K') \leq \epsilon. \tag{4.108}$$

2.
$$\left\| \sum_{m=0}^{K-1} P(K = m) |m\rangle\langle m| - \sum_{m=0}^{K-1} \frac{1}{K} |m\rangle\langle m| \right\| \leq \epsilon. \tag{4.109}$$

3. There is a state $\sigma_0$ such that for all $m$,

$$\left\| \sum_{i_n, \ell} P(A_{(n)} = i_n, C = \ell | K = m) |\ell\rangle\langle\ell| \otimes \rho_{E_{(n)}}^{i_n} - \sigma_0 \right\| \leq \epsilon. \tag{4.110}$$

Then, $R$ is an *achievable rate* if for all $n$ there exist $(n, \epsilon)$–protocols with $\epsilon \to 0$ and $\frac{1}{n} \log_2 M \to R$ as $n \to \infty$. Finally define

$$K_{\rightarrow}(\rho) := \sup\{R : R \text{ achievable}\},$$

the *one–way (or forward) secret key capacity of* $\rho$.

We will argue now, that $K_{\rightarrow}$ is a lower bound on distillable key $K_D$ given in Definition 4.1. We first show that $C_D \geq K_{\rightarrow}$. The latter follows from the observation below:

**Observation 4.21** *For any cqq state* $\rho_{ABE}$*, if there exists an* $(n, \epsilon)$*-protocol acting on* $\rho_{ABE}^{\otimes n}$*, with ranges of key and communication* $M$ *and* $L$ *respectively, defined by (4.106)-(4.110), there is an LOPC operation* $P_{(n,\epsilon)}$ *which acting on* $\rho_{ABE}^{\otimes n}$ *yields* $\rho_{out}$ *satisfying:*

$$||\rho_{out} - \beta_{d_n}|| \leq 4\epsilon, \tag{4.111}$$

*with* $\beta_{d_n}$ *being an ideal ccq state, and* $d_n = M$*.*

**Proof.** We begin with constructing an LOPC operation $P_{(n,\epsilon)}$. This will be a composition of LOPC counterparts of operations used by $(n, \epsilon)$-protocol, interlaced with some partial trace operations, by which Alice and Bob will get rid of already used systems. The correspondence between operations of $(n, \epsilon)$-protocol and the LOPC operations is quite direct.

1. Alice performs locally quantum operation which corresponds to channel $T$. This operation transformes her subsystem of $\rho_{ABE}^{\otimes n}$ into $\sum_{x_n,m,l} P(K = m, C = l, X_n = x_n)|m\rangle\langle m|_A \otimes |l\rangle\langle l|_a$.

2. Alice communicates state of a system $a$ to Bob via classical communication operation and traces out system $a$.

3. Bob performs an operation controlled by system $b$ which holds communicate from Alice: upon receiving $|l\rangle\langle l|_b$ Bob performs corresponding quantum measurement with the Kraus operators $\{A_{m'}\}$ defined by the POVM $\{D^{(\ell)}\}$:

$$A_{m'} := \sqrt{D^{(\ell)}} \otimes |m'\rangle. \tag{4.112}$$

4. Bob traces out system carrying quantum results of this measurement leaving system which carries classical results. The latter is in state $\sum_{x_n,m,l,m'} P(K' = m'|K = m, C = l, X_n = x_n)|m'\rangle\langle m'|$.

Composition of the above operations defines LOPC operation $P_{(n,\epsilon)}$, which applied to input state $\rho_{ABE}^{\otimes n}$ (4.103) yields a state of the form:

$$\rho_{out} = \sum_{i_n,l,m,m'} P(C = l, A_{(n)} = i_n, K = m, K' = m')|mm'\rangle\langle mm'|_{AB} \otimes \rho_{E_{(n)}}^{i_n} \otimes |l\rangle\langle l|_e. \tag{4.113}$$

We will argue now, that this state is close to some ideal ccq state. From (4.108), one gets that $||\rho_{out} - \tilde{\rho}_{out}|| \leq \epsilon$, with

$$\tilde{\rho}_{out} = \sum_{x_n,l,m,m'} \delta_{m,m'} P(C = l, A_{(n)} = i_n, K = m, K' = m') |mm'\rangle\langle mm'|_{AB} \otimes \rho^{i_n}_{E_{(n)}} \otimes |l\rangle\langle l|_e. \tag{4.114}$$

One then finds, that $||\tilde{\rho}_{out} - \hat{\rho}_{out}|| \leq \epsilon$ for

$$\hat{\rho}_{out} = \sum_{x_n,l,m} P(C = l, A_{(n)} = i_n, K = m) |mm\rangle\langle mm|_{AB} \otimes \rho^{i_n}_{E_{(n)}} \otimes |l\rangle\langle l|_e, \tag{4.115}$$

again using (4.108). We can now make use of the assumption (4.110), to see that

$$\sum_m P(K = m) \left\| \sum_{i_n,\ell} P(A_{(n)} = i_n, C = \ell | K = m) |\ell\rangle\langle\ell| \otimes \rho^{i_n}_{E_{(n)}} - \sigma_0 \right\|, \tag{4.116}$$

is not greater than $\epsilon$ and equals

$$\begin{aligned} &|| \sum_m P(K = m) P(A_{(n)} = i_n, C = l | K = m) |mm\rangle\langle mm| \otimes \rho^{i_n}_{E_{(n)}} \otimes |l\rangle\langle l| \\ &-(\sum_m P(K = m) |mm\rangle\langle mm|) \otimes \sigma_0||. \end{aligned} \tag{4.117}$$

Hence, we get, that $||\hat{\rho}_{out} - (\sum_m P(K = m)|mm\rangle\langle mm|) \otimes \sigma_0|| \leq \epsilon$. Now, by as that $||\rho_{out} - \rho^{ccq}_{ideal}|| \leq 4\epsilon$, which ends the proof of this observation. ∎

### 4.6.3 Lower bound on one-way distillable key from Devetak-Winter protocol

Observation 4.21 let us use the lower bound provided by Devetak and Winter in context of distillation of private states[3]. We quote here their result, and show its counterpart in present context.

**Theorem 4.22** *[DW05] For every cqq–state $\rho$,*

$$K_{\rightarrow}(\rho) \geq I(A : B) - I(A : E).$$

Here $I(A : B)$ is quantum mutual information of subsystem $AB$ of the cqq state (4.102).

From this theorem, we get the following corollary:

[3] In fact, as it is argued in [CEH+07], the security conditions (4.109)-(4.110) are strictly stronger then our condition (4.8) of an output state to be close to an ideal ccq state in trace norm, yet the difference in formulation of security condition does not affect the key rate [Win08]

**Corollary 4.23** *For every ccq state $\rho_{ABE}$,*

$$C_D(\rho_{ABE}) \geq C_D^{DW}(\rho_{ABE}) := I(A:B)_\rho - I(A:E)_\rho, \tag{4.118}$$

*where $I(X:Y)_\rho$ denotes quantum mutual information of a bipartite state with subsystems $X$ and $Y$ respectively.*

**Proof.** Since every *ccq* state, is also a *cqq* state, by Theorem 4.22 by Observation 4.21, one needs to show $C_D \geq K_{\rightarrow}$. The proof of this inequality involves elementary technique already presented in proof of Theorem 4.12. Since adaptation of the latter reasoning in present context needs only slight modifications, we just provide the idea.

The Observation 4.21 provides a correspondence: for any $(n,\epsilon)$–protocol with key range $M$ and output secure according to Eqs. (4.108)-(4.110), there is an operation $P_{(n,\epsilon)}$ which outputs a state close by $4\epsilon$ to an ideal *ccq* state with $d_n \times d_n$ $AB$ part, i.e. secure in light of Def. 4.3. Moreover, the correspondence is qualitative: $d_n = M$. We now argue that it can be extended to hold for protocols.

Let $R$ be an achievable rate as given below Eq. (4.110). It follows that there exists a family $\{(n,\epsilon_n)\}_{n=1}^{\infty}$ of $(n,\epsilon_n)$–protocols such that

$$\lim_{n\to\infty}(\epsilon_n, \frac{\log M_n}{n}) = (0,R), \tag{4.119}$$

where we made explicit dependence of $\epsilon$ and $M$ from $n$. The above mentioned correspondence of operations naturally defines a set of LOPC operations $\mathcal{P} = \{P_{(n,\epsilon)}\}_{n=1}^{\infty}$ that constitutes classical key distillation protocol with the same rate $R = \lim_{n\to\infty}\frac{d_n}{n}$. Since construction of $\mathcal{P}$ does not depend on $R$, any rate achieved by family $\{(n,\epsilon_n)\}$ protocols can be achieved by $\mathcal{P}$, proving thereby $C_D \geq K_{\rightarrow}$, which ends the proof of this Corollary. ∎

The LOPC protocol $\mathcal{P}$ described in the proof of the above Corollary, with a rate $C_D^{DW}(\rho_{ABE})$ on a tripartite state $\rho_{ABE}$ we will call the *DW key distillation protocol*. Below, we provide shortly the idea of this protocol following the formulation of Devetak and Winter.

**DW key distillation protocol**

Alice and Bob share $n$ copies of the cqq state. Hence, Alice's state is described by the string of $n$ symbols from some alphabet $\mathcal{I}$. In first step Alice checks if the string $i_n$ is from typical class i.e. if the occurrence of each symbol from $\mathcal{I}$ is close to $p_i$. If not, she aborts the protocol, or tells Bob the type otherwise. Knowing the type, they use an a priori prepared code book $\{C_l\}_{l=1}^{L}$(the set of *codes*[4]) where each code allows for communicating approximately $nI(A:B)$ bits from Alice to Bob.

[4]The 'classical' code is a subset of bit-strings of length $n$ $C \in \{0,1\}^n$ called *code words*. Upon $i_n^A$ is send, and received is a bit string $j_n^B$, receiver can conclude from $j_n^B$ what was $i_n^A$, knowing that $i_n^A \in C$ [CT91]

Alice then selects a random number $l$ such, that $i_n$ is a codeword from a code $C_l$ from this code book, and sends $l$ to Bob. Upon receiving $l$, Bob applies decoding operation $D_l$. After this, which may fail, but only with small probability, they have sequences $i_n^A$ ($j_n^B$ for Bob) of approximate length $nI(A:B)$. The codes are chosen in such a way, that Alice and Bob can treat approximately $n(I(A:B)-I(A:E))$ leading bits of $i_n^A$ ($j_n^B$) as the key: the strings $i_n^A$ and $j_n^B$ are with high probability both perfectly correlated and uniformly random, hence can be used for one-time pad encryption.

Moreover, according to security condition imposed on the output state, Eve's knowledge about the key bit-string after this protocol is represented by almost the same state $\sigma_E$. Of course it may be that this protocol aborts in the middle. E.g. the codes must be $\epsilon$-*good*, so that with high probability $1-\epsilon$ Bob could perform decoding operation.

### 4.6.4 Simple lower bound on distillable key via Devetak-Winter protocol

The main result formulated in this subsection (Theorem 4.25) shows, that one can find lower bound on distillable key of a bipartite state $\rho_{ABA'B'}$ of four systems $ABA'B'$, by calculating this rate for a ccq state (see Eq. (eq:ccq-def)) of a p-squeezed state of $\rho_{ABA'B'}$ (see Section 3.3.2). This is much easier, because the the p-squeezed state is a two-qubit state.

Let us recall here, that the ccq state of a given state is in principle not uniquely defined. It depends on a partial isometry on Eve's subsystem, as emerging from a purification $|\phi_\rho\rangle$ of a bipartite state which is unique up to this transformation. Thus, in what follows we will denoted as $\rho_\phi^{ccq}$. However, as we argue now, the amount of classical distillable key of a ccq state is independent of the purification $|\phi\rangle$ via which this state was obtained. This is the statement of lemma below.

**Lemma 4.24** *For any two different ccq states $\rho_\phi^{ccq}$ and $\rho_\psi^{ccq}$ of a bipartite state $\rho_{AB}$, obtained via purifications $|\phi_\rho\rangle$ and $|\psi_\rho\rangle$ respectively there is $C_D(\rho_\phi^{ccq}) = C_D(\rho_\psi^{ccq}) \equiv C_D(\rho^{ccq})$ .*

**Proof.** From Lemma 2.6, and Corollary A.2, we have that ccq states obtained via two purifications differ only by such partial isometry on system $E$. Now, we can use Theorem 4.4 to have: $C_D(\rho_\psi^{ccq}) = C_D(\rho_\phi^{ccq})$, and the assertion follows ∎

Thanks to the above lemma, the quantity $C_D(\rho^{ccq})$ can be defined as $C_D(\rho_\phi^{ccq}) = C_D(\rho^{ccq})$ where $\phi$ is standard purification of $\rho^{ccq}$. In particular in proofs that concerns quantity $C_D(\rho^{ccq})$ we can use a ccq state of $\rho$ obtained via the most convenient purification. This enable us to formulate the following theorem:

**Theorem 4.25** *For any bipartite state $\rho_{ABA'B'} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$, there holds*

$$K_D(\rho_{ABA'B'}) \geq C_D([\rho^{ps}]^{ccq}_{ABE'}) \tag{4.120}$$

*where $[\rho^{ps}]^{ccq}_{ABE'}$ is a ccq state of a privacy squeezed state of $\rho_{ABA'B'}$.*

**Proof.** We first provide a chain of (in)equalities which shows the thesis, and comment it below.

$$\begin{aligned} K_D(\rho_{ABA'B'}) = C_D(\rho_{ABA'B'}) \geq \\ C_D(\rho^{ccq}_{ABE}) = C_D(\mathrm{Tr}_{A'B'}[\rho^{ps}_{AB}]^{ccq}_{\phi}) \geq C_D([\rho^{ps}_{AB}]^{ccq}_{\phi}) = C_D([\rho^{ps}_{AB}]^{ccq}). \end{aligned} \tag{4.121}$$

The first equality is by Theorem 4.12. The first inequality is due to the fact, that in order to obtain a ccq state out of $\rho_{ABA'B'}$ one needs to perform certain local operations (measurement, tracing out systems $A'$ and $B'$).

To see the second equality we observe that $\rho^{ccq}_{ABE}$ and $\mathrm{Tr}_{A'B'}[\rho^{ps}_{AB}]^{ccq}$ can differ only by some partial isometry on Eve's system.

To this end we need to collect more facts. First, by invariance of ccq states under twisting (Theorem 3.3) the state $\rho^{ccq}$ satisfies:

$$\rho^{ccq} = \mathrm{Tr}_{A'B'}(|\phi\rangle\langle\phi|_{ABA'B'E}) \tag{4.122}$$

where $|\phi\rangle = U_{ABA'B'} \otimes \mathrm{I}_E|\psi_\rho\rangle$ for any $\mathcal{B}$-twisting $U_{ABA'B'}$ with $\mathcal{B}$ being standard product basis.

Taking now $U$ to be the twisting $U^{ps}$ defined by operation of p-squeezing of $\rho$, we observe that $|\phi\rangle_{ABA'B'E}$ is in fact a purification of the state $\rho^{ps}_{AB}$ with a purifying system $E' = A'B'E$. Let us denote denote now $[\rho^{ps}_{AB}]^{ccq}_{\phi}$ as ccq state of $\rho^{ps}_{AB}$ obtained via purification $|\phi_{\rho^{ps}_{AB}}\rangle$ to system $E'$. Then, the state $\mathrm{Tr}_{A'B'}[\rho^{ps}_{AB}]^{ccq}_{\phi}$ equals just $\rho^{ccq}_{ABE}$. Thus we have

$$C_D(\rho^{ccq}_{ABE}) = C_D(\mathrm{Tr}_{A'B'}[\rho^{ps}_{AB}]^{ccq}_{\phi}). \tag{4.123}$$

The second inequality follows directly from the fact that classical distillable key does not decrease under action of Eve (see Theorem 4.4). Indeed, the two states under consideration differs by a quantum operation (partial trace over $A'B'$) on Eve's system $E' = A'B'E$.

Since by Lemma 4.24, one does not need to care from which purification the ccq state was obtained, there is:

$$C_D(\mathrm{Tr}_{A'B'}[\rho^{ps}_{AB}]^{ccq}_{\phi}) = C_D(\mathrm{Tr}_{A'B'}[\rho^{ps}_{AB}]^{ccq}), \tag{4.124}$$

which proves the last equality. ∎

On any tripartite *ccq* state, $C_D$ is greater than the rate of any concrete protocol applied to this state. Owing to this simple fact, in the above theorem we place DW protocol key rate instead of $C_D$ to obtain the following corollary:

**Corollary 4.26** *For any bipartite state $\rho_{ABA'B'} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$, there holds*

$$K_D(\rho_{ABA'B'}) \geq C_D^{DW}([\rho^{ps}]^{ccq}_{ABE'}) \tag{4.125}$$

*where $[\rho^{ps}]^{ccq}_{ABE'}$ is a ccq state of a privacy squeezed state of $\rho_{ABA'B'}$.*

**Remark 4.27** *The Theorem 4.25, and the above corollary holds also for cqq state. To this end one needs to employ the idea of local twisting (see [HLLO06]). It is twisting controlled only on one site (say Alice) and has form: $\sum_{i=0}^{1} |e_i\rangle\langle e_i|_A \otimes U^{(i)}_{A'B'}$. It is then straightforward to see, that the analogues of Theorem 3.3 and Lemma 4.24 holds in this case. However, the local untwisting can apply only two different unitary transformations on system $A'B'$. Hence it is useful when cqq of some state is close to a cqq of some private state. Since the latter is equal to its ccq, the usefulness of considering cqq instead of ccq in the above theorem is questionable.*

### 4.6.5 The MPDW protocol

In general case, Alice and Bob can not perform the p-squeezing by LOCC operations $\rho^{\otimes n}_{ABA'B'}$, so that they could then measure the main parts of the p-sqeezed states and launch the operation of DW protocol on $([\rho^{ps}]^{ccq})^{\otimes n}$. However, let us consider the composition of first von Neumann measurements (on both sites) of the main parts, with the DW protocol. By Theorem 4.12, there is also an LOCC version of this protocol which in place of operations of DW protocol described in Observation 4.21, has its LOCC counterpart $P^{A_1B_1\ldots A_nB_n}_{n,\epsilon}$, and achieves the same rate as DW on the state $[\rho^{ps}]^{ccq}$.

Now, what Alice and Bob are able to perform via LOCC operations on the state $\rho^{\otimes n}_{ABA'B'}$ is modification of the above LOCC protocol achieved by substituting $P^{A_1B_1\ldots A_nB_n}_{n,\epsilon} \otimes \mathrm{I}_{A'_1B'_1\ldots A'_nB'_n}$ in place of $P^{A_1B_1\ldots A_nB_n}_{n,\epsilon}$. That is, they first measure the main parts of the input states $\rho_{ABA'B'}$, and on resulting states apply the operation $P^{A_1B_1\ldots A_nB_n}_{n,\epsilon} \otimes \mathrm{I}_{A'_1B'_1\ldots A'_nB'_n}$. Operating as identity on the side parts is a counterpart of tracing out this system, but only formally (see Observation 2.11), since actually Alice and Bob can not trace out the side part as it act as a shield.

Together with measurement on the main part such naturally modified DW protocol will be called further a *MPDW protocol*, since it can be viewed as applying an LOCC counterpart of DW protocol, but only to the main parts ($AB$ subsystems) of the input systems.

Thus, the operation of p-suqueezing followed by applying operation of usual DW protocol to the ccq state of a p-squeezed state, is merely a mathematical tool, that provides a lower bound on the rate of the MPDW protocol. We use this tool, to avoid calculating the ccq state of a given tripartite state as this is in principle more difficult then the same for a p-squeezed state.

Note, however, that the operation of p-squeezing may decrease the rate of distilled key. To prove a possibly higher value of distillable key rate one may consider the rate obtained by MPDW protocol:

**Corollary 4.28** *For any bipartite state $\rho_{ABA'B'} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$, there holds*

$$K_D(\rho_{ABA'B'}) \geq C_D^{DW}(\rho_{ABE'}^{ccq}), \tag{4.126}$$

*where $\rho_{ABE'}^{ccq}$ is a ccq state of $\rho_{ABA'B'}$.*

**Proof.** From Eqs. (4.121) we get $K_D(\rho_{ABA'B'}) \geq C_D(\rho_{ABE}^{ccq})$, and $C_D^{DW}(\rho_{ABE}^{ccq}) \geq C_D^{DW}(\rho_{ABE'}^{ccq})$, as DW is a specific protocol of classical key distillation. ∎

Consequently, as in Remark 4.27, we have the above corollary for a *cqq* state in place of a *ccq* one.

