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

Autoreferat rozprawy doktorskiej

Karol Horodecki

1 Motywacje

Jednym ze znanych sposobów bezpiecznej komunikacji jest tak zwane szyfrowanie Vernama i Mauborgne'a (inaczej *one-time pad*), wykorzystujące losowy ciąg bitów, znany jedynie nadawcy i odbiorcy (klucz kryptograficzny) [Ver26]. Bezwarunkowe bezpieczeństwo tego kodowania na gruncie teorii informacji zostało udowodnione przez Shannona [Sha48]. Jego wadą jest fakt, że zaszyfrowana wiadomość jest bezpieczna, jeśli do szyfrowania używamy ciągu, którego długość jest proporcjonalna do ilości przesyłanej informacji. Z tego względu, jednym z istotnych problemów w kryptografii, jest problem generowania, oraz przechowywania losowego ciągu bitów, znanego jedynie nadawcy i odbiorcy, którzy są w odległych od siebie miejscach [Ver26, Sha48].

Kwantowa kryptografia, zapoczątkowana przez Wiesnera [Wie83] oraz Bennetta i Brassarda [BB84] pozwala rozwiązać ten problem. Bennett i Brassard zaproponowali protokół, który w tym celu wykorzystuje przesyłanie kubitów - odpowiedników klasycznych bitów. Aby uzyskać klucz kryptograficzny za pomocą kwantowej kryptografii, Alicja i Bob wykorzystują komunikacyjny kanał kwantowy, w celu przesyłania kubitów oraz uwierzytelniony[1] klasyczny kanał komunikacyjny, którym wysyłają klasyczne bity.

Bezpieczeństwo kwantwego rozdzielania klucza można udowodnić w ramach aksjomatów mechaniki kwantowej - teorii fizycznej [NC00]. Innymi słowy, podstawą kwantowego bezpieczeństwa jest fakt, że podsłuchiwacz (Ewa), podlega zasadom mechaniki kwantowej, która jest powszechnie akceptowaną teorią i została wielokrotnie potwierdzona w eksperymentach.

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 wyko-

[1] Założenie uwierzytelnienia kanału komunikacyjnego zapewnia, że Alicja i Bob są pewni, że rozmawiają ze sobą, tj. wyklucza atak zwany 'men in the middle'. Do uwierzytalniania potrzeba bardzo niewielkiej, jednakże niezerowej ilości klucza. Z tego powodu, kwantowe ustalanie klucza zwane bywa *kwantowym zwiększaniem klucza*.

rzystać tą własność w dowodach bezpieczeństwa kwantowych protokołów rozdzielania klucza[2]. Na szczęście, znany jest inny fenomen - kwantowe korelacje zwane *czystym splątaniem*, który jest użyteczny w dowodach kwantowego bezpieczeństwa [SP00, LC99]. Są to korelacje między dwoma podukładami układu współdzielonego przez 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' [Eke91, Sch35].

Teoria splątania rozwijała się równolegle, pozostając w widocznym związku z kwantową kryptografią. W szczególności, znane są protokóły kwantowego rozdzielania klucza bazujące częściowo [Eke91] lub wyłącznie na czystych stanach splątanych [DEJ$^+$96, BBM92, LC99]. 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. Rozkład prawdopodobieństwa tej mieszanki może być interpretowany jako nasza niewiedza o tym, w którym ze stanów czystych znajduje się układ. Wiadomo, że niektóre stany splątane, które są mieszane mogą zostać zamienione (w przybliżeniu) w stany czyste splątane za pomocą *destylacji splątania*. Schemat destylacji splątania jest podstawowym schematem teorii splątania [BDSW96]. Zgodnie z nim, Alicja i Bob przekształcają wiele kopii stanu dwuukładowego ρ_{AB}, w pewną, być może mniejszą liczbę kopii przybliżonych stanów maksymalnie splątanych. Ten schemat został zinterpretowany jako sposób otrzymywania klucza z mieszanych stanów kwantowych w [DEJ$^+$96].