### 4.6.6 States enough close to private bits are key distillable

Before we formulate the main result of this section, we need a technical observation.

**Observation 4.29** *Let $\sigma_{ABE}$ be a ccq state of a bipartite state $\rho_{AB}$. Then $I(A : E)_\sigma \leq S(AB)_\rho$, with $\sigma_{AB} = \mathrm{Tr}_E \sigma_{ABE}$.*

**Proof.** This fact is a consequence of the property 6 of the von Neumann entropy and joint concavity theorem (property 7), given in Section 2.7.1.

We can now show the main result which states that if a given state is close enough to pbit in trace norm, it has distillable key. This fact follows easily from Theorem 4.25, and the fact that the rate $C_D^{DW}$ of Devetak-Winter protocol is continuous function of $\rho$.

**Theorem 4.30** $||\rho - \gamma^{(2)}|| \leq \delta < 10^{-3}$ *implies* $K_D(\rho) > 0$.

**Proof.** By Corollary 4.25, to prove the above theorem it is enough to show that $C_D^{DW}(\rho') > 0$ with $\rho' = [\rho^{ps}]^{ccq}$, if only

$$||\rho - \gamma^{(2)}|| \leq \delta < 10^{-3} \tag{4.127}$$

We need to prove a lower bound on:

$$C_D^{DW}(\rho') = I(A : B)_{\rho'} - I(A : E)_{\rho'}. \tag{4.128}$$

Let us fix $\delta > 0$. By assumption (4.127), and the fact that trace norm does not increases under quantum operations we have:

$$||\rho^{ps} - P_+^{(2)}|| \leq \delta. \tag{4.129}$$

For ccq state of $P_+^{(2)}$ we have by Observation 4.29:

$$I(A:E) \leq S(AB) = 0 \tag{4.130}$$

and $I(A:B) = 1$. Analogously, we have for $\rho'$:

$$I(A:E)_{\rho'} \leq S(AB)_{\rho^{ps}}. \tag{4.131}$$

By equivalence of the trace norm and fidelity (Lemma 2.20), there is:

$$||\rho' - [P_+^{(2)}]^{ccq}|| \leq 2\sqrt{2\delta} \tag{4.132}$$

Thanks to the above inequality we can use continuity of von Neumann entropy, to bound the rate of DW protocol for $\rho$. From Fannes inequality (see Eq. (2.24)), we get

$$I(A:B)_{\rho'} \geq 1 - \epsilon \log d_{AB} - 3\eta(\epsilon), \tag{4.133}$$

$$I(A:E)_{\rho'} \leq S(AB)_{\rho^{ps}} \leq \frac{1}{2}\epsilon \log d_{AB} - \eta(\epsilon). \tag{4.134}$$

with $\epsilon = 2\sqrt{\delta}$. Thus we obtain that

$$C_D^{DW}(\rho) \geq I(A:B) - I(A:E) \geq 1 - 6\sqrt{\delta} - 2\eta(2\sqrt{\delta}). \tag{4.135}$$

The above bound is nonzero if only $\delta > 10^{-3}$, as we have found using `Mathematica` 5.0. This ends the proof of this theorem. ∎

**Remark 4.31** *Let us note, that the upper bound on $\delta$ of order $10^{-3}$ is rather rigorous, and can be easily improved, by more careful estimations used in the proof above [HHHO05a].*

The above sufficient condition has been generalized in [CCK+07] to hold on states which are transformable via LOCC into state that is close enough to private state. Independently, the same result was noted and merged with necessary condition in [AH06], giving the following necessary and sufficient condition of key distillability:

**Theorem 4.32** *([AH06], see also [CCK+07]) For a bipartite state there holds $K_D(\rho) > 0$ if and only if there is sufficiently small $\epsilon \geq 0$, a natural number $m$ and an LOCC operation $\Lambda_m$ such that*

$$||\Lambda_m(\rho) - \gamma^{(d_m)}|| < \epsilon \tag{4.136}$$

*for some private state $\gamma^{(d_m)}$ with $d_m \geq 2$.*

### 4.6.7 Lower bound on distillable key of mixtures of key-part-orthogonal private bits

The result which are to present now, was obtained in [HPHH05], by direct arguments. To show it now, we use a more general lemma:

**Lemma 4.33** *(reformulation of analogous lemma from [CCK+07]) Let $\rho_{AB}$ be a bipartite state, and $\rho^{ps}$ its ccq state. Then, $C_D^{DW}([\rho^{ps}]^{ccq}) = 1 - S(AB)_{\rho^{ps}}$.*
**Proof.** Let $\sigma_{ABE} = [\rho^{ps}]^{ccq}$. The result $C_D^{DW}(\sigma) = 1 - S(E)_\sigma$ can be found in [CCK+07]. There is also $S(AB)_{\rho^{ps}} = S(E)_\sigma$, because $\rho^{ps}$ is a bipartite state. ∎

We can formulate now the following proposition:

**Proposition 4.34** *Consider two pbits $\gamma_1$, $\gamma_2$ and take any biased mixture of the form:*

$$\varrho = p_1\gamma_1 + p_2\sigma_x^A\gamma_2\sigma_x^A \tag{4.137}$$

*with, say, $p_1 > p_2$ and $\sigma_x^A = [\sigma_1]_A \otimes I_{A'BB'}$. The distillable key $K_D(\varrho)$ fulfills $K_D(\varrho) \geq 1 - h(p_1)$ where $h(p_1)$ is the binary entropy of distribution $\{p_1, p_2\}$, and $\sigma_1$ is one of Pauli operations given in (2.50).*
**Proof.** It is straightforward to check, that the p-squeezed state of the state $\varrho$ is a mixture of two orthogonal maximally entangled states: $pP_{|\phi^+\rangle} + (1-p)P_{|\psi^+\rangle}$, where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Its von Neumann entropy equals then $1 - h(p)$. Hence, by Lemma 4.33 we get $C_D^{DW}([(\rho)^{ps}]^{ccq}) \geq 1 - h(p)$. This by Theorem 4.25 proves the thesis. ∎

## 4.7 Further development and open problems

As we have noted, the entanglement monotone approach initiated in [HHHO05c, HHHO05a] was then developed in [CEH+07]. It is shown, that *any* bipartite monotone $E$, which is continuous and normalized on private states (i.e. $E(\gamma_d) \geq \log d$), is an upper bound on distillable key, as invoked in Theorem 4.13. In [Chr06] it is shown, that entanglement measure called *squashed entanglement* [Tuc02, CW04] is an upper bound on $K_D$. This result has been recently generalized for multipartite key distillation protocols defined, in recent paper [YHH+07]. In particular it is shown that the *multipartite squashed entanglement* is also an upper bound on distillable key. Although the latter result is much stronger than the one we have presented, it uses independent result, that an optimal key distillation protocol uses only communication which is linear in number of input copies.

As we have invoked in Section 4.4.1, some properties of $K_D$ as entanglement measure, was in studied in [Chr06]. Some sufficient conditions for key distillability

in terms of the p-squeezed state was provided in [CCK$^+$07]. The link between key distillability and uncertainty principle is shown in [Koa07].

In [MCL06] other upper bound on distillable key are developed for practical protocols of key extraction, the so called *unconditionally secure quantum key distribution protocols* (see Section 5.6, for detail formulation). Although these new bound beats the $E_r^\infty$, it is demonstrated, that providing better devices involved in realization of the protocol, the $E_r^\infty$ bound can be still competitive with the new one.

### 4.7.1 Open problems

These are exemplary open questions that rises in context of distillable key:

1. For which bipartite states $\rho$ there are protocols which achieving $K_D$ achieves at the same time $E_D$ ? (note, that exemplary are pure states for which protocols realizing $E_D$ realize at the same time $K_D$, since the two quantities are equal to each other)

2. (Upper bound on the key) Better upper bounds on $K_D$ than $E_r^\infty$ are welcome, that hold for all states, or indication which axiomatic monotones can yield better bound on which bipartite states.

3. Is $K_D$ monogamous, i.e. $K_D(\rho_{AB}) + K_D(\rho_{AE}) \leq \log Rank(\rho_A)$ for any pure state $|\psi_\rho\rangle_{ABE}$ with subsystems $\rho_{AB}$, $\rho_{BE}$ and $\rho_A$ respectively (note, that this holds for key distilled with use of one-way communication only [KW04])?

4. Is $K_D$ asymptotically continuous (see Section 4.4.2) or convex (see Section 4.4.2)?

5. (Irreversibility) For which states there holds $K_D(\rho) = K_C(\rho)$ [HHHO05c]?

# Chapter 5

# Secure key from certain PPT states

In this Chapter we present a slightly improved and extended version of the material, that can be found in [HHHO05a], in Section X, [HHHO05c] and [HPHH05]. We show that there are states which remain positive after partial transposition (PPT states) and have distillable key. We provide examples of bipartite states which are key distillable via two-way and one-way key distillation protocols. Interestingly, the only way we know that these states are entangled is that they are key distillable. Since PPT states have zero distillable entanglement, these are the first examples of bound entangled (entangled, with $E_D = 0$), key distillable (with $K_D > 0$) states (BE-KD).

In Section 5.1 we introduce the family of states denoted as $\mathcal{F}_{rec}$. It is further shown in Section 5.2, that some of states from this family, are PPT and key distillable (PPT-KD). This proof uses two facts: (i) some states from $\mathcal{F}_{rec}$ are PPT (ii) some PPT states from $\mathcal{F}_{rec}$ are close to private states. Since any state which is close enough to private state is key distillable, these states are PPT-KD, and hence also BE-KD (Theorem 5.7).

Subsequently, in Section 5.4, we introduce another family of states, denoted as $\mathcal{F}_s$, and show that all states from this family are PPT-KD. These states are unbiased mixtures of two pbits that have key parts in states orthogonal to each other, which assures their key distillability by Proposition 4.34. Moreover, by suitable choice of mixing probabilities they are also invariant under partial transposition.

In Section 5.4.1, we present some properties of $\mathcal{F}_s$. In particular, we show its subfamily with the highest distillable key among $\mathcal{F}_s$, and provide example of the state with this property. We then show that states from $\mathcal{F}_s$ lays on the boundary of (are *extremal* in) the set of PPT states.

Section 5.5 is devoted to reveal the way the states from $\mathcal{F}_{rec}$ were constructed [HHHO05a]. It involves the so called *hiding states* [TDL01, DLT02, EW02], and the so called R protocol. We sketch also the original way, some states from $\mathcal{F}_{rec}$ were shown to be PPT, presented in [HHHO05a].

In Section 5.3 we briefly comment on important consequences of existence of PPT-KD states. In Section 5.6 we present briefly further results on this subject, especially in context of the so called *unconditionally secure quantum key distribution.*

## 5.1 The family $\mathcal{F}_{rec}$

**Definition 5.1** *Consider states from* $B(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes (\mathcal{C}^{d^k} \otimes \mathcal{C}^{d^k})^{\otimes m})$*, with a matrix form*

$$\rho^{rec(m)}_{(d,k,p)} = \frac{1}{N_m} \begin{bmatrix} [p(\frac{\tau_1+\tau_2}{2})]^{\otimes m} & 0 & 0 & [p(\frac{\tau_1-\tau_2}{2})]^{\otimes m} \\ 0 & [(\frac{1}{2}-p)\tau_2]^{\otimes m} & 0 & 0 \\ 0 & 0 & [(\frac{1}{2}-p)\tau_2]^{\otimes m} & 0 \\ [p(\frac{\tau_1-\tau_2}{2})]^{\otimes m} & 0 & 0 & [p(\frac{\tau_1+\tau_2}{2})]^{\otimes m} \end{bmatrix}, \tag{5.1}$$

*where* $N_m$ *is appropriate normalizing factor,* $\tau_1 = (\frac{\rho_a+\rho_s}{2})^{\otimes k}$ *and* $\tau_2 = (\rho_s)^{\otimes k}$*, with* $\rho_s$ *and* $\rho_a$ *the symmetric and antisymmetric Werner state in* $B(\mathcal{C}^d \otimes \mathcal{C}^d)$*.*

*The family* $\mathcal{F}_{rec}$ *reads:*

$$\mathcal{F}_{rec} = \{\rho^{rec(m)}_{(d,k,p)} | d \geq 2, k \geq 1, p \in (0, \frac{1}{2}], m \geq 1\} \tag{5.2}$$

*The family of* $\mathcal{F}_{rec}$ *restricted to states* $\rho^{rec(m)}_{(d,k,p)}$ *with* $m = 1$*, is denoted as* $\mathcal{F}^{(m=1)}_{rec}$*.*

## 5.2 Proving that some PPT-KD states are within $\mathcal{F}_{rec}$

We set out to search for the parameters $(d, k, p)$ for which states from $\mathcal{F}_{rec}$ are PPT. The proof given here is direct, i.e. it does not base on the construction of the states from $\mathcal{F}_{rec}$, that was presented in [HHHO05a]. We first need the following definition:

**Definition 5.2** *A positive matrix acting on* $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ *with* $\dim A = \dim B = 2$ *and* $\dim A' = \dim B' \geq 2$ *written in a form*

$$\begin{bmatrix} A_{0000} & 0 & 0 & A_{0011} \\ 0 & A_{0101} & 0 & 0 \\ 0 & 0 & A_{1010} & 0 \\ A_{1100} & 0 & 0 & A_{1111} \end{bmatrix}. \tag{5.3}$$

*is simple-PPT if it satisfies (i) $A_{ijij}$ are PPT for $i,j \in \{0,1\}$, that is are positive itself and positive after partial transposition along $A' : B'$ cut, (ii) $A_{0011}$ is hermitian and $A^{\Gamma}_{0101} \geq |A^{\Gamma}_{0011}|$, and $\Gamma$ is partial transposition along $A' : B'$ cut.*

**Observation 5.1** *A simple-PPT matrix is a (possibly unnormalized) PPT state.*
**Proof.** Follows directly from the form of matrix (5.3) when subjected to partial transposition along AA':BB' cut (see Example 2.16), and Lemma A.3∎

**Lemma 5.2** *If a matrix (5.3) is simple-PPT, then this matrix with $A^{\otimes m}_{ijkl}$ and $m \geq 2$ in place of $A_{ijkl}$ is also simple-PPT.*
**Proof.** To see that property (i) is preserved, we note that there is

$$(D^{\otimes m})^{\Gamma} = (D^{\Gamma})^{\otimes m}. \tag{5.4}$$

for a positive matrix $D$ acting on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$, where $\Gamma$ is transposition along $A' : B'$ cut (see Section 2.5, Eq. (2.62)). Moreover, $A^{\Gamma}_{ijij}$ are positive because the matrix (5.3) is simple-PPT, and positivity is preserved under tensoring.

To see the property (ii) we first observe that hermiticity is preserved under tensoring. Moreover we know, that $\Gamma$ preserves hermiticity (see Section 2.5, Eq. (2.66)). We can prove now the second part of (ii). To this end we observe that for positive matrices, $D \geq A$ implies $D^{\otimes m} \geq A^{\otimes m}$ (see [Bha97]). This gives $(A^{\Gamma}_{0101})^{\otimes m} \geq |A^{\Gamma}_{0011}|^{\otimes m}$. Now, for hermitian matrices, there is $|A|^{\otimes m} = |A^{\otimes m}|$. This implies $(A^{\Gamma}_{0101})^{\otimes m} \geq |(A^{\Gamma}_{0011})^{\otimes m}|$. Finally, applying (5.4) on both sides of this inequality, we get desired inequality of (ii). ∎

**Observation 5.3** *If $\rho_{(d,k,p)} \in \mathcal{F}^{(m=1)}_{rec}$ is simple-PPT, then $\rho^{rec(m)}_{(d,k,p)} \in \mathcal{F}_{rec}$ is PPT.*
**Proof.** It is immediate from definition of the families under consideration, that the Lemma 5.2 applies, so that if $\rho_{(d,k,p)}$ is simple-PPT, the matrix $N_m \rho^{rec(m)}_{(d,k,p)}$ (an unnormalized matrix of $\rho^{rec(m)}_{(d,k,p)}$), is simple-PPT. This by Observation 5.1 implies that it is also a PPT state after normalization, which gives finally that $\rho^{rec(m)}_{(d,k,p)}$ is PPT. ∎

Hence, to assure a state $\rho^{rec(m)}_{(d,k,p)}$ from $\mathcal{F}_{rec}$ to be PPT, it is enough to assure $\rho^{rec(1)}_{(d,k,p)}$ from $\mathcal{F}^{(m=1)}_{rec}$ to be simple-PPT. We now show the parameters for which it holds.

**Lemma 5.4** *For $p \in (0, \frac{1}{3}]$ and any $k \geq 1$ there exists $d$ such that $\rho^{rec(1)}_{(d,k,p)}$ is simple-PPT. More specifically, the state $\rho^{rec(1)}_{(d,k,p)}$ is simple-PPT if and only if*

$$\begin{aligned} &0 < p \leq \frac{1}{3} \text{ and} \\ &\frac{1-p}{p} \geq \left(\frac{d}{d-1}\right)^k \end{aligned} \tag{5.5}$$

**Proof.** The matrix of the state $\rho^{rec(1)}_{(d,k,p)}$ after partial transposition has the form

$$\rho^{\Gamma}_{ABA'B'} = \begin{bmatrix} p(\frac{\tau_1+\tau_2}{2})^{\Gamma} & 0 & 0 & 0 \\ 0 & (\frac{1}{2}-p)\tau_2^{\Gamma} & p(\frac{\tau_1-\tau_2}{2})^{\Gamma} & 0 \\ 0 & p(\frac{\tau_1-\tau_2}{2})^{\Gamma} & (\frac{1}{2}-p)\tau_2^{\Gamma} & 0 \\ 0 & 0 & 0 & p(\frac{\tau_1+\tau_2}{2})^{\Gamma} \end{bmatrix}. \tag{5.6}$$

Since $\tau_1$ and $\tau_2$ are separable (and hence PPT), so is their mixture. Thus extreme-diagonal blocks of the above matrix are PPT, as well as the middle diagonal, proportional to $\tau_2$. It remains to check when the condition

$$(\frac{1}{2}-p)\tau_2^{\Gamma} \geq p|(\frac{\tau_1-\tau_2}{2})^{\Gamma}| \tag{5.7}$$

is satisfied, to obtain the parameters for which the state (5.6) is simple-PPT. Having $\rho_s = \frac{1}{d^2+d}(I+V)$ and $\rho_a = \frac{1}{d^2-d}(I-V)$ where $V$ swaps d-dimensional spaces and applying $V^{\Gamma} = dP_+$, (here exceptionally the projector onto state $|\Psi^{(d)}_+\rangle = \frac{1}{d}\sum_{i=0}^{d-1}|ii\rangle$ we denote as $P_+$), one easily gets that

$$\tau_1^{\Gamma} = \left(\frac{P_+^{\perp}}{d^2-1}\right)^{\otimes k} \tag{5.8}$$

$$\tau_2^{\Gamma} = \left(\frac{P_+^{\perp}}{d^2+d} + \frac{(1+d)P_+}{d^2+d}\right)^{\otimes k} \tag{5.9}$$

where $P_+^{\perp} \equiv I - P_+$ is projector onto subspace orthogonal to the projector onto maximally entangled state $P_+ = |\psi_+\rangle\langle\psi_+|$.

We check then the inequality

$$\begin{aligned} &(\frac{1}{2}-p)\left(\frac{P_+^{\perp}}{d^2+d} + \frac{(1+d)P_+}{d^2+d}\right)^{\otimes k} \geq \\ &\geq \frac{p}{2} \times \left| \left(\frac{P_+^{\perp}}{d^2-1}\right)^{\otimes k} - \left(\frac{P_+^{\perp}}{d^2+d} + \frac{(1+d)P_+}{d^2+d}\right)^{\otimes k} \right| \end{aligned} \tag{5.10}$$

To solve this inequality it is useful to represent the term on LHS as a sum:

$$\left(\frac{P_+^{\perp}}{d^2+d} + \frac{(1+d)P_+}{d^2+d}\right)^{\otimes k} = \left(\frac{P_+^{\perp}}{d^2+d}\right)^{\otimes k} + R \tag{5.11}$$

where operator $R$ is an unnormalised state which consists of all terms coming out of $k$-fold tensor product of $\left(\frac{P_+^\perp}{d^2+d} + \frac{(1+d)P_+}{d^2+d}\right)$ apart from the first term $\left(\frac{P_+^\perp}{d^2+d}\right)^{\otimes k}$. It is good to note that $R$ has support on subspace orthogonal to $(P_+^\perp)^{\otimes k}$. This fact allows to omit the modulus with appropriate change of sign, getting:

$$\begin{aligned}(\frac{1}{2} - p)\left[\left(\frac{P_+^\perp}{d^2+d}\right)^{\otimes k} + R\right] \geq \\ \geq \frac{p}{2}\left[(P_+^\perp)^{\otimes k}\left(\frac{1}{(d^2-1)^k} - \frac{1}{(d^2+d)^k}\right) + R\right],\end{aligned} \tag{5.12}$$

which is equivalent to (5.10). Since $R$ and $(P_+^\perp)^{\otimes k}$ are orthogonal, this inequality is equivalent to the following two inequalities

$$(\frac{1}{2} - \frac{3}{2}p)R \geq 0 \tag{5.13}$$

$$\begin{aligned}(\frac{1}{2} - p)\left(\frac{P_+^\perp}{d^2+d}\right)^{\otimes k} \geq \frac{p}{2}(P_+^\perp)^{\otimes k} \times \\ \times \left(\frac{1}{(d^2-1)^k} - \frac{1}{(d^2+d)^k}\right)\end{aligned} \tag{5.14}$$

To save first inequality one needs $p \leq \frac{1}{3}$. Preserving the second one requires

$$\frac{1-p}{p} \geq \left(\frac{d}{d-1}\right)^k. \tag{5.15}$$

This however is fulfilled for any $p \in (0, \frac{1}{3}]$ if $d$ is taken properly large for some fixed k. Indeed, the $k$-th root of $\frac{1-p}{p}$ (which converges to 1 with k) can be greater than $\frac{d}{d-1}$ (which converges to 1 with d) for some large d. ∎

We study now for which parameters $(d, k, p)$ and $m$ the state $\rho_{(d,k,p)}^{rec(m)}$ from $\mathcal{F}_{rec}$ is key distillable.

**Proposition 5.5** *For $0 < \epsilon < 1/(8e^2)$ and $p \in (\frac{1}{4}, 1]$, there are $k$, $d$ and $m$ so, that the sate $\rho_{(d,k,p)}^{rec(m)}$ is close to a pbit:*

$$||\rho_{(d,k,p)}^{rec(m)} - \gamma^{(2)}|| \leq \delta(\epsilon) \tag{5.16}$$

*where $\delta(\epsilon) = 2\sqrt{4\sqrt{2\epsilon} + \eta(2\sqrt{2\epsilon})} + 2\sqrt{2\epsilon}$.*

**Proof.** We consider $\rho^{rec(m)}_{(d,k,p)}$ as is written in block form $\sum_{ijkl=0}^{1} |ij\rangle\langle kl| \otimes A_{ijkl}$ (5.42) (see the convention introduced in Section 2.58). Let us focus on the upper-right block of the matrix (5.42), without normalization factor $N_m$. We denote it $\tilde{A}_{0011}$ to distinguish from $A_{0011}$. Norm of this block equals:

$$\|\tilde{A}_{0011}\| = \left(\frac{p}{2}\right)^m ||((\frac{\rho_a - \rho_s}{2})^{\otimes k} - {\rho_s}^{\otimes k})^{\otimes m}|| = \left(\frac{p}{2}\right)^m \left(2(1-2^{-k})\right)^m = p^m(1-2^{-k})^m, \tag{5.17}$$

where second equality is consequence of the fact, that $\rho_a$ and $\rho_s$ have orthogonal supports which gives that $\rho_s^{\otimes k}$ is orthogonal to any term in expansion of $(\frac{\rho_a-\rho_s}{2})^{\otimes k}$ but the one $\frac{1}{2^k}\rho_s^{\otimes k}$. Thus the result is equal to norm of $[(\frac{\rho_a-\rho_s}{2})^{\otimes k} - \frac{1}{2^k}\rho_s^{\otimes k}]$ (which is $(1-\frac{1}{2^k})$) plus norm of the difference $|\frac{1}{2^k}\rho_s^{\otimes k} - \rho_s^{\otimes k}|$ which gives the above formula. Thus the norm of the upper-right block $A_{0011}$ of the state (5.42) is given by

$$\|A_{0011}\| = \frac{1}{N_m}\|\tilde{A}_{0011}\| = \frac{1}{2}(1-\frac{1}{2^k})^m \frac{1}{1+(\frac{1-2p}{2p})^m}. \tag{5.18}$$

We check now that one can increase this norm to be arbitrary close to $1/2$. Since $p > \frac{1}{4}$, we get that $(\frac{1-2p}{2p})^m$ converges to 0 with $m$. Although increasing $m$ diminishes the term $(1-\frac{1}{2^k})^m$, we can first fix $k$ large enough, so that the whole expression (5.18) will be arbitrarily close to $\frac{1}{2}$. Now, Theorem 3.19 assures that for any $0 < \epsilon_1 < 1/(8e^2)$, if only $\frac{1}{2}(1-\frac{1}{2^k})^m \frac{1}{1+(\frac{1-2p}{2p})^m} > 1/2 - \epsilon$, there is:

$$||\rho^{rec(m)}_{(d,k,p)} - \gamma^{(2)}|| \leq \delta(\epsilon), \tag{5.19}$$

with $\delta(.)$ vanishing as $\epsilon \to 0$, hence the assertion follows. ∎

We now show, that for ceratin parameters $(d,k,p)$, the states from $\mathcal{F}_{rec}$ are both PPT and key distillable (PPT-KD):

**Theorem 5.6** *There are PPT states, which approximate private states. More specifically, For any $\epsilon > 0$, and $p \in (\frac{1}{4}, \frac{1}{3}]$ there exist $k$, $d$ and $m$ such that $\rho^{rec(m)}_{(d,k,p)} \in PPT$ and $||(\rho^{rec(m)}_{(d,k,p)}) - \gamma^{(2)}|| \leq \epsilon$, for some pbit $\gamma^{(2)}$.*

**Proof.** Let us fix $\epsilon > 0$, and $p$ from interval $(1/4, 1/3]$. We choose now small enough $0 < \epsilon_1 < 1/(8e^2)$ so that $\delta(\epsilon_1) < \epsilon$, where $\delta(.)$ is defined in thesis of Proposition 5.5. It is possible, because $\delta$ vanishes whith $\epsilon_1$ approaching zero. By this proposition, there is high $m$ and for such $m$, high enough $k$, such, that the state $\rho^{rec(m)}_{(d,k,p)}$ (5.42) is close to pbit in trace norm distance up to $\delta(\epsilon_1) < \epsilon$. We can fix now also $m$ and $k$, and choose $d$ so large that by Lemma 5.4 the state $\rho^{rec(1)}_{(d,k,p)}$ is PPT. This however

assures by Observation 5.3 that simultaneously the state $\rho^{rec(m)}_{(d,k,p)}$ is also PPT and the assertion follows. ∎

We now collect the facts that we know about states from $\mathcal{F}_{rec}$ to obtain the theorem which proves that some of them are bound entangled and key distillable.

Let us first note, that in general, states which are PPT and approximate private states are entangled. This is because separable states can not approximate private states (Observation 4.20). Now, since PPT states have $E_D = 0$, PPT states which approximate private states are bound entangled. We can now formulate a desired result, which uses this fact in present context:

**Theorem 5.7** *There are bound entangled states that have nonzero distillable key.*
**Proof.** From Theorem 5.6, it follows that for any $\epsilon > 0$, there are parameters $(d, k, p)$ such that the states $\rho^{rec(m)}_{(d,k,p)}$ from $\mathcal{F}_{rec}$ are both PPT and within $\epsilon$ distance in trace norm to some private bit. These states are entangled, since as we have shown in Observation 4.20, it is impossible for separable states to approximate private states. Since they are PPT and entangled, by Theorem 2.28, they are bound entangled. Finally, by Theorem 4.30, the states close by $\delta < 10^{-3}$ in trace norm to private bits are key distillable. Since $\epsilon > 0$ can be taken arbitrarily small the latter can be achieved, which ends the proof of this theorem. ∎

The above theorem is one of the main results of this thesis. We discuss its major consequences in the next section.

## 5.3 Interpretation of the existence of BE-KD states: possibility of teleportation and communicating in private do not coincide in general

The fact, that there are BE-KD states has fundamental meaning for better understanding of both the privacy present in bipartite quantum states and their entanglement. From example 2.6.1 (the phenomenon of teleportation), we know, that sharing maximally entangled states allows for quantum communication. On the other hand, it is shown in [HHH99], that sharing bound entangled states does not allow for such possibility. Since PPT-KD states are bound entangled, their existence implies that possibility of sending qubits, is only sufficient, but not necessary condition for private communication. Moreover, from results of [HHH99], it follows that existence of PPT-KD states receives the interpretation in terms of the so called *channel capacities*. Namely, it means that there are quantum channels with zero quantum capacity, but non-zero private capacity. Another cryptographical formulation of this fact is that pure entanglement is only the sufficient condition of privacy, but not necessary.

The interpretation of this phenomenon from entanglement theory point of view, is that bound entanglement can be useful for some task, which was not clear at all (see [Mas05] for more general results in this subject). The PPT-KD states are also the first bound entangled states for which the fact that they are entangled is understood in operational way: they are key distillable.

## 5.4 One-way key distillable bound entangled states - construction of the family $\mathcal{F}_s$

We construct here the class $\mathcal{F}_s$ of bound entangled states of the form $\rho = p_1\gamma_1 + p_2\gamma_2$, where $\gamma_1$ and $\gamma_2$ are key-part-orthogonal private bits, i.e. such that their key parts are orthogonal: $\mathrm{Tr}[\mathrm{Tr}_{A'B'}\gamma^{(2)}_{ABA'B'}\mathrm{Tr}_{A'B'}\tilde{\gamma}^{(2)}_{ABA'B'}] = 0$.

Recall first, that any private bit from $B(\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^d \otimes \mathcal{C}^d)$ on systems ABA'B', can be represented in its $X$-form by an operator $X$ of trance norm 1, which uniquely determines it (see Section 3.4.2), so that the mixture of two pbits represented by $X_1$ and $X_2$ that are key-part-orthogonal has matrix form:

$$\rho = \frac{1}{2}\begin{bmatrix} p_1\sqrt{X_1X_1^\dagger} & 0 & 0 & p_1X_1 \\ 0 & p_2\sqrt{X_2X_2^\dagger} & p_2X_2 & 0 \\ 0 & p_2X_2^\dagger & p_2\sqrt{X_2^\dagger X_2} & 0 \\ p_1X_1^\dagger & 0 & 0 & p_1\sqrt{X_1^\dagger X_1} \end{bmatrix}. \tag{5.20}$$

in some product basis, which we choose now to be a standard basis. The essential part of the construction of $\mathcal{F}_s$ is the following substitution: $X_1 = \frac{1}{||W_U||}W_U$ where

$$W_U = \sum_{ij} u_{ij}|ij\rangle\langle ji| \tag{5.21}$$

and $u_{ij}$ are matrix elements of some unitary matrix $U$ on $\mathcal{C}^d$. The second operator we choose $X_2 = \frac{W_U^\Gamma}{||W_U^\Gamma||}$ with $\Gamma$ being partial transposition on subsystem $B'$. The corresponding mixing probabilities are

$$p_1 = \frac{||W_U||}{||W_U|| + ||W_U^\Gamma||} \quad p_2 = \frac{||W_U^\Gamma||}{||W_U|| + ||W_U^\Gamma||} \tag{5.22}$$

respectively.

In turn we obtain a desired family of states $\mathcal{F}_s$. These are states on systems $ABA'B'$ with $\dim A = \dim B = 2$ and $\dim A' = \dim B' = d$, that can be written in a form

$$\rho_U = \frac{1}{N}\begin{bmatrix} \sum_{ij}|u_{ij}||ij\rangle\langle ij| & 0 & 0 & \sum_{ij}u_{ij}|ij\rangle\langle ji| \\ 0 & \sum_i |ii\rangle\langle ii| & \sum_{ij}u_{ij}|ii\rangle\langle jj| & 0 \\ 0 & \sum_{ij}u^*_{ij}|jj\rangle\langle ii| & \sum_i |ii\rangle\langle ii| & 0 \\ \sum_{ij}u^*_{ij}|ji\rangle\langle ij| & 0 & 0 & \sum_{ij}|u_{ij}||ji\rangle\langle ji| \end{bmatrix} \quad (5.23)$$

with $N = 2(\sum_{i,j=0}^{d-1}|u_{ij}||ij\rangle\langle ij| + d)$, the indices $i, j \in \{0, \ldots, d-1\}$ in the summations, and $U$ a unitary transformation with at least $d+1$ nonzero matrix elements when written in standard basis.

We can prove now the essential property of the states from $\mathcal{F}_s$.

**Proposition 5.8** *For $\rho = p\gamma_1 + (1-p)\gamma_2 \in \mathcal{F}_s$, where $\gamma_1$ and $\gamma_2$ are key-part-orthogonal pbits, $\rho$ is both PPT and key distillable. Moreover it is invariant under partial transposition (PT-invariant), and has $K_D(\rho) \geq 1 - h(p_1)$,*

**Proof.** Let $\rho = \rho_U \in \mathcal{F}_s$ with $U$ a unitary transformation from definition of $\mathcal{F}_s$. It is easy to observe first that $[W_U W_U^\dagger]^{\frac{1}{2}} = \sum_{ij}|u_{ij}||ij\rangle\langle ij|$ and $[W_U^\dagger W_U]^{\frac{1}{2}} = \sum_{ij}|u_{ij}||ji\rangle\langle ji|$. In both cases after normalisation by factor $||W_U||$ we obtain separable, PT-invariant state. Moreover $[W_U^\Gamma (W_U^\Gamma)^\dagger]^{\frac{1}{2}} = [(W_U^\Gamma)^\dagger W_U^\Gamma]^{\frac{1}{2}} = \sum_i |ii\rangle\langle ii|$, (again after normalisation giving PT-invariant separable state). From this we obtain that $\rho_U$ with is PT-invariant. At the same time we have desired security condition $p_1 > p_2$ if only

$$\frac{p_1}{p_2} = \frac{||W_U||}{||W_U^\Gamma||} = \frac{\sum_{ij}|u_{ij}|}{d} > 1. \quad (5.24)$$

The above inequality is satisfied for a unitary U which written in $\{|ij\rangle\}$ basis has more than $d$ nonzero entries. Indeed $\sum_{ij}|u_{ij}|^2 = d \leq \sum_{ij}|u_{ij}|$ by unitarity of $U$ (note, that for each $i$, the $|u_{ij}|^2$ are probabilities). This inequality is strict, if only there are $d+1$ nonzero elements, since in this case there is a column with two nonzero elements, that has the sum of their modulus strictly greater than the sum of the squares of their modulus. The fact that $K_D(\rho_U) \geq 1 - h(p)$ follows from Proposition 4.34, since $\rho_U$ is a mixture of two key-part-orthogonal private states. Hence, they are BE-KD states, because separable states are not key distillable (see discussion in Section 4.6.1). ∎

Thus, we have a large class of states that contain secure key and are bound entangled.

**Remark 5.9** *The choice of $X_1$ and the element $\sqrt{X_2 X_2^\dagger}$ which assures positivity of the matrix (5.20) with blocks of zeros in place of the two off-diagonal blocks: $X_2$ and $X_2^\dagger$ has been found using numerical methods by Ł Pankowski [Pan05]. By now,*

*no algorithm is known, that decides for which operator of the form $p_1 X_1$ there is an operator of the form $(1-p_1)\sqrt{X_2 X_2^\dagger}$ which assures $\rho$ to be a PPT state. Interestingly, the private bit determined by $X_2$ in $X$-form is a flower state, that was presented in Chapter 3.*

### 5.4.1 Some properties of $\mathcal{F}_s$

**Observation 5.10** *The ratio of $p_1$ and $p_2$ in (5.24) which is related to key rate $C_D^{DW} \geq 1 - h(p_1)$ achieves the highest value for unimodular unitaries $U$ (ie. such that $|u_{ij}| = \frac{1}{\sqrt{d}}$). Then it amounts to $[\frac{p_1}{p_2}]_{optimal} = \sqrt{d}$.*

**Proof.** We use the Lagrange multipliers method for the following function: $f : R^{d^2} \setminus \{0\} \to R_{>0}$, defined as $f(\vec{u}) = \sum_{ij=0}^{d-1} |u_{ij}|^2$, with the constraint $g : R^{d^2} \setminus \{0\} \to R_{>0}$ defined as $g(\vec{u}) = \sum_{ij} |u_{ij}|^2 - d$ (see e.g. [wik08b]). It is easy to see, that this method gives desired optimality of ratio $\frac{p_1}{p_2} = \frac{1}{\sqrt{d}}$. We only have to argue, that the constraint $g$ is proper in our context. The constraint that follows from assumption is just a unitarity condition: $UU^\dagger = \mathrm{I}$, that reads:

$$\sum_{ijk=0}^{d-1} u_{ij} u_{kj}^* = \delta_{i,k}. \tag{5.25}$$

It follows then, that for each $i$, with $k = i$ there is

$$\sum_{j=0}^{d-1} |u_{ij}|^2 = 1. \tag{5.26}$$

This condition allows us for the constraint $g$, which is more general - can be satisfied by non-unitary matrices as well. Fortunately, the maximum can be attained by unitary matrices as well, e.g. by the unimodular unitary transformations presented in proof of Corollary 3.12. ∎

**Example of $4 \otimes 4$ bound entangled states with $K_D > 0$ from $\mathcal{F}_s$**

Setting $d = 2$ in (5.23) we obtain the smallest $(4 \otimes 4)$ PPT-KD states from family $\mathcal{F}_s$. An easy example is a state with $U$ equal to 1-qubit Hadamard gate $H$ (see Section 2.2.2). The state $\rho_H$ can be written as a mixture of Bell states on $AB$ subsystem of state, that are 'classically' correlated with some other states on $A'B'$. Namely we have

$$\varrho_H = \sum_i q_i |\psi_i\rangle\langle\psi_i|_{AB} \otimes \varrho_{A'B'}^{(i)} \tag{5.27}$$

where the correlated states are the following:

$$\begin{aligned}\varrho^{(0)} &= \frac{1}{2}[P_{00} + P_{\psi_2}] \\ \varrho^{(1)} &= \frac{1}{2}[P_{11} + P_{\psi_3}] \\ \varrho^{(2,3)} &= P_{\chi_\pm}\end{aligned} \tag{5.28}$$

with $P_{\psi_i}$ being projectors onto corresponding maximally entangled states: $|\psi_{0,1}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi_{2,3}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ and $P_{\chi_\pm}$ projectors onto pure states

$$\chi = \frac{1}{\sqrt{2 \pm \sqrt{2}}}(|00\rangle \pm |\psi_0\rangle) \tag{5.29}$$

respectively. The mixing distribution $\{q_i\}_{i=0}^3$ is $\{\frac{p_1}{2}, \frac{p_1}{2}, \frac{p_2}{2}, \frac{p_2}{2}\}$. Since $d = 2$, one has $p_1 = \frac{\sqrt{2}}{1+\sqrt{2}}$, so by proposition 4.34 a positive key rate can be gained from this 4-qubit PPT state. It reads:

$$C_D^{DW}(\varrho_H) = 1 - h(p_1) = 0.0213399. \tag{5.30}$$

We will show now, that state $\rho_H$ is extremal in set of PPT states in $B(\mathcal{C}^4 \otimes \mathcal{C}^4)$. To this end, we acquire topological definitions of the neighbourhood of a point and the boundary of a set in metric space:

**Definition 5.3** *(see e.g. [wik08c]) In metric space a set $V$ is neighbourhood of a point $p$, if there is an open ball with center at $p$ and radius $r$,*

$$B(p, r) = \{x : ||x - s|| < r\},$$

*which is contained in $V$.*

**Definition 5.4** *(see e.g. [wik08d]) For a subset $S$ of topological space $X$, the set of points $p$ of $X$ such that every neighborhood of $p$ contains at least one point of $S$ and at least one point not of $S$.*

If a point $p$ belongs to a boundary, we say, that it is *extremal* in $S$. In our context, we identify $X$ with $B(\mathcal{C}^d \otimes \mathcal{C}^{d'})$, for some $d, d' \geq 2$ that will be fixed later, and $S$ with the set of $PPT$ states (PPT) in $B(\mathcal{C}^d \otimes \mathcal{C}^{d'})$. Since PPT is closed, we have $\partial PPT \subset PPT$. Using this terminology, we can formulate the following observation:

**Observation 5.11** *The state $\varrho_H$ is extremal in PPT.*

**Proof.** We show it by constructing a sequence of balls with center at $\rho_H$ and vanishing radius, which contains a point out of PPT (i.e. NPT). Recall that $\varrho_H$ is

a mixture of the form (5.20) with $X_1 = W_H$ and $X_2 = X_1^\Gamma$. It is straightforward to check, that any such mixture with $p_1 \neq \frac{\sqrt{2}}{1+\sqrt{2}}$ gives an NPT state. Changing weight of $p_1$ we can interpolate between the two pbits and any point on a line $L = \{\rho | \rho = p_1\gamma_{X_1} + p_2\gamma_{X_2}\}$ but $\rho_H$ is NPT. Hence for every ball B with nonzero radius with center at $\rho_H$, there is some NPT state in $B \cap L$. Let us fix some neighbourhood $N(\rho_H)$ of $\rho_H$. By Definition 5.3, it contains a ball $B(\rho_H, r)$ for some $r > 0$. We have then, that $N(\rho_H)$ contains $\rho_H \in PPT$ and some state from $B(\rho_H, r) \cap L$ which is NPT, hence the assertion follows.∎

**Remark 5.12** *The same argument as in the above observation proves extremity of the state $\varrho_U$ with $X_1 = W_U$, if only $X_1$ is hermitian operator, and either $X_1$ or $X_1^\Gamma$ has some positive eigenvalue.*

## 5.5 On the construction of bound entangled states with nonzero distillable key

In previous sections we have presented PPT-KD states from family $\mathcal{F}_{rec}$. They are of quite special form, which at first may appear strange. One can ask if it is just a coincidence that states of such structure are PPT-KD. The original way in which these states were constructed in [HHHO05a] gives the answer to this question. The fact that the states are PPT-KD, can be understood from their structure. It is therefor instructive to follow the way in which these states were designed. From this, it will follow that the paradigm of private states presented in previous chapters perfectly suits the goal of getting PPT-KD states, giving insightful view on the existence of PPT-KD states in general. We sketch also briefly the original idea of the proof that some states from $\mathcal{F}_{rec}$ are PPT.