Wiadomo jednak, że są *mieszane* stany splątane, które nie mogą być przetransformowane w stany czyste splątane, kiedy są współdzielone przez dwie osoby odległe od siebie[HHH98]. Stany te nazwane są *stanami o związanym splątaniu*. Otrzymywanie klucza kwantowego z tych stanów nie może opierać się bezpośrednio na destylacji czystego splątania.

Jeden z pierwszych wyników dotyczące splątania i bezpieczeństwa dowolnych dwuukładowych stanów kwantowych jest autorstwa Curty, Lewensteina i Lütkenhausa w [CLL04]. Jest to ważny związek jakościowy: *splątanie jest warunkiem koniecznym bezpieczeństwa*. Pierwszy ilościowy wynik dotyczący otrzymywania klucza z szerokiej klasy dwuukładowych stanów kwantowych, został przedstawiony przez Devetaka i Wintera [DW05, DW04]. Autorzy podają protokól otrzymywania klucza ze stanów zwanych "cqq", gdzie podukład Alicji stanu trójukładowego ρ_{ABE} (podukład E jest w posiadaniu Ewy) może być interpetowany jako zmienna losowa. Devetak i Winter podają pierwsze ograniczenie

[2]Pierwszy dowód bezpieczeństwa protokółu Bennetta i Brassarda wykorzystujący ten fakt był wyjątkowo skomplikowany [May01]

dolne na klucz destylowalny, przedstawiając rezultaty analogiczne do znanych w klasycznej kryptografii [Wyn75, Mau93, CK78].

Mimo że związek między czystym splątaniem i kwantowym bezpieczeństwem ustalony przez schemat destylacji jest całkiem dobrze znany, rozumienie relacji miedzy kwantowym bezpieczeństwem i kwantowym splątaniem w ogólności *mieszanych* splątanych, stanów kwantowych, nie jest dostatecznie rozwinięte. W związku z tym, w rozprawie rozważamy następujące problemy:

- Z jakich stanów bezpiecznych można otrzymać w wyniku pomiaru *bezpośrednio dostępny*, klasyczny klucz (Rozdział 3)?
- Jak mierzyć zawartość bezpieczeństwa stanów kwantowych ? [DW05, DW04] (Rozdział 4)
- Jakie są własności splątania stanów bezpiecznych ? (Rozdział 3, Sekcja 5.5)
- Czy można otrzymać bezpieczny klucz ze stanów o związanym splątaniu [DW05, DW04] ? (Rozdział 5)
- Jak łatwo jest odróżnić stan bezpieczny od jego zaatakowanej wersji, kiedy jeden z nich jest współdzielony przez odległe od siebie osoby ? (Rozdział 6)

W rozprawie podajemy kilka zasadniczych odpowiedzi na powyższe pytania.

2 Opis głównych wyników pracy

Wyniki przedstawione w rozprawie, mają zgodnie z naturą tematu podwójny charakter. Z jednej strony pozwalają lepiej poznać kwantową kryptografię, z drugiej strony, prowadzą do głębszego zrozumienią natury kwantowego splątania stanów mieszanych.

W **Rozdziale 2** przedstawiamy podstawowe pojęcia, definicje i fakty. W **Rozdziale 3** badamy strukturę dwuukładowych stanów kwantowych ρ_{AB}, które mają bezpośrednio dostępny, klasyczny klucz. Zakładamy, że Ewa ma dostęp do stanu ρ_E systemu puryfikującego stan ρ_{AB}, tj. Alicja Bob i Ewa mają stan czysty $|\psi_\rho\rangle_{ABE}$, którego podukład jest w stanie ρ_{AB}. Przez klasyczny klucz rozumiemy klucz kryptograficzny reprezentowany przez trójukładowe stany kwantowe postaci

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

Przez *bezpośrednią dostępność* rozumiemy dostępność za pomocą pomiaru zupełnego von Neumanna na *podukładach* układów A i B. Z tego powodu rozważamy klasę stanów duukładowych ρ o dwóch częściach: głównej AB i dodatkowej $A'B'$. Mówimy, że stan ma bezpośrednio dostępny klucz, jeśli z jego puryfikacji można otrzymać przez (i) pomiar na części głównej (ii) pozbycie się części dodatkowej, stan ρ_{key}.