The construction of $\mathcal{F}_{rec}$ (5.1) is divided into three steps:

1. Construct states $\rho^{de}_{(d,k)}$, which approximate pbits (for large enough k), but have vanishing $E_D$ (for large enough d).

2. Admix special separable state $\rho_{noise}$ to get the family of states

$$\mathcal{F}^{(m=1)}_{(d,k,p)} = \{\rho_{(d,k,p)} = 2p\rho^{de}_{(d,k)} + (1-2p)\rho_{noise} \,|\, d \geq 2,\, k \geq 1,\, p \in (0,1]\}, \quad (5.31)$$

   such that $\rho_{(d,k,p)} \in PPT$, for certain $d, k, p$.

3. Apply the probabilistic LOCC transformation called R protocol to obtain from $\rho^{\otimes m}_{(d,k,p)}$ for sufficiently high $m$ the states from $\mathcal{F}_{rec}$, with nonzero probability.

### 5.5.1 On hiding states and how to construct approximate pbits with arbitrarily small $E_D$

In this section we first invoke the scheme and main achievements of *quantum data hiding* [TDL01, DLT02], and show its connection with the structure of private states with hermitian $X$ when written in $X$ form. Basing on this we argue that ceratin states approximate private states, yet have arbitrarily small distillable entangled states (see Section 5.5.1).

#### Hiding states

In scenario of distinguishing states (see e.g. [HMM$^+$06] and references therein) in case of two states we are given one of two bipartite states $\rho_0$ and $\rho_1$ with probability $p_0$ and $p_1$ respectively. We can perform quantum operations from some class of operations OP, and at the end guess which state we were given. The guess is inconclusive, that is we may be wrong. Our aim is to find an operation which maximises probability of a good guess. Since what matters is just a probability of success, instead of optimizing over operations we can optimize over corresponding POVMs. For $OP$ being the set of all quantum operations, it is easy to argue, that optimal POVM which distinguishes between two states has only two elements $E_0$ and $E_1$, and the probability of success is given by

$$p_{s(Q)}(\rho_0, \rho_1) = p_0 Tr E_0 \rho_0 + p_1 Tr E_1 \rho_1. \tag{5.32}$$

(A formula for $p_{s(OP)}$ with OP a general class of operations see chapter 6). In this case, the famous Helstrom formula holds, which for $p_0 = p_1 = \frac{1}{2}$ gives:

$$p_{s(Q)}(\rho_0, \rho_1) = \frac{1}{2} + \frac{1}{4}||\rho_0 - \rho_1||. \tag{5.33}$$

One can expect, that if the class $OP$ is restricted, e.g. equal to LOCC, the probability becomes smaller. Surprisingly, the recent results shows that the difference between the $p_{s(LOCC)}$ and $p_{s(Q)}$ can be extremal, i.e. almost $\frac{1}{2}$. This phenomenon was found by DiVincenzo, Leung and Terhal in [TDL01, DLT02], and exploited to develop a so called *quantum data hiding* scheme. According to the latter, one can hide one bit of information by correlating the bit with a pair of states $\{\rho^{hide1}, \rho^{hide2}\}$, which are

(i) almost indistinguishable by means of LOCC operations: $p_{s(LOCC)}(\rho^{hide1}, \rho^{hide2}) \approx \frac{1}{2}$,

(ii) almost distinguishable by means of quantum operations $p_{s(Q)}(\rho^{hide1}, \rho^{hide2}) \approx 1$.

Any pair of states satisfying these two properties is called a pair of *hiding* states. The resulting state with the hidden bit on system $C$ is of the form:

$$\rho_{hb} = \frac{1}{2}|0\rangle\langle 0|_C \otimes \rho_{AB}^{hide1} + \frac{1}{2}|1\rangle\langle 1|_C \otimes \rho_{AB}^{hide2}. \tag{5.34}$$

The bit on system $C$ is inaccessible to the parties who perform LOCC operations on system $AB$ thanks to property (i), yet it can be reviled if they come together and perform quantum operation, which is assured by property (ii).

This amusing phenomenon has been developed by Eggeling and Werner in [EW02]. They have found a pair of hiding states $\tau_1$ and $\tau_2$ (called further EW hiding states), which are additionally both separable, which appears to be crucial in our further considerations. Eggeling and Werner also derived a general upper bound (called further *EW bound*) on probability of distinguishing by means of PPT operations (and hence also LOCC operations), which can be seen as a counterpart of Helstrom formula (see Proposition 6.1):

$$p_{s(PPT)}(\rho_1, \rho_2) \leq \frac{1}{2} + \frac{1}{4}||\rho_1^\Gamma - \rho_2^\Gamma||. \tag{5.35}$$

where $\Gamma$ denotes the operation of partial transposition (Def. 2.7). The EW hiding states are

$$\tau_1 = (\frac{\rho_s + \rho_a}{2})^{\otimes k}, \quad \tau_2 = (\rho_s)^{\otimes k}, \tag{5.36}$$

with $\rho_s$ and $\rho_a$ the symmetric and antisymmetric Werner states acting on $d \times d$ dimensional Hilbert space (See Eq. (3.53)). To improve distinguishability via quantum operations one needs to increase $k$. To make at the same time arbitrarily small LOCC distinguishability, one needs to increase initial dimension $d$. It is shown in [EW02], that for the pair $\{\tau_1, \tau_2\}$, the EW bound is small, hence they are hiding.

### Approximate pbits with almost zero $E_D$

We now adopt the idea of hiding bits to find states with arbitrarily small distillable entanglement, yet with non vanishing amount of distillable key. In [HHHO05a], this method was called 'hiding entanglement', as in this way we have 'hide' maximally entangled states. We do not use this name in present context, as we preserve it for the issue of distinguishing entangled states from separable states (see Chapter 6).

Instead of bits one can correlate two, orthogonal maximally entangled states with the two hiding $\tau_1$, $\tau_2$ states to obtain:

$$\rho_{(d,k)}^{de} = \frac{1}{2}|\phi_+\rangle\langle\phi_+|_{AB} \otimes \tau_1^{A'B'} + \frac{1}{2}|\phi_-\rangle\langle\phi_-|_{AB} \otimes \tau_2^{A'B'} \tag{5.37}$$

Now, the two properties of hiding states which we have invoked, are connected the two new properties of some states $\rho_{(d,k)}^{de}$, for sufficiently high $d$ and $k$:

(i) $E_D(\rho^{de}_{(d,k)}) \approx 0$ ($E_D$ is decreased)

(ii) $K_D(\rho^{de}_{(d,k)}) \approx 1$, (approximate pbit)

We will not use these properties directly, however it appears that the successful construction of PPT-KD states within $\mathcal{F}_{rec}$ is tightly connected to these two properties. Namely, it is easier to construct a PPT-KD state from state with a gap between $E_D$ and $K_D$, when $E_D$ is already small. To serve a background, but not to diverge too much from the subject, we give only the idea of the proof of these two properties.

The idea of the proof of (i) is the following. Adapting Lemma 3.7, to states of the form (5.37), one gets $E_N(\rho^{de}_{(d,k)}) = \log(1 + \frac{1}{2}||\tau_1^\Gamma - \tau_2^\Gamma||)$. The quantity $||\tau_1^\Gamma - \tau_2^\Gamma||$ appears in the Eggeling Werner bound (5.35), which is small for $\tau_1$ and $\tau_2$. Hence, also $E_N$ is small, and small is finally the $E_D$ upper bounded by $E_N$ [VW02]. The higher $d$, the smaller $E_D$ becomes.

The idea to see (ii) is to compare states $\rho^{de}_{(d,k)}$ to a pbit. Because $\tau_i$ are hiding, they are orthogonal i.e. satisfy $\frac{1}{2}||\tau_1 - \tau_2|| > 1 - 2\epsilon$, for some $\epsilon$. Now, writing $\rho^{de}_{(d,k)}$ in block form $\sum_{ijkl=0}^{1} |ij\rangle\langle kl| \otimes A_{ijkl}$ one can see, that $A_{0011} = \frac{1}{4}(\tau_1 - \tau_2)$. Hence, $||A_{0011}|| > \frac{1}{2} - \epsilon$. This by Proposition 3.19 implies that $\rho^{de}_{(d,k)}$ is close to some private bit in trace norm, providing sufficiently small $\epsilon$, which can be achieved by increasing parameter $k$. We know also by Theorem 4.30, that if $\rho^{de}_{(d,k)}$ is close enough to pbit, then its distillable key tends to 1. The fact, that $K_D(\rho^{de}_{(d,k)}) \leq 1$ follows from Proposition 3.13.

It might be a good place to note, that choosing $\rho^{de}_{(d,k)}$ as a starting point, had double advantage. First, because $\tau_1$ and $\tau_2$ are hiding, $\rho^{de}_{(d,k)}$ does not allow for distillation of entanglement by just distinguishing them. Second, as it was mentioned, this particular hiding states are separable, so they do not bring in any entanglement.

### 5.5.2 From approximate pbit with small $E_D$, to PPT states...

Having constructed states $\rho^{de}_{(d,k)}$, that approximate pbits with small $E_D$, we are ready to make them PPT, i.e. with zero $E_D$. This transformation fortunately does not decrease distillable key too much. In this way we obtain the family $\mathcal{F}^{(m=1)}_{rec}$, which is the second step to construct $\mathcal{F}_{rec}$. The parameters $k$ and $d$ of $\mathcal{F}^{(m=1)}_{rec}$ are inherited from $\rho^{de}_{(d,k)}$. We introduce now the parameter $p$.

To this end, we first observe, that the state:

$$\rho^{de}_{(d,k)} = \begin{bmatrix} \frac{1}{2}(\frac{\tau_1+\tau_2}{2}) & 0 & 0 & \frac{1}{2}(\frac{\tau_1-\tau_2}{2}) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2}(\frac{\tau_1-\tau_2}{2}) & 0 & 0 & \frac{1}{2}(\frac{\tau_1+\tau_2}{2}) \end{bmatrix}, \tag{5.38}$$

is obviously negative after partial transposition (is NPT). Indeed, consider partial transposition over system $BB'$ (i.e. transposition on system $BB'$ only). It is a composition of partial transpositions of $B$ and $B'$ subsystems, transforming the state (5.38) into:

$$\begin{aligned} \rho^{\Gamma}_{ABA'B'} &= (I_A \otimes T_B \otimes I_{A'} \otimes T_{B'})(\rho_{ABA'B'}) = \\ &= \begin{bmatrix} \frac{1}{2}(\frac{\tau_1+\tau_2}{2})^{\Gamma} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2}(\frac{\tau_1-\tau_2}{2})^{\Gamma} & 0 \\ 0 & \frac{1}{2}(\frac{\tau_1-\tau_2}{2})^{\Gamma} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2}(\frac{\tau_1+\tau_2}{2})^{\Gamma} \end{bmatrix} \end{aligned} \tag{5.39}$$

where $\Gamma$ denotes partial transposition over subsystem $B'$ (as partial transposition over B caused interchange of blocks of matrix of (5.38), see Example 2.16). This matrix is obviously not positive for the lack of middle-diagonal blocks. To prevent this we admix to $\rho^{de}_{(d,k)}$ a separable state $\frac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \tau_2$ with a probability $(1-2p)$, where $p \in (0, \frac{1}{2}]$. It's matrix reads then

$$\rho_{(d,k,p)} = \begin{bmatrix} p(\frac{\tau_1+\tau_2}{2}) & 0 & 0 & p(\frac{\tau_1-\tau_2}{2}) \\ 0 & (\frac{1}{2}-p)\tau_2 & 0 & 0 \\ 0 & 0 & (\frac{1}{2}-p)\tau_2 & 0 \\ p(\frac{\tau_1+\tau_2}{2}) & 0 & 0 & p(\frac{\tau_1+\tau_2}{2}) \end{bmatrix}, \tag{5.40}$$

In subscript we explicitly write the parameters on which this state depends implicitly: $d = d_{A'} = d_{B'}$ is the dimension of symmetric and antisymmetric Werner states used for hiding states (5.36) and $k$ is parameter of tensoring in their construction. Thus we have the desired family of states:

$$\mathcal{F}^{(m=1)}_{rec} = \{\rho_{(d,k,p)} \,|\, d \geq 2,\, k \geq 1,\, p \in (0,1]\}, \tag{5.41}$$

in accordance with Definition 5.1. As it was shown in Lemma 5.4, these states are PPT for certain range of parameters $(d, k, p)$.

### 5.5.3 ... and back - to approximate pbits in higher dimensions, using PPT states and recurrence protocol

In this section we finalize the construction of states from $\mathcal{F}_{rec}$. These are the states from $\mathcal{F}_{rec}^{(m=1)}$ but improved via the probabilistic LOCC operations performed on some number $m$ of the copies of the latter. The probabilistic operations, forming an R protocol gives with nonzero probability state from $\mathcal{F}_{rec}$, which is much closer to a pbit, than the states from $\mathcal{F}_{rec}^{(m=1)}$.

To this end, we first describe the following LOCC procedure, that will be central for obtaining more and more secure states out of $\rho_{(d,k,p)}^{\otimes m}$.

#### Recurrence protocol for getting states close to pbits

In this section we introduce a protocol, called *recurrence protocol* (R). It allows Alice and Bob sharing $\rho_{(d,k,p)}^{\otimes m}$ to obtain via two-way LOCC operation with nonzero probability a state which is close to private state. This protocol is a direct analogue of recurrence protocol introduced by Maurer in context of classical key agreement [Mau93], in analogy to approach of [BDSW96].

**Description of the R protocol**

Let Alice and Bob share $m$ copies of a state $\rho$. They take first system in the state $\rho$ as *source system*, and iterate the following procedure. In $i$-th step they take the $i$-th system in state $\rho$, and treat it as a *target system*. Let us remind that both systems have four subsystems $A$, $B$, $A'$ and $B'$. To distinguish the source and target system, the corresponding subsystems of the target system we call $\tilde{A}, \tilde{B}, \tilde{A}', \tilde{B}'$. On the source and target system they both perform a Control-NOT unitary operation[1] with the source at the $A(B)$ part of the source system and target at $\tilde{A}(\tilde{B})$ part of the target system for Alice (Bob) respectively. Then, they both measure the $\tilde{A}$ and $\tilde{B}$ subsystem of the target system in computational basis respectively, and compare the results. If the results agree, they proceed the protocol, getting rid of the $\tilde{A}\tilde{B}$ subsystem. If they do not agree, they abort the protocol i.e. trace out the state, and prepare (properly embedded) state $|22\rangle\langle 22|$. With nonzero probability of success they can perform this procedure $m-1$ times having each time the same source system. That is they start with $m$ systems in state $\rho$ and in each step (upon success) they use up one system and pass to the next step.

We will show now, that applying the R protocol to $\rho_{(d,k,p)}^{rec(1)} \in \mathcal{F}_{rec}$, one can obtain

[1]The Control-NOT operation (CNOT) is defined via acting on standard basis as follows: $CNOT|i\rangle_s|j\rangle_t := |i\rangle_s|i \oplus j\rangle_t$, where $s, t$ denotes the source and target system respectively.

$\rho^{rec(m)}_{(d,k,p)} \in \mathcal{F}_{rec}$ for $m > 1$. Let us recall, that they are of the form:

$$\rho^{rec(m)}_{(d,k,p)} = \frac{1}{N_m} \begin{bmatrix} [p(\frac{\tau_1+\tau_2}{2})]^{\otimes m} & 0 & 0 & [p(\frac{\tau_1-\tau_2}{2})]^{\otimes m} \\ 0 & [(\frac{1}{2}-p)\tau_2]^{\otimes m} & 0 & 0 \\ 0 & 0 & [(\frac{1}{2}-p)\tau_2]^{\otimes m} & 0 \\ [p(\frac{\tau_1-\tau_2}{2})]^{\otimes m} & 0 & 0 & [p(\frac{\tau_1+\tau_2}{2})]^{\otimes m} \end{bmatrix}, \tag{5.42}$$

where $N_m = 2[p^m + (\frac{1}{2}-p)^m]$. We first need the following observation about these states.

**Observation 5.13** *$\rho^{rec(m)}_{(d,k,p)}$ written in block form $\sum_{ijkl=0}^{1} |ij\rangle\langle kl| \otimes Z_{ijkl}$ satisfies $Z_{ijkl} = Z_{\bar{i}\bar{j}\bar{k}\bar{l}} = \frac{1}{N_m} W^{\otimes m}_{ijkl}$, where $W_{0000} = p(\frac{\tau_1+\tau_2}{2})$, $W_{0101} = (\frac{1}{2}-p)\tau_2$, $W_{0011} = p(\frac{\tau_1-\tau_2}{2})$ and $\bar{i}$ denotes binary negation of index $i$ with the same for $j, k, l$.*

**Proof.** Follows easily from definition of the family $\mathcal{F}_{rec}$.

In what follows we will refer to the property from the above observation, as to the symmetry&tensor property. We can pass now to desired lemma.

**Lemma 5.14** *The output of R protocol applied to $[\rho^{rec(1)}_{(d,k,p)}]^{\otimes m}$ has form $\rho^{(m)}_{out} = q^{(m)}_{RP}\rho^{rec(m+1)}_{(d,k,p)} + (1-q^{(m)}_{R})|22\rangle\langle 22|$, with $q^{(m)}_{RP} > 0$.*

**Proof.** We focus on the first step of the procedure, in a form general enough to show how the induction proves the result.

Let us consider the state $\rho_{ABA'B'} = \rho^{rec(1)}_{(d,k,p)}$ and arbitrary state $\sigma_{\tilde{A}\tilde{B}\tilde{A}'\tilde{B}'}$ from $B(\mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{B}} \otimes \mathcal{H}_{\tilde{A}'} \otimes \mathcal{H}_{\tilde{B}'})$ with $\dim\mathcal{H}_{\tilde{A}} = \dim\mathcal{H}_{\tilde{B}} = 2$. When both written in a block form, their tensor product reads:

$$\sigma_{\tilde{A}\tilde{B}\tilde{A}'\tilde{B}'} \otimes \rho_{ABA'B'} = \sum_{ijkl=0,rstv=0}^{1,1} |i\rangle\langle k|_A \otimes |j\rangle\langle l|_B \otimes X^{A'B'}_{ijkl} \otimes |r\rangle\langle t|_{\tilde{A}} \otimes |s\rangle\langle v|_{\tilde{B}} \otimes Y^{\tilde{A}'\tilde{B}'}_{rstv} \tag{5.43}$$

After applying the CNOT operations on systems $A\tilde{A}$ and $B\tilde{B}$ respectively, the above state reads:

$$\rho_{CNOTs} = \sum_{ijkl=0,rstv=0}^{1,1} |i\rangle\langle k|_A \otimes |j\rangle\langle l|_B \otimes X^{A'B'}_{ijkl} \otimes |r\oplus i\rangle\langle t\oplus k|_{\tilde{A}} \otimes |s\oplus j\rangle\langle v\oplus l|_{\tilde{B}} \otimes Y^{\tilde{A}'\tilde{B}'}_{rstv}. \tag{5.44}$$

The form of the output state follows from the fact, that upon result $|00\rangle\langle 00|$ on $\tilde{A}\tilde{B}$, the resulting (unnormalized) state has form:

$$\rho^{00}_{CNOTs} = \sum_{ijkl=0}^{1} |i\rangle\langle k|_A \otimes |j\rangle\langle l|_B \otimes X^{A'B'}_{ijkl} \otimes |0\rangle\langle 0|_{\tilde{A}} \otimes |0\rangle\langle 0|_{\tilde{B}} \otimes Y^{\tilde{A}'\tilde{B}'}_{ijkl}, \tag{5.45}$$

and upon result $|11\rangle\langle 11|$, the state reads:

$$\rho^{11}_{CNOTs} = \sum_{ijkl=0}^{1} |i\rangle\langle k|_A \otimes |j\rangle\langle l|_B \otimes X^{A'B'}_{ijkl} \otimes |1\rangle\langle 1|_{\tilde{A}} \otimes |1\rangle\langle 1|_{\tilde{B}} \otimes Y^{\tilde{A}'\tilde{B}'}_{\bar{i}\bar{j}\bar{k}\bar{l}}. \tag{5.46}$$

In first iteration, according to R, we have $\sigma_{\tilde{A}\tilde{B}\tilde{A}'\tilde{B}'} = \rho_{ABA'B'}$. By Observation 5.13, and equations (5.45) and (5.46), after this iteration there is:

$$\rho^{(2)}_{out} = \frac{\mathrm{Tr}_{\tilde{A}\tilde{B}}[\rho^{00}_{CNOTs} + \rho^{11}_{CNOTs}]}{\mathrm{Tr}[\rho^{00}_{CNOTs} + \rho^{11}_{CNOTs}]} = \rho^{rec(2)}_{(d,k,p)}. \tag{5.47}$$

It is also straightforward to check that

$$q^{(1)}_{RP} = \mathrm{Tr}[\rho^{00}_{CNOTs} + \rho^{11}_{CNOTs}], \tag{5.48}$$

which gives:

$$\begin{aligned} q^{(1)}_{RP} = (&\mathrm{Tr}X_{0000}\mathrm{Tr}Y_{0000} + \mathrm{Tr}X_{0101}\mathrm{Tr}Y_{0101} + \mathrm{Tr}X_{1010}\mathrm{Tr}Y_{1010} + \mathrm{Tr}X_{1111}\mathrm{Tr}Y_{1111}) + \\ &(\mathrm{Tr}X_{0000}\mathrm{Tr}Y_{1111} + \mathrm{Tr}X_{0101}\mathrm{Tr}Y_{1010} + \mathrm{Tr}X_{1010}\mathrm{Tr}Y_{0101} + \mathrm{Tr}X_{1111}\mathrm{Tr}Y_{0000}) \end{aligned} \tag{5.49}$$

This probability is nonzero since the entries $\mathrm{Tr}X_{ijij}$ sum up to 1, and $X_{ijij} = Y_{ijij}$ in this case.

If we assume now the thesis for $\rho^{rec(m)}_{(d,k,p)}$, we can substitute this matrix in place of $\sigma_{\tilde{A}\tilde{B}\tilde{A}'\tilde{B}'}$ to get analogues of the formulas (5.45) and (5.46). Now, again by Observation 5.13, both the matrix $\rho^{rec(1)}_{(d,k,p)}$ and $\rho^{rec(m)}_{(d,k,p)}$ satisfy the symmetry&tensor property. From this facts, in analogy to (5.47), $\rho^{(m)}_{out} = \rho^{rec(m+1)}_{(d,k,p)}$. The probability of obtaining this matrix is nonzero from the assumption that $q^{(m)}_{RP}$ is nonzero, and from the formula analogous to (5.49). This proves the assertion. ∎

### PPT states within $\mathcal{F}_{rec}$ - sketch of the original proof

Having described the construction, we are able to invoke the original argumentation for that some states from $\mathcal{F}_{rec}$ are PPT, given in [HHHO05a]. It can be called *operational*, since it follows from the fact, that:

- the probabilistic LOCC operations (such as R protocol) transforms PPT states into PPT states (see Theorem 2.17)

Hence, if we have assured the states from $\mathcal{F}^{(m=1)}_{rec}$ to be PPT, so must be the corresponding states from $\mathcal{F}_{rec}$, obtained by the R protocol, and the assertion follows. It is different from that we have presented in Section 5.2, in that it uses more general notions: of probabilistic LOCC operations, and the R protocol.

### 5.5.4 Remarks on general approach to distill key from biparite states

The choice of R protocol in construction of $\mathcal{F}_{rec}$ is not accidental. The original idea of [HHHO05a] was just to distill key from the states $\rho_{(d,k,p)}$, for which the R protocol was used. This fact did not receive clear enough statement in [HHHO05c, HHHO05a]. The fact, that some states from $\mathcal{F}_{rec}^{(m=1)}$ are also distillable, was noted explicitly in [CCK$^+$07]. We comment now on the use of the R protocol to distill key from these states.

The R protocol on input $\rho \in \mathcal{F}_{rec}^{(m=1)}$ outputs an approximate private state $\rho_{out} \in \mathcal{F}_{rec}$ only with nonzero probability $q_R$ of success. Thus, the R protocol can be called a *probabilistic key distillation protocol*, while Def. 4.1 of key distillation involves protocols which outputs approximate private states *with certainty*. It is however easy to make from the R protocol an LOCC operation which outputs state that is close to $\rho_{out}$ in trace norm, by amplifying probability $q_R$. One achieves this applying repetitively the probabilistic LOCC operation, and make appropriate postselection of the results. Success of this approach follows from the well known Chernoff bound. Since $\rho_{out}$ is an approximate private state, and reachable from $\rho$ via LOCC operation, such modified R protocol is legitimate key distillation protocol for $\rho$, which proves $K_D(\rho) > 0$.

It is easy to see that in fact, *any* probabilistic key distillation protocol can be turned into key distillation protocol via modification presented above. This approach: first distillation via some LOCC operation followed by the application of the MPDW protocol has been noted as necessary [CCK$^+$07], and in fact necessary and sufficient condition [AH06] for key distillability of any state (see Theorem 4.32).

In particular, not only the states which approximate private states such as PPT-KD states from $\mathcal{F}_{rec}$ are key distillable. Indeed: the PPT-KD states from $\mathcal{F}_s$ as well as $\mathcal{F}_{rec}^{(m=1)}$ are clearly far from private states in trace norm, as their p-squeezed states are so. It is the protocol of key distillation which transforms (many copies of) them into some (large) states that are close to private states.

#### On one and two-way key distillability

An interesting issue is the use of classical communication in the key distillation protocol. The MPDW protocol (see Section 4.6.5 and Sections 4.6.3,4.6.2) which we base on here, uses only one-way communication. This protocol gives key from the states $\rho_{(d,k,p)}^{rec(m)}$ and from $\mathcal{F}_s$. In [CCK$^+$07] it is argued, that the one-way key distillation MPDW can not be launched directly on states from $\mathcal{F}_{rec}^{(m=1)}$, as they have negative $C_D^{DW}$. Hence, the only way they are known to be key distillable is via use of the modified R protocol described above, which clearly uses two-way

communication, as the R does so. It seems thus, that the PPT-KD states from $\mathcal{F}_{rec}^{(m=1)}$ are distillable only by two-way key distillation protocols. One could think, that two-way communication may be needed here, because states from $\mathcal{F}_{rec}^{(m=1)}$ are far in trace norm from private states, and that this is general reason for two-way communication. As it is the main surprise of [HPHH05], this is not the case: the states from $\mathcal{F}_s$ are distillable via one-way MPDW protocol, despite of the fact, that they are far from private states.

### Searching for minimal dimension of BE-KD states in $\mathcal{F}_{rec}^{(m=1)}$

To check the key distillability of the states from $\rho \in \mathcal{F}_{rec}^{(m=1)}$, we will check if it is indicated by the sufficient condition, based on the R followed by Devetak-Winter protocol.

**Observation 5.15** *Some numerical investigations suggests that minimal dimension $d$, and parameter $k$ for which there is $p \in (\frac{1}{4}, \frac{1}{3}]$, such that $C_D^{DW}([(\rho_{(d,k,p)}^{rec(m)})^{ps}]^{ccq}) > 0$ is nonzero for some $m$, and $\rho_{(d,k,p)}$ is PPT, equals $d = 5$ and $k = 4$. In this case, minimal $m$ is $m = 6$. In particular there is*

$$C_D^{DW}([(\rho_{(5,3,\frac{1}{3})}^{rec(6)})^{ps}]^{ccq}) = 0.0336181. \tag{5.50}$$

**Proof.** To see this we use Lemma 4.33, which calculates the DW key rate for p-squeezed states of certain form. In our case, this rate reads:

$$C_D^{DW}([(\rho_{(d,k,p)}^{rec(m)})^{ps}]^{ccq}) = 1 - H((x+y, x-y, z, z)), \tag{5.51}$$

where $x = p^m/(2p^m + 2(1/2-p)^m)$, $y = (\frac{1}{2})(1-2^{(-k)})^m(1/(1+(\frac{1-2p}{2p})^m))$, $z = \frac{1}{2} - x$. The investigation of minimal parameters $d, k, m$ is as follows.

A simple search using `For` loop in `Mathematica 5.0` with 2D plot of the above rate function (5.51), yields that minimal $k$ for which it is positive for some range of $p \in (\frac{1}{4}, \frac{1}{3}]$ is $k = 3$. In this case minimal is $m = 6$, and $p$ is close to $1/3$. For example:

$$C_D^{DW}([(\rho_{(5,3,\frac{1}{3})}^{rec(6)})^{ps}]^{ccq}) = 0.0336181. \tag{5.52}$$

Increasing $m$ for smaller $k$ doeas not give hope for getting some $C_D^{DW}$ positive for $k < 3$, yet we did not perform an analytical proof of this fact.

Analogously, we do a brute-force test to find the minimal $d$ for which the function

$$f_{PPT}(p, d, k) := \frac{1-p}{p} - (\frac{d}{d-1})^k, \tag{5.53}$$

is not negative, assuring that $\rho^{rec(m)}_{(d,k,p)}$ is PPT. To this end we fix $k = 3$ and search for the smallest $d$ for which the plot of $p$ in range $(\frac{1}{4}, \frac{1}{3}]$ shows the $f_{PPT}$ to be positive.

We have found that minimal $d$ for which $f_{PPT} \geq 0$ with probability $p$ for which quantity (5.51) is positive, equals 5. Exemplary $p$ for which positivity of both (5.51) and (5.53) is satisfied with $k = 3, d = 5, m = 6$ equals $\frac{1}{3}$.

Thus we have numerical suggestion, that the smallest state $\rho_{(d,k,p)}$ which has positive distillable key occupies $\lceil \log(2^2 \times (d_0^{k_0})^2) \rceil = \lceil \log(4 \times (5^3)^2) \rceil = 16$ qubits.

**On key distillability of $2 \otimes n$ states**

In this section we consider states from $B(\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes n})$ for $n \geq 4$. In this case, there can be also some PPT entangled states, which have $E_D = 0$, yet may be key distillable. No such state is known so far.

Let us note, that all PPT-KD states constructed in this Chapter have the property, that their p-squeezed states are key distillable. We observe, that the states in $B(\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes n})$ for $n \geq 4$ does not have this property. In the proposition below, without loss of generality we show this for $n = n' \times n''$ (other cases can be covered by proper embedding of an $n$-dimensional system).

**Proposition 5.16** *For a bipartite PPT state $\rho_{ABB'} \in B(\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes n'} \otimes \mathcal{C}^{\otimes n''})$ the p-squeezed state of $\rho_{ABB'}$ is not key distillable.*

**Proof.** It is easy to see, that for $\rho_{ABB'}$, the operation of p-suqeezeing can be performed on Bob's site. This is because instead of untwisting $U_{ps}$, which is ingredient of p-squeezing[2], Bob can perform the local twisting, which has form $\sum_{i=0}^{1} |e_i\rangle\langle e_i|_B \otimes U^{(i)}_{B'}$ and subsequently trace out the $B'$ system. Now, if the state $\rho^{ps}$ was key distillable it would be entangled, i.e. would have $E_D > 0$, as all two-qubit entangled states are distillable [HHH97]. Hence, Bob could transform a PPT state which has $E_D = 0$, into state with $E_D > 0$ by local operations, which is impossible, by Theorem 2.28. ∎

For this reason, we conjecture, that if there are entangled states which are not key distillable, it can be some PPT states in $B(\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes n})$ for $n \geq 4$ [BHH$^+$08].

## 5.6 Further developement and open problems

It might by a good place to note, the abstract of [HHHO05c] is unfortunately too sound in saying that "'It is shown that one can distill arbitrarily secure key from bound entangled states"'. The sentence should be: "'It is shown that one can distill

[2]For consistency with definition of privacy squeezing (see Section 3.3.2), one should assume existence of system $A'$ with associated 1-dimensional Hilbert space, which we omit here as technical detail.

arbitrarily secure key from *certain bound entangled states*"', which we have noticed, while writing this thesis.

### Key distillability, and PPT-KD states

In [CCK$^+$07] it has been observed, that states from $\mathcal{F}_{rec}^{(m=1)}$ has negative $C_D^{DW}$ for law $d$ and $k$, so that a two-way protocol is needed. Also, other key distillable states based on those presented in this Chapter has been found there. As it was already stated, the necessary [CCK$^+$07] and necessary and sufficient condition [AH06] for key distillability has been explicitly stated. In [CCK$^+$07] it is noted, that there are PPT-KD states in $\mathcal{F}_{rec}^{(m=1)}$. Moreover, in [AH06], new PPT-KD states in $\mathcal{C}^{\otimes 6} \otimes \mathcal{C}^{\otimes 6}$ has been found.

### Multipartite PPT-KD states

The mulitpartite PPT-KD states have been found [Aug08]. The main Theorems of this thesis are shown to be true also in multipartite setting. In this setting some different (multiparite) phenomena comes into play: there are PPT-KD states which have twisted a so called *noisy W state*, (not just a *GHZ* which is a multipartite counterpart of the maximally entangled state).

### Unconditionally secure quantum key distribution and private states

So far in this thesis we have explored the LOCC scenario (see Sections 2.6, and 2.14). In this scenario Alice and Bob are promised to be given $n$ copies of a quantum state $\rho$, while Eve is given their purifying systems. This is a fundamental scenario, yet not fully realistic. In reality, Alice and Bob would like to trust only themselves, while the LOCC scenario implicitly assumes one of the two: (i) existence of a person who provides the states (ii) Alice sends 'parts' of the states to Bob via channel.

To avoid trusting the person in case (i) or assuming that the channel is not tampered with in case (ii), Alice and Bob have to *verify* if they are given good states, before they try to extract secure key. If they did not check the quality of input, Eve who can be in principle the provider, or (in case (ii)) who can operate during transmision via the channel, could manipulate them providing states from which they will never obtain a secure output.

For the sake of verification they perform certain LOCC operations, and if the input is acceptable, they proceed to transform it into state which represents secure key. If the input is not acceptable, they reject it, and close the protocol. These operations ( including verification followed by privacy extraction or rejection) establishes what is called *unconditionally secure quantum key distribution protocol*.

In [HLLO06] and [HHH$^+$07, HHH$^+$08], the following questions are studied respectively, and answered in positive:

- Are (i) private bits, ((ii) approximate private bits) verifiable via LOCC operations ?

In [RS07] the simple proof for security of the protocols based on noisy preprocessing has been found. It bases on the fact, that a coherent version of any quantum key distribution protocol, to be unconditionally secure need to produce private states (see also [RB08, RB07]).

### 5.6.1 Open problems

The most widely open problem (see also [Wer99, AH06]) is the following:

1 Are all entangled states key distillable ?

This fundamental issue weather privacy and entanglement are qualitatively equivalent, has variety of simplified sub-questions. Exemplary can be the following:

2 Are some previously known PPT entangled states key distillable ?

3 What is the maximal value of key obtained from PPT entangled states in $\mathcal{C}^{\otimes d} \otimes \mathcal{C}^{\otimes d}$. Is it reached only by the states from the boundary of PPT?

4 Characterization of the states belonging to boundary of PPT, which are key distillable.

5 Are there bound entangled key distillable states in $\mathcal{C}^{\otimes 3} \otimes \mathcal{C}^{\otimes 3}$ and $\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes 4}$ (see [AH06] and Section 5.5.4)?

6 Is there a criterion that reports entanglement of PPT-KD states presented here, which does not base on the fact that they are key distillable ?

# Chapter 6

# Distinguishing private states from attacked private states - hiding entanglement scheme

In this Chapter we discuss the subject of discriminating between two states via LOCC operations [Hor08]. We consider distinguishing $k$ copies of a private bit from $k$ copies of its attacked version, which is the pbit with key part already measured by Eve, who makes a copy of the key bits. This attack can be performed by Eve either during performance of quantum key distribution protocols, or via hacking into Alice's or Bob's site.

We consider the family of pbits presented in Section 3.4.3 (Eq (3.51)), with increasing dimension $d$ of shield. For this family, attacked versions of $\gamma_d$ are separable. We show that one needs exponentially $k = \Omega(d)$ many (as a function of occupied space $O(\log d)$) number of $\gamma_d$ to distinguish them from separable states. We refer to this phenomenon as to *hiding of entanglement*.

In Section 6.1 we consider the Eggeling-Werner bound on probability of success of discriminating between two states $\rho_0$ and $\rho_1$ via LOCC operations in case $\rho_0 = \rho^{\otimes k}$ and $\rho_1 = \sigma^{\otimes k}$, when at least one of them is in PPT. We provide a lower bound on the number $k$ of pbits needed in order to distinguish them approximately from their attacked versions, which scales proportionally to the inverse of log-negativity $E_N$ of the pbit.

## 6.1 Distinguishing between two states provided in many copies with restricted class of operations

In what follows, we assume distinguishing scenario introduced in Section 5.5.1 focusing on distinguishing by means of restricted class of operations $OP$. According to this scenario, we want to maximize the probability of success of inconclusive distinguishing between two states provided with equal proabability, which is

$$p_{s(OP)}(\rho_0,\rho_1) = \sup_{\{E_j^{(i)}\}} \frac{1}{2}(\mathrm{Tr}\sum_i E_0^{(i)}\rho_0 + \mathrm{Tr}\sum_i E_1^{(i)}\rho_1), \tag{6.1}$$

where $\{E_j^{(i)}\}$ is a POVM with elements $E_j^{(i)}$ originating from some operation from $OP$ (note, that in case $OP$ being all quantum operations the formula for probability of success $p_{s(OP)}$ is simpler, but it can not be so for e.g. LOCC operations).

We will use in this chapter three classes of operations: LOCC, PPT and quantum operations Q (see Section 2.6). The probability of success for each of them we denote as $p_{s(LOCC)}$, $p_{s(PPT)}$ and $p_{s(Q)}$ respectively. Note, that since we have $LOCC \subset PPT \subset Q$, there is :

$$p_{s(LOCC)}(\rho_0,\rho_1) \leq p_{s(PPT)}(\rho_0,\rho_1) \leq p_{s(Q)}(\rho_0,\rho_1). \tag{6.2}$$

Moreover, by Eq. (6.1) the probability of success is monotonous under allowed operations:

$$p_{s(OP)}(\rho_0,\rho_1) \geq p_{s(OP)}(\Lambda(\rho_0),\Lambda(\rho_1)). \tag{6.3}$$

for any $\Lambda \in OP$, and $OP \in \{PPT, LOCC, Q\}$.

Note also, that $p_{s(OP)}(\rho_0,\rho_1) \geq \frac{1}{2}$, since we can always decide randomly, independent of a given state. We are ready to reformulate the Eggeling-Werner bound in Helstrom like way:

**Proposition 6.1** *(adapted from [EW02]) If $\rho_0$ and $\rho_1$ are provided with equal probabilities, there is*

$$p_{s(PPT)}(\rho_0,\rho_1) \leq \frac{1}{2} + \frac{1}{4}||\rho_0^\Gamma - \rho_1^\Gamma|| \tag{6.4}$$

**Proof.** This proposition is an immediate consequence of the fact, that POVM elements which originates from LOCC operations are PPT operators (have positive partial transposition) and elementary properties of partial transposition (Eq. 2.67), trace norm and hermitian operators (see Sections A.1.1 and 2.5).∎

In what follows we will deal with the case $\rho_0 = \rho^{\otimes k}$ and $\rho_1 = \sigma^{\otimes k}$. Consequently, we denote $p_{s(OP)}(\rho^{\otimes k}, \sigma^{\otimes k})$ as $p^{(k)}_{s(OP)}(\rho,\sigma)$.

In spirit of [VW02] we make the following observation:

**Observation 6.2** *The function* $||(\rho)^\Gamma - (\sigma)^\Gamma||$ *is a metric on* $B(\mathcal{H})$*, for* $\rho, \sigma \in B(\mathcal{H})$*.*

**Proof.** It follows directly from the fact that $||\rho^\Gamma||$ is generalized matrix norm [VW02, HJ85]. ∎

Consequently, we will denote $||\rho^\Gamma - \sigma^\Gamma||$ as $||\rho - \sigma||_\Gamma$.

**Remark 6.3** *This notation is consistent with the fact that* $||\rho^\Gamma - \sigma^\Gamma|| = ||(\rho - \sigma)^\Gamma||$*, which follows from linearity of* $\Gamma$*.*

**Lemma 6.4** *For bipartite states* $\rho$ *and* $\sigma$ *from* $\mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ *there holds:*

1. *If* $\rho \in NPT$ *and* $\sigma \in PPT$*, then*

$$||\rho^{\otimes k} - \sigma^{\otimes k}||_\Gamma \leq [\frac{||\rho||_\Gamma^k - 1}{||\rho||_\Gamma - 1}]\, ||\rho - \sigma||_\Gamma \tag{6.5}$$

2. *If* $\rho, \sigma \in PPT$ *, then*

$$||\rho^{\otimes k} - \sigma^{\otimes k}||_\Gamma \leq k||\rho - \sigma||_\Gamma, \tag{6.6}$$

*where* $NPT = \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B) - PPT$*.*

**Proof.** Let us invoke elementary algebra of norms of tensor products of matrices [Bha97]. Since $A^{\otimes k} - B^{\otimes k} = \sum_{j=1}^k A^{\otimes k-j} \otimes (A - B) \otimes B^{\otimes j-1}$ for any matrices $A$ and $B$, by the triangle inequality we have:

$$||A^{\otimes k} - B^{\otimes k}|| \leq (\sum_{j=1}^{k} ||A||^{k-j}||B||^{j-1})||A - B||. \tag{6.7}$$

In general the above inequality reads

$$||A^{\otimes k} - B^{\otimes k}|| \leq kM^{k-1}||A - B||. \tag{6.8}$$

with $M = max(||A||, ||B||)$. However in special cases we can have one of the norm equal to 1. Namley, if $B = \sigma \in PPT$ (with no assumption about $A$), we have $||\sigma||_\Gamma = 1$. Providing the fact that $[\rho^{\otimes k}]^\Gamma = [\rho^\Gamma]^{\otimes k}$, we obtain the first part of this lemma. The second follows the same argument, as in this case also $||\rho||_\Gamma = 1$.∎

### 6.1.1 Distinguishing some pbits from key-part-attacked pbits

Consider a private state $\gamma = \sum_{ij=0}^{d-1} \frac{1}{d}|ii\rangle\langle jj|_{AB} \otimes U_i \rho_{A'B'} U_j^\dagger$. The state

$$\upsilon_\gamma^d := \sum_{i=0}^{d-1} \frac{1}{d}|ii\rangle\langle ii|_{AB} \otimes U_i \rho_{A'B'} U_i^\dagger, \tag{6.9}$$

is called *key-part-attacked private state*, as it is private state which has been measured on its key part. We denote it $\upsilon_\gamma$ when dimension is clear from the context. We also refer to $\upsilon_\gamma$ as to *key-part-attacked version* of $\gamma$.

We give now a lower bound on the number of $k$ copies of a private bit $\gamma^{(2)}$ from certain class, needed in order to distinguish it with high probability from that many copies of $\upsilon_\gamma^2$.

**Theorem 6.5** *Let $\gamma \in \mathcal{B}(\mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes 2} \otimes \mathcal{C}^{\otimes d_{A'}} \otimes \mathcal{C}^{\otimes d_{B'}})$ be a private bit represented in $X$-form, such that $\sqrt{XX^\dagger}$ and $\sqrt{X^\dagger X}$ are positive under partial transposition, there holds*

$$k \geq \lceil \frac{\log(4p_s^{(k)} - 1)}{\log(||X||_\Gamma + 1)} \rceil = \lceil \frac{\log(4p_s^{(k)} - 1)}{E_N(\gamma)} \rceil. \tag{6.10}$$

*with $p_s^{(k)} = p_{s(PPT)}^{(k)}(\gamma, \upsilon_\gamma^2)$, and $E_N(\gamma) = \log ||\gamma^\Gamma||$ the log-negativity, where $\upsilon_\gamma^2$*

**Remark 6.6** *Note, that log-negativity of any private bit is greater than zero. It follows immediately from the fact that $0 < E_D(\gamma) \leq E_N(\gamma)$ [HA06, VW02].*
**Proof.** Consider a private bit in $X$ form:

$$\gamma_{ABA'B'}^{(2)} = \frac{1}{2} \begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sqrt{X^\dagger X} \end{bmatrix}, \tag{6.11}$$

where $||X|| = 1$. By Lemma 3.7, there is

$$||\gamma||_\Gamma = 1 + ||X||_\Gamma. \tag{6.12}$$

Then, by (6.5)

$$||\gamma^{\otimes k} - \sigma^{\otimes k}||_\Gamma \leq [\frac{(||X||_\Gamma + 1)^k - 1}{||X||_\Gamma}]||\rho - \sigma||_\Gamma. \tag{6.13}$$

It is easy to see, that $||\gamma - \upsilon_\gamma||_\Gamma = ||X||_\Gamma$, so

$$||\gamma^{\otimes k} - \sigma^{\otimes k}||_\Gamma \leq (||X||_\Gamma + 1)^k - 1. \tag{6.14}$$

We can turn now to the probability of success $p_s^{(k)} \equiv p_s(\gamma^{\otimes k}, \upsilon_\gamma{}^{\otimes k})$ of distinguishing $k$ copies of $\gamma$ from $k$ copies of its dephased version, when provided with equal probability. Applying Proposition (6.1), and the above inequality, we obtain the following bound:

$$p_s^{(k)} \leq \frac{1}{2} + \frac{1}{4}((||X||_\Gamma + 1)^k - 1), \tag{6.15}$$

which gives after inserting (6.12)

$$k \geq \frac{\log(4p_s^{(k)} - 1)}{\log(1 + ||X||_\Gamma)} = \frac{\log(4p_s^{(k)} - 1)}{E_N(\gamma)}, \tag{6.16}$$

where $E_N(\gamma) = \log ||\gamma||_\Gamma$ stands for log-negativity, which we set out to prove. ∎

### 6.1.2 Family of private states which are exponentially hard in distinguishing from their attacked versions

Consider again the private bit of the form (3.53):

$$\gamma^V = p|\psi_+\rangle\langle\psi_+| \otimes \rho_s + (1-p)|\psi_-\rangle\langle\psi_-| \otimes \rho_a, \tag{6.17}$$

with $\rho_{a/s}$ being normalized projectors onto symmetric and antisymmetric subspaces, and the probability $p = \frac{1}{2}(1 + \frac{1}{d})$. Recall, that the log negativity of this state is $E_N(\gamma^V) = \log(1 + \frac{1}{d})$ (see Section 3.4.3).

**Observation 6.7** *For $p_s^{(k)} = p_{s(PPT)}^{(k)}(\gamma^V, \upsilon_\gamma)$ there is*

$$k \geq \lceil d \log(4p_s^{(k)} - 1) \rceil. \tag{6.18}$$

*In particular, for $p_{s(PPT)}^{(k)} = \frac{3}{4}$, there is $k \geq \frac{1}{2}d$, where $d \times d$ is the dimention of the shield of $\gamma^V$ give in Eq. (6.17).*

**Proof.** Indeed, any $k$ that allows for distinguishing with a fixed probability $p_s$ has to satisfy the bound (6.10). Now, since there is $\log(1 + x) \leq x$ for $x \geq 0$, we have that $\log(1 + \frac{1}{d}) \leq \frac{1}{d}$, so that $d \log(4p_s^{(k)} - 1) \leq \frac{\log(4p_s^{(k)} - 1)}{\log(1 + \frac{1}{d})} \leq k$ For probability of success $p_{s(PPT)}^{(k)} = 3/4$ one needs $k \geq d \log \frac{3}{2} \geq \frac{1}{2}d$. This is exponential number as a function of number of qubits that one copy of the state occupies, which is $2 \log d$. ∎

We have shown a pbit on $O(\log d)$ qubits, such that distingiushing it from its key-part-attacked version needs $\Omega(d)$ copies. We have now the following observation:

**Observation 6.8** *There holds:*

1. *$\gamma^V$ is irreducible, that is $K_D(\gamma^V) = 1$.*

*2. $\upsilon_\gamma^2$ is a separable state.*

**Proof.** It follows from definition of the private state $\gamma^V$ and $\upsilon_\gamma^2$. ∎

By these properties, the demonstrated phenomenon receives an interpretation of *hiding entanglement*. Namely, we have a state of say $k = \lfloor d/2 \rfloor$ copies of $\gamma^V$ which is clearly entangled, having $K_D((\gamma^V)^{\otimes \lfloor d/2 \rfloor}) = \lfloor d/2 \rfloor$, yet it can not be distinguished by means of LOCC operations with arbitrarily high probability of success from a separable (disentangled) state ${\upsilon_\gamma}^{\otimes k}$. More formal definition of this phenomenon will be presented in [Hor08].

**Remark 6.9** *The phrase "hiding entanglement" has been used in [HHHO05c]. However, what it meant there, was the fact that distillable entanglement rapidly decreases after twisting a state. That is, that k copies of maximally entangled 2-qubit states have $E_D = k$ and after twisting them, one gets k copies of $\gamma_V$, which has $E_D \leq \mathcal{N} \leq k \log(1 + \frac{1}{d})$. Here, we strengthen the meaning of this phrase, by showing, that twisting can decrease all kinds of entanglement, so that the probability of saying that the state is not separable (that is not a state $\upsilon_\gamma$), is exponentially small in number of qubits which it occupies.*

**Remark 6.10** *In Section 5.6, we have briefly introduced the unconditionally secure quantum key distribution. In that scheme, one considers in principle arbitrary number of qubits exchanged between (or send to both) Alice and Bob. In practice, they exchange some finite number n of qubits, and want to establish key which is $\epsilon$-secure, for some small $\epsilon > 0$ parameter of security. The minimal number of n for some fixed $\epsilon$ for which security can be obtained has been studied recently (see [SR07] and references therein, as well as review papers [GRTZ01, DLH01, SBPC+08]).*

*Exemplary origin for the lower bound for quantum communication in quantum key distribution protocol as connected with the length of the verification procedure*[1] *was provided in [CLL04a] (see also Section 5.6). Intuitively, this length (in terms of number of checked input systems) has to be large enough so that Alice and Bob were sure that the rest of systems are good for obtaining secure key. In particular, as it has been shown in [CLL04a], they have to exclude possibility of sharing separable states, which are insecure (see Section 4.6.1). Our speculation in this remark explores this fact, indicating the lower bound on the length of verification procedure when some private states are under consideration.*

**The scenario**

*We assume, that Alice and Bob share a certain number n of systems in unknown quantum state, which are expected to be in a state $\rho^{\otimes n}$ with $\rho$ belonging to some*

[1] By the *length of the verification procedure* of unconditionally secure quantum key distribution protocol we will mean the number of states that are processed in this procedure.

*acceptable set of states $A \subset B(\mathcal{C}^d \otimes \mathcal{C}^d)$ (in our case $\rho$ will be a private state). They then pass to verify if they are able to distill secure key from the state which they are given. We do not specify how they happened to share these systems, so that definition of quantum key distribution protocol that uses finite resources which we are going to provide, works for both the case when systems are distributed by Alice, and in case where they are given to Alice and Bob by some provider.*

**Necessary condition for security**

*As discussed above, from [CLL04a], it follows that to assure unconditional security of quantum key distribution protocol, Alice and Bob having performed the verification procedure, have to be sure with probability close to 1, that they do not share separable*

**Eve's attacks**

*Eve measures the Bob's subsystem of the key part of each of the private states in basis in which it is secure, either (i) while they are being distributed (eavesdropping) or (ii) while they are stored in their lab (hacking). We refer to these attacks as to key-part attacks.*

*We present now intuitive claim, whose rigorous proof we provide in [Hor08], along with rigorous definition of finite quantum key distribution protocols based on private states.*

**Claim**

*Any unconditionally secure quantum key distribution protocol, which accepts private state $\gamma^V$ residing on more than 30 qubits, requires verification procedure of length $k \geq 10^4$.*

*Let us note here, that with increasing dimension of the shield, the density of key measured in the number of key bits per the number of qubits the private state occupies, goes down. Hence, the private states with so large shield, that the above effect enters may not be welcome at all in quantum cryptographic protocols. It is however not known what is the minimal dimension of the shield, increasing significantly the length of verification procedure.*

**Note added:** The results on distinguishing of private states from separable states presented in section 6.1, has been announced on the seminar of the Institute of Physics of Polish Academy of Science in Warsaw, Poland, as well as on the $XXI$ Forum of Theoretical Informatics in Zakopane, Poland, in the time interval [April,May] of year 2007. After completing final version of these results for the purpose of this thesis, we have encountered a paper by W. Matthews and A. Winter [MW07]. There, in spirit of quantum Chernoff bound, the minimal probability of error with respect to class of operation is defined. The minimal error is calculated for the states $\rho_a$ and $\rho_s$ in asymptotic case. The result concerning this states seems to be directly related to the fact that $\gamma_d$ is written in form of a mixture of $\rho_a$ and

$\rho_s$, yet correlated to two maximally entangled states.

# Chapter 7

# Conclusions

In this thesis, we have studied the presence of secure correlations in bipartite quantum states. We based on the fact, that quantum information theory provides natural formalism for describing states of *closed systems*, called *pure states*. They are closed in a sense, that any operation which is performed outside of the system has outcome *statistically independent* from the state of the system. This fact, enabled us to characterize the states which have 'directly accessible' 'classical key'. We have shown various ways of interpretation of 'direct accessibility', and proved that all they lead to states which are up to irrelevant transformations equivalent to the so called *private states* which are of the form:

$$\gamma^{(d)}_{ABA'B'} = \sum_{ij} \frac{1}{d} |ii\rangle\langle jj| \otimes U_i \rho_{A'B'} U_j. \tag{7.1}$$

They are entangled for their privacy, but are in general *mixed* states. As we conclude in this section, the notion of private states, is central to investigations presented in this thesis. We show also, how these results receive parallel interpretations from perspective of quantum cryptography and theory of entanglement.

### 7.0.3 Insights from the private states

Treating the set of private states, as the target class in LOCC scenario, we have defined the *distillable key* $K_D$, which is an operational entanglement measure. It is defined via transformation of bipartite states into bipartite states: the input states into private states, via LOCC operations. We have considered also a natural cryptographic scenario, called LOPC scenario, in which there are *three* parties: Alice, Bob (the honest) and Eve (a dishonest one). We focused on its worst case, where the honest parties share many copies of *tripartite pure state*. The *classical distillable*

*key* in this scenario is defined via transformation of tripartite states into tripartite states: the input pure states into states representing classical key:

$$\beta_{ABE}^{(d)} = \left( \sum_{i=0}^{d-1} \frac{1}{d} |ii\rangle\langle ii| \right) \otimes \rho_E, \tag{7.2}$$

by means of LOPC operations.

The link between the LOCC and LOPC operations we provide is that whenever Alice and Bob can obtain from $\rho_{AB}$ an (approximate) ideal ccq state, they can obtain, an (approximate) private state. And vice versa: whenever, they can obtain an (approximate) private state, they can measure it on key part sharing in result an (approximate) ideal ccq state. This fact, applied to the LOCC and LOPC scenarios gave us another link between quantum security and entanglement theory, as described in a table below:

| **relevant objects** | **worst-case LOPC** | **LOCC** |
|---|---|---|
| scenario | Alice, Bob and Eve | Alice and Bob |
| input state | tripartite $\|\psi\rangle_{ABE}^{\otimes n}$ | bipartite $\rho_{AB}^{\otimes n} = \mathrm{Tr}_E \|\psi\rangle\langle\psi\|_{ABE}^{\otimes n}$ |
| allowed operations | LOPC | LOCC |
| output state | ideally secure ccq $\beta_{ABE}^{(d_n)}$ | private $\gamma_{ABA'B'}^{(d_n)}$ |
| quantity | classical distillable key $C_D(\|\psi\rangle_{ABE}) = K_D(\rho_{AB})$ distillable key | |

Table 7.1: Recasting of the worst-case LOPC scenario as LOCC scenario

In other words, the LOCC scenario, is not weaker as far as security is concerned: the Eve *is taken into account*. All the knowledge about the Eve, is already included in bipartite state of Alice and Bob. For this reason we may omit her *in notation*, while keeping her *in the calculations* of the key content, etc.

The notion of private states is central also to other results presented in this thesis. The private state consist of three basic elements: the pure maximally entangled state on the key part, the state which is in general mixed on the shield, and the operation of twisting, which correlates ('twists') the pure entangled and the mixed state. With each of the three elements we associate some phenomenas presented in this thesis.

First, because private state contains in construction the pure entanglement, and operation of twisting does not spoil its security, this state contains ideal privacy. In other words, its privacy is reminiscent of a pure entanglement that the state has been built from.

Second, because the pure entangled state present in private state is subjected to twisting, its entanglement may change. In particular, there may not exist inverse

operation to twisting within LOCC operations, and in result, the pure maximally entangled state on the key part may irreversibly loose its original pure form. This shows why some private states have $E_D < K_D$. The pure entanglement in them is twisted so much, that it can not be made pure by LOCC again.

Third, the private state can be mixed due to its shield, where whole its von Neumann entropy is located. Hence, some private states can be close in trace norm to some mixed states. In particular, we proved that there are even bound entangled states (having $E_D = 0$), with $K_D > 0$. That is the states whose entanglement can not be made pure by LOCC, and are still key distillable (BE-KD). At first, this result seems to be clear, providing there are private states with small distillable entanglement - just admix some noise, and try to get rid of it via key distillation. Such was the idea of the construction of some BE-KD states, however it has not been shown, that mere existence of private states with a gap between $K_D$ and $E_D$ implies existence of BE-KD states. The reason for existence of BE-KD states, although structurally understood to some extent, should receive deeper study. In particular it would be interesting to find BE-KD states among the states that were constructed in the past.

The above 'operational' structure of private states is not the only way, we got the insight into origin of some entanglement and security phenomena. In case of private bits we obtain it in a more algebraic way, using the $X$-form. Recall, that any pbit is uniquely represented in terms of a single operator $X$ of trace norm 1, in the so called $X$-form. The results that we list now, base merely on the fact, that $||X^\Gamma|| < ||X||$: (i) $K_D > E_D$ for some pbit, (ii) construction of some BE-KD states, (iii) the locking of (log-) negativity and (iv) the distinguishability of the pbit from its key-part attacked version can be small.

### 7.0.4 The interrelation between quantum cryptography and theory of entanglement

The following table organizes in parallel the interpretations of some of the objects and facts presented in this thesis: first from quantum cryptography point of view, second from the position of entanglement theory. Its aim is to give a flavour of the nice correspondence between the two theories.

What is a direct consequence of the results summarized in the Table 7.1, can be phrased in the following sentence:

- Privacy, is one of the manifestations of quantum correlations called entanglement.

It is now tempting to ask again the main open question which is complementary to the above outlined sentence:

| **Introduced objects and proved facts** | **Quantum cryptography perspective** | **Entanglement theory perspective** |
|---|---|---|
| **Private states** $\gamma$ | bipartite states with ideally secure key | states exhibiting (1) locking of ent. measures (EM) (2) sharp inequalities between EMs: $E_D < K_D, E_r, E_C$ |
| **Some private states are hardily distinguishable from separable states** | some private states are hardily distinguishable from insecure states | some entangled states are hardily distinguishable from disentangled states |
| **Distillable key** $K_D$ | quantifies security content of bipartite states | another operational EM |
| $K_D \leq E_r^{\infty}$ | upper bound on $K_D$ | another inequality for ordering some EMs, via entering the sequence: $E_D \leq K_D \leq E_r^{\infty} \leq E_C$. |
| $K_D(\rho) = C_D(\|\psi_\rho\rangle)$ | security content of a bipartite state is an EM. | one of natural EMs (extension of $E_D$ to private states) quantifies security content |
| **Examples of bound entangled key distillable states** | security without pure entangled states is possible | The states whose bound ent. is understood, as 'too much twisted and noisy' to be distilled |

Table 7.2: Interplay between quantum cryptography (QC) and entanglement theory (ET). The objects and facts are interpreted subsequently from QC and ET perspective. We use 'ent.' as the acronym for entanglement.

- Does privacy always assist entanglement ? More formally: are all bipartite entangled states key distillable ?

As we have invoked, the above results has been partially developed in recent years (see for example [CEH$^+$07, Aug08, RS07, Chr06, CCK$^+$07, HHH$^+$07]). It seems, that the people working on both the entanglement theory and quantum cryptography may experience analogous feelings to those experienced by C. Shannon as expressed in the phrase quoted in the first motto of this thesis. To paraphrase his words,

"entanglement theory and quantum cryptography do not come one before another: they are so close together, one can not separate them".

# Chapter 8

# Notation

**Notation introduced in Chapter 2.**

- $\mathcal{C}^d$ - d-fold cartesian product of the field of Complex numbers - an example of a Hilbert space.
- $\mathcal{H}_X$ symbol for a Hilbert space associated with a system $X$. Usually, $X \in \{A, B, A', B', E\}$.
- $\dim\mathcal{H}$ - the dimension of a Hilbert space $\mathcal{H}$.
- $B(\mathcal{H})$ - the set of density matrices (positive and of trace one), that act on a Hilbert space $\mathcal{H}$.
- $|.\rangle$ - vector in a Hilbert space with label ".".
- $\langle .|$ - the transposed, and complex-conjugated vector $|.\rangle$.
- $|.\rangle\langle .|$ - "outer product" of $|.\rangle$ and $\langle .|$, or the projector onto the subspace spanned by $|.\rangle$.
- $P_{|\psi\rangle}$ a projector onto vector $|\psi\rangle$
- $\{(q_i, \rho_i)\}$ or $\{(q_i, \rho_i)\}_{i=1}^K$ - the ensamble of states $\rho_i$ with corresponding probabilities $q_i$.
- $\Lambda$ - a quantum operation.
- $\{M_m\}$ - a quantum operation with Kraus operators $M_m$.
- $\{E_m\}$ - a POVM with elements $E_m$.

- $M_\Lambda$ - a POVM associated with an operation $\Lambda$.
- $\{|k\rangle\}$ - the standard basis in some Hilbert space $\mathcal{H}$, which is understood to be known from the context. The index $k$ ranges from 0 to $\dim\mathcal{H} - 1$.
- $U$ - generic symbol for unitary operation.
- $V$ - the swap unitary transformation.
- H - Hadamard unitary transformation
- $\rho$ - generic symbol for a density matrix.
- $\rho_{AB}$ - a density matrix of the the state of a bipartite system (a bipartite state) with two subsystems $A$ and $B$.
- $\otimes$ - the operation of tensor product.
- $\mathcal{H}_{XY}$ symbol for a tensor product of Hilbert spaces $\mathcal{H}_X$ and $\mathcal{H}_Y$.
- $\oplus$ - the operation of direct sum.
- Tr(.) - the trace.
- $\mathrm{Tr}_X(.)$ - the partial trace over system $X$.
- $(.)^\dagger$- composition of element wise complex conjugation and matrix transposition of matrix labeled "."
- $(.)^T$ - transposition of a matrix labeled by "." If it is not explicitly stated, it is assumed that transposition is taken in standard basis $\{|k\rangle\}$.
- $(.)^*$ - complex conjugation of a matrix labeled by "."
- $\bar{a}$ - complex conjugation of the number a.
- $|\psi\rangle$ - a generic symbol for a pure state (vector).
- $|\psi\rangle_{AB}$ - the pure state of a bipartite system (a bipartite pure state) with two subsystems $A$ and $B$.
- $|\psi_\rho\rangle$ - the purification of the state $\rho$.
- $|\psi_\rho\rangle_{ABA'B'E}$ - the purification of the state $\rho$, on systems $ABA'B'E$.
- I - the identity matrix.

- $|\Psi_+^{(d)}\rangle$ - the maximally entangled state of the form $\sum_{i=0}^{d-1} \frac{1}{\sqrt{d}}|i\rangle \otimes |i\rangle$.
- $MS^{(d)}$ - the set of maximally entangled states in two qudits.
- $\{|\psi^-\rangle, |\psi^+\rangle, |\phi^-\rangle, |\phi^+\rangle\}$ - a Bell basis in $\mathcal{C}^2 \otimes \mathcal{C}^2$.
- $|\psi^-\rangle$ - the singlet state (a two qubit maximally entangled state of the form $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$).
- $\sigma_i$ with $i \in \{0, 1, 2, 3\}$ - the Pauli operators. They form a group of one-qubit unitary matrices.
- $\Gamma$ - operation of partial transposition.
- PPT - the set of so called "PPT operations", or the set of states with positive partial transposition.
- $LOCC_{\mathcal{H}_1,\mathcal{H}_2}$ - the set of Local Operations and Classical Communication that transform the states from $B(\mathcal{H}_1)$ into states from $B(\mathcal{H}_2)$.
- $LOCC$ - generic symbol for the set of LOCC operations (without explicitly marked input and output Hilbert space).
- $SEP_{\mathcal{H}_1,\mathcal{H}_2}$ - the set of separable operations transforming states from $B(\mathcal{H}_1)$ into states from $B(\mathcal{H}_2)$.
- $SEP$ - either the generic symbol for a set of separable operations (without explicitly marked input and output Hilbert space) or the set of separable states.
- $\Lambda_A$ - local quantum operation on Alice's site.
- $\Lambda_B$ - local quantum operation on Bob's site.
- $\Lambda_A^{(c)}$ - operation of classical communication from Alice to Bob.
- $\Lambda_B^{(c)}$ - operation of classical communication from Bob to Alice.
- $\Lambda^{sep}$ - a separable operation.
- $D(\rho, \sigma)$ - quantum distance measure between $\rho$ and $\sigma$.
- $||.||$ - the trace norm.
- $F(\rho, \sigma)$ - quantum fidelity of $\rho$ and $\sigma$.
- log - a binary logarithm function.

- $H(X)$ - classical (Shannon) entropy of a random variable $X$.
- $I(A:B)$ - classical mutual information of a joint distribution of random variables $A$ and $B$.
- $S(P||Q)$ - the classical relative entropy of variables $Q$ and $P$.
- $S(\rho)$ - quantum von Neumann entropy of a state $\rho$.
- $\eta(x)$ a function defined on $(0,1]$ as $\eta(x) = -x \log x$.
- $S(A)_\rho$ - the entropy of subsystem $A$ of the compound system in state $\rho$.
- $I(A:B)_\rho$ - the quantum mutual information of the subsystem $AB$ of the system in state $\rho$.
- $S(\rho||\sigma)$ - the quantum relative entropy of $\rho$ and $\sigma$.
- $\chi(\{(q_i, \rho_i)\})$ - the Holevo quantity of an ensamble $\{(q_i, \rho_i)\}$ defined as $S(\sum_i q_i \rho_i) - \sum_i q_i S(\rho_i)$.
- $H(\vec{p})$ - the Shannon entropy of a distribution $\vec{p} = (p_1, \ldots, p_K)$ for some natural number $K$.
- $R_{\geq 0}$ - the set of nonnegative real numbers.
- $E(\rho)$ - a generic symbol for an entanglement measure $E$.
- $E^\infty$ - regularization of an entanglement measure $E$.
- $E_D$ - distillable entanglement.
- $E_r$ - the relative entropy of entanglement.
- $E_f$ - the entanglement of formation.
- $E_C$ - entanglement cost.
- $\mathcal{N}$ - the negativity.
- $E_N$ - the logarithmic negativity.
- $Q(\Lambda)$ - quantum channel capacity.
- $\rho_\Lambda$ - the state $\rho$ related to an operation $\Lambda$ via the Choi-Jamiołkowski isomorphism.

**notation introduced in Chapter 3.**

- $\rho_{ccq}^{ideal}$ - the ideal ccq state i.e. the state representing an ideal secure key.
- a cqq state - a state of the form $\sum_i |i\rangle\langle i|_A \otimes \rho_{BE}^{(i)}$
- $[\rho_{ABA'B'}]^{ccq}$ - a ccq state of a bipartite state $\rho$, obtained via tracing out system $A'B'$ of any purification $|\psi_\rho\rangle_{ABA'B'E}$.
- $\gamma^{(d)}$ - a private state with d-dimensional key part.
- $\gamma^{(d,d')}$ a private state with d-dimensional key part and $d'$-dimensional shield.
- Re(.) - the real part of an imaginary number labeled as "."
- $P_{sym} = \frac{1}{2}(\mathrm{I} + V)$ and $P_{asym} = \frac{1}{2}(\mathrm{I} - V)$ - the projectors onto symmetric and antisymmetric subspaces respectively where $V$ is the swap unitary transformation.
- $\rho_s$ and $\rho_a$ - the symmetric and antisymmetric Werner states, that is normalized projectors $P_{sym}$ and $P_{asym}$.
- $\rho_{flower}^{(d)}$ - a member of the family of flower states with d-dimensional key part (recall that it is a private state).
- $PS^{(d,d')}$ - the set of private states with $4 \geq k \leq d \times d$-dimensional key part and $l \leq d' \times d'$ dimensional shield.
- $PS$ the set of all private states (with arbitrary dimensional key part and shield).
- $\{|i\rangle|j\rangle\}_{i,j=1}^{K}$ - a standard product basis (a basis of product of the Hilbert spaces), both of dimension $K$.
- $X_\pm$ - the positive (negative) part of the hermitian operator $X$.
- $K_D(\rho_{AB})$ - the entanglement measure called distillable key of $\rho_{AB}$.
- $I_c$ - the function of classical correaltions of a bipartite quantum state.
- $\rho_{aAB}^{cl}$ - a state which exhibits locking of $I_c$.
- Non Lock - a property of entanglement measures, called non-lockability
- E is $(\kappa \downarrow \Delta) -$ Tr-lockable - a property of entanglement measure. Informally speaking, reports that $E$ decreases by $\Delta$ after operation on system of dimension $2^\kappa$.

- The family $\{\rho^c_{aAB}\}$ reveals $(\kappa \downarrow \Delta) -$ Tr-lockability of $E$- when $\Delta$ is explicit function of parameter $c$, reprots that $E$ is $(\kappa \downarrow \Delta(c)) -$ Tr-lockable.
- $\sigma_{abs}$ - an absolutely separable state.

**notation introduced in Chapter 4.**

- $C_D(\rho_{ABE})$ - distillable classical key of a tripartite state $\rho_{ABE}$
- $C_D(\rho_{AB})$ - distillable classical key of tripartite pure state $|\psi_\rho\rangle_{ABE}$ which is a purification of $\rho_{AB}$ to system $E$. where $\psi_\rho^{ABE}$ is a purification of $\rho_{AB}$.
- $LOPC$ - the set of Local Operations and Public Communication
- $CLOPC$ operation - the coherent LOPC operation
- $\Lambda^{coh}$ - a coherent (version of) operation $\Lambda$
- $\Lambda_Q$ - an LOPC operation
- $P_n^{\delta,\epsilon}$ - an LOPC operation acting on $n$ copies of input state $\rho$, that outputs a state which is $\epsilon$ close in trace norm to some ideal *ccq*-state, that belongs to a distillation protocol with a rate greater than $C_D(\rho) - \delta$.
- $Q_n^{\delta,\epsilon}$ - similarly as $P_n^{\delta,\epsilon}$ but for LOCC operation.
- $S^\tau$ - the set of separable states to which a fixed twisting $U$ was applied.
- $E_r^S$ - the relative entropy entanglement with a compact, convex set $S$ in place of that of separable states in definition of relative entropy of entanglement $E_r$.
- $C_D^{DW}$ the key rate of the protocol of Devetak and Winter.
- $SEP^{(d,d')}$ - The set of states on systems $ABA'B'$, separable in $AA' : BB'$ cut where $\dim A = \dim B = d$ and $\dim A' = \dim B' = d'$
- $\rho^{ps}$ - a p-squeezed state of state $\rho$

**notation introduced in Chapter 5.**

- $\tau_1 = (\frac{\rho_s+\rho_a}{2})^{\otimes k}$ and $\tau_2 = (\rho_s)^{\otimes k}$ - the Eggeling-Werner hiding states, with $\rho_a$ and $\rho_s$ the antisymmetric and symmteric Werner states.
- $\rho^{de}_{(d,k)} = \frac{1}{2}|\phi_+\rangle\langle\phi_+|_{AB} \otimes \tau_1^{A'B'} + \frac{1}{2}|\phi_-\rangle\langle\phi_-|_{AB} \otimes \tau_2^{A'B'}$
- $\rho_{(d,k,p)} = p\rho^{de}_{(d,k)} + (1-2p)\frac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \tau_2$

- $\mathcal{F}_{rec}^{(m=1)}$ - the set of states $\{\rho_{(p,k,d)}^{rec(1)}\}$ parametrized by triples $(p,k,d)$ with $p \in (0, \frac{1}{2}]$, $k \geq 1$ natural, $d \geq 2$ natural.

- $\mathcal{F}_s$ - the family of states that are mixture of two private states one represented in $X$-form by $X_1 = \frac{1}{||W_U||} \sum_{ij} u_{ij}|ii\rangle\langle jj|$ with $u_{ij}$ the elements of some unitary $U$, and $X_2 = \frac{1}{||W_U^\Gamma||} W_U^\Gamma$ with probability $p = \frac{||W_U||}{||W_U|| + ||W_U^\Gamma||}$ and $1-p$ respectively.

**notation introduced in Chapter 6.**

- $Q$ - the class of quantum operations.

- $p_s(\rho_0, \rho_1)$ - the probability of inconclusive distinguishing between states $\rho_0$ and $\rho_1$, supplied with equal probabilities by means of quantum operations.

- $p_{s(OP)}(\rho_0, \rho_1)$ with $OP \in \{Q, LOCC, PPT\}$ the probability of inconclusive distinguishing between states $\rho_0$ and $\rho_1$, supplied with equal probabilities by means of operations from class $OP$.

- $p_{s(OP)}^{(k)}(\rho, \sigma)$ with $OP \in \{Q, LOCC, PPT\}$ - shorthand notation for $p_{s(LOCC)}(\rho^{\otimes k}, \sigma^{\otimes k})$.

- $||A||_\Gamma$ - shorthand for $||(A)^\Gamma||$ with $\Gamma$ the partial transposition.

- $\upsilon_\gamma^d$ - a private state $\gamma$ after complete von Neumann measurement on its key part (also called key-part-attacked private state, or attacked version of $\gamma$).

# Appendix A

# Useful facts

In this Chapter we provide some facts from linear algebra, which are mostly independent of the formalism of quantum information theory. In particular we recall a definition of the operation of tensor product of Hilbert spaces. Most of these facts are collected in [NC00].

## A.1 Implementing partial isometry via quantum operations

To see, that an isometry can be implemented via quantum operations, we first show that one can perform the embadding and partial projection operations, that can be called together an *exchanging operation*.

**Lemma A.1** *(exchanging operation) Any state $\rho \in B(\mathcal{H}_1)$ can be transformed into $\rho \in B(\mathcal{H}_2)$, by means of quantum operations, providing* $\dim\mathcal{H}_2 \geq Rank(\rho)$. *The operation which does this task, we call exchanging operation.*
**Proof.** To see this, consider first adding an ancillary system in state $|0\rangle \in \mathcal{H}_2$ composed with the izometry:

$$\forall_{|i\rangle\in\mathcal{H}_1}\ V(|i\rangle_1 \otimes |0\rangle_2) := (|0\rangle_1 \otimes |i\rangle_2). \tag{A.1}$$

It is easy to see, that there exists an extension of this izometry to the unitary transformation $V' : \mathcal{H}_1 \otimes \mathcal{H}_2 \to \mathcal{H}_1 \otimes \mathcal{H}_2$ (see Exercise 2.6 of [NC00]). Hence, adding $|0\rangle \in \mathcal{H}_2$, performing $V'$ and tracing out system $\mathcal{H}_1$ transforms the state $|i\rangle$ from $\mathcal{H}_1$ to $\mathcal{H}_2$, and the assertion follows. By linearity of this operation, we have the assertion for $\rho$ under assumptions about the dimension of $\mathcal{H}_2$. ∎

We can make now desired corollary:

**Corollary A.2** *(partial isometry via basic quantum operations) Consider two systems $E$ with $\dim E' \geq \dim E$. Any isometry $W : \mathcal{H}_E \to \mathcal{H}_{E'}$ and partial isometry $W' : \mathcal{H}_{E'} \to \mathcal{H}_E$ can be performed by means of quantum operations.*

**Proof.** To see the two facts from this corollary, we will use the operations of embadding and partial projection. We first give the idea how to use them, and then argue, that they can be implemented by quantum operations.

To implement $W$ via quantum operations we consider two cases: (1) $\dim E' = \dim E$ (2) $\dim E' > \dim E$ In first case, $W$ is just a unitary transformation, which is a quantum operation. In case (2), a quantum operation implementing $W$ is a composition of (i) embadding of the Hilbert space $\mathcal{H}_E$ into $\mathcal{H}_{E'}$ (ii) applying unitary transformation which is an extension of $W : \mathcal{H}_E \subset \mathcal{H}_{E'} \to \mathcal{H}_{E'}$ (see Exercise 2.6 of [NC00]).

To implement $W'$ via quantum operations one composes similar operations, in inversed order: (i) the unitary $U$ operation which extends $W'$ to space $\mathcal{H}_{E'}$ ($U$ constructed similarly as for the proof of Exercise 2.6 of [NC00]). (ii) a partial projection, acting from $E'$ to $E$.

Both embadding and partial projection can be made by the *exhanging operation* described in Lemma A.1. ∎

### A.1.1 Some properties of the trace norm

The trace norm $||A|| = Tr|\sqrt{A^\dagger A}|$, fulfills:

$$||A|| = \sup_U TrUA, \tag{A.2}$$

where supremum is taken over unitary transformations $U$ and

$$||A|| = \sup_{0 \leq P \leq \mathrm{I}} TrPA, \tag{A.3}$$

where $P$ is a projector laying between 0 and the identity matrix, in operator order.

The trace norm is unitarily invariant [HJ85], that is, for any unitary transformations $U$ and $W$ from $B(\mathcal{H})$, and any operator $A \in B(\mathcal{H})$, there holds:

$$||UAW|| = ||A||. \tag{A.4}$$

### A.1.2 Polar and Singular Value matrix decomposition

Any matrix $A$ can be decomposed into the so called *polar decomposition* of the form

$$A = U\rho = \sigma U, \tag{A.5}$$

where $\rho = \sqrt{A^\dagger A}$ and $\sigma = \sqrt{AA^\dagger}$ are unique positive operators, and U is a unitary matrix.

Any matrix $A$ can be decomposed into the so called *singular value decomposition* which has the form

$$A = U\Sigma W, \tag{A.6}$$

with $\Sigma$ diagonal, positive operator and $U$ and $W$ unitary. The eigenvalues of $\Sigma$ are called the *singular values* of an operator $A$.

### A.1.3 Sufficient condition for positivity of a block matrix

**Lemma A.3** *If $A$ and $B$ are hermitian and $A \geq |B|$, the block matrix*

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}, \tag{A.7}$$

*is positive.*

**Proof.** The matrix (A.7) is positive if it is diagonalizable, and has non-negative eigenvalues. It can be diagonalized by transforming first with unitary operation $H \otimes \mathrm{I}$ into a block diagonal form

$$\begin{bmatrix} A+B & \\ & A-B \end{bmatrix}. \tag{A.8}$$

and then diagonalizing the blocks $A + B$ and $A - B$. Hence, the matrix (A.7) is positive if these blocks are so. Since for hermitian $B$, $|B| \geq B$ and $|B| \geq -B$, from assumption we have $A \geq |B|$, which implies $A \geq B$ and $A \geq -B$. ∎

# Bibliography


[AB02] H. Aschauer and H. J. Briegel. Private entanglement over arbitrary distances, even using noisy apparatus. *Phys. Rev. Lett.*, 88:047902, 2002.

[ABH+01] G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. F. Werner, and A. Zeilinger. *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*. Springer, 2001.

[AC93] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography. *IEEE Trans. Inf. Theory*, 39:1121–1132, 1993.

[ACM04] A. Acín, J. I. Cirac, and Ll. Masanes. Multipartite bound information exists and can be activated. *Phys. Rev. Lett.*, 92:107903, 2004, quant-ph/0311064.

[AEJ+01] K. Audenaert, J. Eisert, E. Jané, M. B. Plenio, S. Virmani, and B. De Moor. Asymptotic relative entropy of entanglement. *Phys. Rev. Lett.*, 87:217902, 2001, quant-ph/0103096.

[AH06] R. Augusiak and P. Horodecki. On quantum cryptography with bipartite bound entangled states. In *Quantum Information Processing: From Theory to Experiment*, volume 199, pages 19–29. D.G. Angelakis et al. (eds.), NATO Science Series III,IOS Press, Amsterdam, 2006, 2006, arXiv:0712.3999.

[AMG03] A.io Acín, L. Masanes, and N. Gisin. Equivalence between two-qubit entanglement and secure key distribution. *Phys. Rev. Lett.*, 91:167901, 2003, quant-ph/0303053.

[Aug08] R. Augusiak, 2008. private communication.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, India, December 1984, 1984. IEEE Computer Society Press, New York.

[BBB+98] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. Security of quantum key distribution against all collective attacks. 1998, arXiv:quant-ph/9801022.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[BBM92] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[BBP+96] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–725, 1996, quant-ph/9511027.

[BDF+99] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A*, 59:1070–1091, 1999, quant-ph/9804053.

[BDM+99] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases and bound entanglement. *Phys. Rev. Lett.*, 82:5385–5388, 1999, quant-ph/9808030.

[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, 1996, quant-ph/9604024.

[BH98] V. Buzek and M. Hillery. Universal optimal cloning of arbitrary quantum states: From qubits to quantum registers. *Phys. Rev. Lett.*, 81:5003–5006, 1998, arXiv:quant-ph/9801009.

[Bha97] R. Bhatia. *Matrix analysis*, volume 169 of *Graduate Texts in Mathematics*. Springer, New York, 1997.

[BHH+08] P. Badziag, P. Horodecki, K. Horodecki, M. Nowakowski, and Ł. Pankowski, 2008. in preparation.

[BL07] D. Bruß and G. Leuchs. *Lectures on Quantum information*. Wiley-Vch GmbH & Co. KGaA, 2007.

[BM97] E. Biham and T. Mor. On the security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 78:2256–2259, 1997, arXiv:quant-ph/9605007.

[BOHL+05a] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *TCC*, pages 386–406, 2005, quant-ph/0409078.

[BOHL+05b] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *TCC*, pages 386–406, 2005, quant-ph/0409078.

[BP00] D. Bruß and A. Peres. Construction of quantum states with bound entanglement. *Phys. Rev. A*, 61:030301, 2000, quant-ph/9911056.

[BR03] P. Oscar Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67:042317, 2003, quant-ph/0003059.

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[BZ06] I. Bengtsson and K. Życzkowski. *Geometry of Quantum States. An Introduction to Quantum Entanglement*. Cambridge University Press, 2006.

[CCK+07] D. Pyo Chi, J. Woon Choi, J. San Kim, T. Kim, and Soojoon Lee. Bound entangled states with nonzero distillable key rate. 2007, arXiv:quant-ph/0612225.

[CEH+07] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner. Unifying classical and quantum key distillation. In *Proceedings of the 4th Theory of Cryptography Conference*, volume 4392, pages 456–478. Lecture Notes in Computer Science, 2007, quant-ph/0608199.

[CGLL05] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus. Detecting two-party quantum correlations in quantum-key-distribution protocols. *Phys. Rev. A*, 71:022306, 2005, quant-ph/0409047.

[Chr02] M. Christandl. The quantum analog to intrinsic information. *Diploma Thesis, Institute for Theoretical Computer Science,ETH Zurich*, 2002.

[Chr06] M. Christandl. *The Structure of Bipartite Quantum States - Insights from Group Theory and Cryptography.* PhD thesis, University of Cambridge, 2006.

[CK78] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE*, 24:339–348, 1978.

[Cla06] L. Clarisse. *Entanglement Distillation; A Discourse on Bound Entanglement in Quantum Information Theory.* PhD thesis, University of York, 2006, quant-ph/0612072.

[CLL04a] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004, quant-ph/0307151.

[CLL04b] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004, quant-ph/0307151.

[CMS02] N. J. Cerf, Serge Massar, and S. Schneider. Multipartite classical and quantum secrecy monotones. *Phys. Rev. A*, 66:042309, 2002, quant-ph/0202103.

[CP02] D. Collins and S. Popescu. Classical analog of entanglement. *Phys. Rev. A*, 65:032321, 2002, quant-ph/0107082.

[CT91] T. M. Cover and Joy A. T. *Elements of information theory.* Wiley, 1991.

[CW04] M. Christandl and A. Winter. "squashed entanglement": An additive entanglement measure. *J. Math. Phys.*, 45:829–840, 2004, quant-ph/0308088.

[CW05] M. Christandl and A. Winter. Uncertainty, monogamy, and locking of quantum correlations. *IEEE Trans. Inf. Theory*, 51:3159, 2005, quant-ph/0501090.

[DEJ+96] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818–2821, 1996, quant-ph/9604039.

[DHL+04] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal. Locking classical correlations in quantum states. *Phys. Rev. Lett.*, 92:067902, 2004, quant-ph/0303088.

[DHR02] M. J. Donald, M. Horodecki, and O. Rudolph. The uniqueness theorem for entanglement measures. *J. Math. Phys.*, 43:4252–4272, 2002, quant-ph/0105017.

[DLH01] M. Dusek, N. Lutkenhaus, and M. Hendrych. Quantum cryptography. *Progress in Optics*, 49:381–454, 2001, arXiv:quant-ph/0601207.

[DLT02] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. *IEEE Trans. Inf. Theory*, 48:580–599, 2002, quant-ph/0103098.

[DW04] I. Devetak and A. Winter. Relating quantum privacy and quantum coherence: an operational approach. *Phys. Rev. Lett.*, 93:080501, 2004, quant-ph/0307053.

[DW05] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A*, 461:207–235, 2005, quant-ph/0306078.

[EFP+00] J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio, and M. Wilkens. Classical information and distillable entanglement. *Phys. Rev. Lett.*, 84:1611–1614, 2000, quant-ph/9907021.

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[EW02] T. Eggeling and R. F. Werner. Hiding classical data in multi-partite quantum states. *Phys. Rev. Lett.*, 76:097905, 2002, quant-ph/0203004.

[Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Comm. Math. Phys.*, 31:291, 1973.

[Fv97] C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum mechanical states. 1997, quant-ph/9712042.

[GH08] A. Grudka and M. Horodecki, 2008. Private communication.

[Gou07] G. Gour. How many ebits can be unlocked with one classical bit? *Phys. Rev. A*, 75:054301, 2007, arXiv:quant-ph/0703246.

[GRTZ01] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. 2001, arXiv:quant-ph/0101098.

[GW99] N. Gisin and S. Wolf. Quantum cryptography on noisy channels: quantum versus classical key-agreement protocols. *Phys. Rev. Lett.*, 83:4200–4203, 1999, quant-ph/9902048.

[GW00] N. Gisin and S. Wolf. Linking classical and quantum key agreement: is there "bound information"? 2000, quant-ph/0005042.

[HA06] P. Horodecki and R. Augusiak. Quantum states representing perfectly secure bits are always distillable. *Phys. Rev. A*, 74:010302, 2006, quant-ph/0602176.

[HH06] M. Horodecki and P. Horodecki. private communication. 2006.

[HHH97] M. Horodecki, P. Horodecki, and R. Horodecki. Inseparable two spin-$\frac{1}{2}$ density matrices can be distilled to a singlet form. *Phys. Rev. Lett.*, 78:574–577, 1997.

[HHH98] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, 80:5239–5242, 1998, quant-ph/9801069.

[HHH99] M. Horodecki, P. Horodecki, and R. Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60:1888–1898, 1999, quant-ph/9807091.

[HHH00] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. *Phys. Rev. Lett.*, 84:2014–2017, 2000, quant-ph/9908065.

[HHH01] R. Horodecki, M. Horodecki, and P. Horodecki. Balance of information in bipartite quantum-communication systems: Entanglement-energy analogy. *Phys. Rev. A*, 63:022310, 2001, quant-ph/0002021.

[HHH$^+$05] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, Aditi Sen(De), Ujjwal Sen, and B. Synak-Radtke. Local versus nonlocal information in quantum-information theory: Formalism and phenomena. *Phys. Rev. A*, 71:062307, 2005, quant-ph/0410090.

[HHH+07] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity. 2007, quant-ph/0608195.

[HHH+08] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. Unconditional privacy over channels which cannot convey quantum information. *Phys. Rev. Lett.*, 100:110502, 2008, quant-ph/0702077.

[HHHH07] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. 2007, quant-ph/07022205v2.

[HHHO05a] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. 2005, quant-ph/0506189.

[HHHO05b] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Locking entanglement with a single qubit. *Phys. Rev. Lett.*, 94:200501, 2005, quant-ph/0404096.

[HHHO05c] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94:160502, 2005, quant-ph/0309110.

[HHT01] P. M. Hayden, M. Horodecki, and B. M. Terhal. The asymptotic entanglement cost of preparing a quantum state. *J. Phys. A: Math. Gen*, 34:6891–6898, 2001, quant-ph/0008134.

[Hil05] R. Hildebrand. Ppt from spectra. 2005, quant-ph/0502170.

[HJ85] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, Cambridge, 1985.

[HLLO06] K. Horodecki, D. Leung, Hoi-Kwong Lo, and J. Oppenheim. Quantum key distribution based on arbitrarily weak distillable entangled states. *Phys. Rev. Lett.*, 96:070501, 2006, quant-ph/0510067.

[HMM+06] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani. Bounds on multipartite entangled orthogonal state discrimination using local operations and classical communication. *Phys. Rev. Lett.*, 96:040501, 2006, arXiv:quant-ph/0506170.

[Hor97] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232:333, 1997, quant-ph/9703004.

[Hor01] M. Horodecki. Entanglement measures. *Quantum Inf. Comp.*, 1:3–26, 2001.

[Hor03] R. Horodecki. *Sum ergo cogito.* Marpress, Gdańsk, 2003.

[Hor08] K. Horodecki. On hiding entanglement using private states, 2008. unpublished.

[HPHH05] K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki. Low dimensional bound entanglement with one-way distillable cryptographic key. 2005, quant-ph/0506203.

[HV00] L. Henderson and V. Vedral. Information, relative entropy of entanglement and irreversibility. *Phys. Rev. Lett.*, 84:2263–2266, 2000, quant-ph/9909011.

[Joz94] R. Jozsa. *J. Mod. Opt.*, 41:2315, 1994.

[Kah96] D. Kahn. *The Code-breakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Scribner, 1230 Avenue of the Americans, New York, NY 10020, 1996.

[Koa07] M. Koashi. Complementarity, distillable secret key, and distillable entanglement. 2007, arXiv:0704.3661.

[KRBM05] R. Koenig, R. Renner, A. Bariska, and U. Maurer. Locking of accessible information and implications for the security of quantum cryptography. 2005, quant-ph/0512021.

[KW04] M. Koashi and A. Winter. Monogamy of quantum entanglement and other correlations. *Phys. Rev. A*, 69:022309, 2004, quant-ph/0310037.

[KZ01] M. Kuś and K. Życzkowski. Geometry of entangled states. *Phys. Rev. A*, 63:032307, 2001.

[LC99] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999, quant-ph/9803006.

[Lin75] G. Lindblad. Completely positive maps and entropy inequalities. *Comm. Math. Phys.*, 40:147–151, 1975.

[LPSW99] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland. Reversibility of local transformations of multiparticle entanglement. 1999, quant-ph/9912039.

[Mas05] Ll. Masanes. Useful entanglement can be extracted from all nonseparable states. 2005, quant-ph/0510188.

[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE*, 39:773–742, 1993.

[MCL06] T. Moroder, M. Curty, and N. Lütkenhaus. Upper bound on the secret key rate distillable from effective quantum correlations with imperfect detectors. *Phys. Rev. A*, 73:012311, 2006, quant-ph/0507235.

[Mor05] H. Moriya. Validity and failure of some entropy inequalities for car systems. *J. Math. Phys.*, 46:033508, 2005.

[MTd00] M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels and the cost of randomizing quantum information. 2000, quant-ph/0003101.

[MW07] W. Matthews and A. Winter. On the chernoff distance for asymptotic locc discrimination of bipartite quantum states. 2007, arXiv:0710.4113.

[MY04] K. Matsumoto and F. Yura. Entanglement cost of antisymmetric states and additivity of capacity of some quantum channels. *J. Phys. A: Math. Gen.*, 37:L167–L171, 2004, quant-ph/0306009.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press,Cambridge, 2000.

[OP93] M. Ohya and Denes Petz. *Quantum entropy and its use*. Springer-Verlag, Heidelberg, 1993.

[Pan05] 2005. Ł. Pankowski, private communication.

[Per96] A. Peres. Collective tests for quantum nonlocality. *Phys. Rev. A*, 54:2685–2689, 1996.

[PHHH08] Ł. Pankowski, K. Horodecki, M. Horodecki, and P. Horodecki. On the private states, 2008. In preparation.

[PPHH07] Ł. Pankowski, M. Piani, M. Horodecki, and P. Horodecki. Few steps more towards npt bound entanglement. 2007, arXiv:0711.2613.

[PV06] M. B. Plenio and S. Virmani. An introduction to entanglement measures. *Quantum Inf. Comp.*, 7:1, 2006, quant-ph/0504163.

[Rai97] E. M. Rains. Entanglement purification via separable superoperators. 1997, quant-ph/9707002.

[Rai98] E. M. Rains. A rigorous treatment of distillable entanglement. 1998, quant-ph/9809078.

[Rai99] E. M. Rains. Bound on distillable entanglement. *Phys. Rev. A*, 60:179–184, 1999, quant-ph/9809082.

[Rai00] E. M. Rains. Erratum: Bound on distillable entanglement [phys. rev. a, **60**, 179 (1999)]. *Phys. Rev. A*, 63:019902, 2000.

[RB07] J. M. Renes and J-C. Boileau. Privacy amplification, private states, and the uncertainty principle. 2007, arXiv:quant-ph/0702187.

[RB08] J. M. Renes and J-C. Boileau. Physical underpinnings of privacy. 2008, arXiv:0803.3096.

[Ren05] R. Renner. *Sequrity of Quantum Key Distribution.* PhD thesis, ETH, Zurich, 2005.

[RGK05] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, 2005, quant-ph/0502064.

[RS07] J. M. Renes and G. Smith. Noisy processing and distillation of private quantum states. *Phys. Rev. Lett.*, 98:020502, 2007, quant-ph/0603262.

[SBPC$^+$08] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev. A framework for practical quantum cryptography. 2008, arXiv:0802.4155.

[Sch35] E. Schrödinger. Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, 23:807–812, 1935.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech.*, 28:656, 1949.

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, 2000, quant-ph/0003004.

[SR07] V. Scarani and R. Renner. Quantum cryptography with finite resources. 2007, arXiv:0708.0709.

[SRH06] B. Synak-Radtke and M. Horodecki. On asymptotic continuity of functions of quantum states. *J. Phys. A: Math. Gen.*, 39:L423–L437, 2006, quant-ph/0507126.

[TDL01] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung. Hiding bits in Bell states. *Phys. Rev. Lett.*, 86:5807–5810, 2001, quant-ph/0011042.

[Tuc02] R. R. Tucci. Entanglement of distillation and conditional mutual information. 2002, quant-ph/0202144.

[Uhl76] A. Uhlmann. *Rep. Math. Phys.*, 9:273, 1976.

[Uhl77] A. Uhlmann. Relative entropy and the wigner-yanase-dyson-lieb concavity in an interpolation theory. *Comm. Math. Phys.*, 54:21–32, 1977.

[Ver26] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. AIEE*, 45:109, 1926.

[Vid00] G. Vidal. Entanglement monotones. *J. Mod. Opt.*, 47:355–376, 2000, quant-ph/9807077.

[VP98] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57:1619–1633, 1998, quant-ph/9707035.

[VPRK97] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Phys. Rev. Lett.*, 78:2275–2279, 1997, quant-ph/9702027.

[VW01] K. G. H. Vollbrecht and R. F. Werner. Entanglement measures under symmetry. *Phys. Rev. A*, 64:062307, 2001, quant-ph/0010095.

[VW02] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, 2002, quant-ph/0102117.

[VWW04] K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf. Irreversibility of entanglement distillation for a class of symmetric states. *Phys. Rev. A*, 69:062304, 2004, quant-ph/0301072.

[Wer89] R. F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, 1989.

[Wer99] R. F. Werner, 1999. The list of open problems opened by R. F. Werner at the Internet under address http://www.imaph.tu-bs.de/qi/problems/.

[Wer01] R. F. Werner. All teleportation and dense coding schemes. *J. Phys. A: Math. Gen.*, 34:7081–7094, 2001, quant-ph/0003070.

[WH02] J. Walgate and L. Hardy. Nonlocality, asymmetry, and distinguishing bipartite states. *Phys. Rev. Lett.*, 89:147901, 2002, quant-ph/0202034.

[Wie83] S. Wiesner. Conjugate coding. *Sigact news*, 15:1:78–88, 1983.

[wik08a] 2008. $http://en.wikipedia.org/wiki/One-time\_pad\#cite\_note-kahn-2$.

[wik08b] 2008. $http://en.wikipedia.org/wiki/Lagrange\_multipliers$.

[wik08c] 2008. $http://en.wikipedia.org/wiki/Neighbourhood\_\%28topology\%29$.

[wik08d] 2008. $http://en.wikipedia.org/wiki/Boundary\_(topology)$.

[Win08] A. Winter, 2008. Private communication.

[WSHV00] J. Walgate, A. J. Short, L. Hardy, and V. Vedral. Local distinguishability of multipartite orthogonal quantum states. *Phys. Rev. Lett.*, 85:4972–4975, 2000, quant-ph/0007098.

[WW01] R. F. Werner and M. M. Wolf. Bound entangled gaussian states. *Phys. Rev. Lett.*, 86:3658–3661, 2001, quant-ph/0009118.

[Wyn75] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54:1355–1387, 1975.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[YHH+07] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song. Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof. 2007, arXiv:0704.2236.

[YHHSR05] D. Yang, M. Horodecki, R. Horodecki, and B. Synak-Radtke. Irreversibility for all bound entangled states. *Phys. Rev. Lett.*, 95:190501, 2005, quant-ph/0506138.

[ZHSL98] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Phys. Rev. A*, 58:883–892, 1998, quant-ph/9804024.

# Index