Następnie definiujemy klasę stanów dwuukładowych, nazywanych **stanami bezpiecznymi**, których część główną i dodatkową nazywamy odpowiednio *częścią klucza* i *tarczą*. Stany te są postaci:

$$\gamma^{(d)}_{ABA'B'} = U|\Psi_+\rangle\langle\Psi_+| \otimes \rho_{A'B'}U^\dagger, \tag{2}$$

gdzie transformacja unitarna U jest postaci:

$$U = \sum_{kl} |kl\rangle\langle kl| \otimes U_{kl}, \tag{3}$$

oraz U_{kl} są dowolnymi unitarnymi trasformacjami, działającymi na $A'B'$ zaś $|\Psi_+\rangle = \sum_i \frac{1}{\sqrt{d}}|i\rangle_A \otimes |i\rangle_B$, jest stanem maksymalnie splątanym.

Mówiąc kolokwialnie, stany bezpieczne są "wkręconymi stanami maksymalnie splątanymi", jako że składają się z maksymalnie splątanego stanu $|\Psi_+\rangle$ na podukładzie AB, który zostaje "wkręcony" przez transformację unitarną U w układ $A'B'$. Z tego powodu, U zdefinowana w równaniu (3) jest nazywana *wkręceniem*.

Wykazujemy, że

- stany dwuukładowe, które mają bezpośrednio dostępny klasyczny klucz, są stanami bezpiecznymi.

Rozważamy również inne interpetacje *bezpośredniej dostępności* klasycznego klucza, (również te zaproponowane przez innych autorów, używane w kontekście stanów bezpiecznych [RS07, BHH$^+$08]). Okazuje się, że można je łatwo przekształcić w stany bezpieczne (i vice versa), za pomocą lokalnych operacji (cf. [RS07, BHH$^+$08]).

W **Rozdziale 4**, w celu mierzenia zawartości bezpieczeństwa dowolnego duukładowego stanu kwantowego, definiujemy *destylowalny klucz* K_D w terminach stanów bezpiecznych oraz *klasyczny klucz destylowalny* C_D w terminach stanów ρ_{key} (cf. [DW05, DW04]).

Klucz destylowalny ...

Definicja klucza destylowalnego K_D opiera się na tzw. scenariuszu LOKK (inaczej destylacji splątania), który, jak wspomnieliśmy, jest głównym scenariuszem teorii splątania [BDSW96]: Alicja i Bob otrzymują n kopii stanu ρ_{AB}. Mogą przetwarzać je za pomocą lokalnych operacji (w swoich miejscach) oraz komunikować się ze sobą 'klasycznie' tzn.

przez telefon. Ich zadaniem jest otrzymać (w przybliżeniu) stan bezpieczny z jak największą częścią klucza (powiedzmy k-kubitową). K_D jest zdefiniowane jako największy możliwy do otrzymania stosunek $\frac{k}{n}$ w granicy dużych n.

Warto zaznaczyć tutaj, że tak zdefiniowana wielkość jest *miarą splątania*, ponieważ nie można jej zwiększyć za pomocą operacji LOKK [Vid00]. Jest ona naturalnym rozszerzeniem miary zwanej destylowalnym splątaniem E_D [BDSW96], zdefiniowanej jako największa liczba dwukubitowych stanów maksymalnie splątanych, które można otrzymać z (wielu kopii) stanu ρ_{AB}.

... i klasyczny klucz destylowalny ...

Definicja klasycznego klucza destylowalnego, C_D opiera się na scenariuszu kryptograficznym [DW05, DW04] zwanym LOPK. W tym scenariuszu mamy trzy osoby: zaufane - Alicję i Boba, oraz podsłuchująca - Ewe (od ang. eavesdropper). Te trzy osoby mają dostęp do n kopii ρ_{ABE} (każda do odpowiedniego podukładu). Alicja i Bob mogą przetwarzać swoje części stanu AB za pomocą lokalnych operacji oraz publicznej (dostępnej dla podsłuchiwacza) komunikacji. Ich celem jest otrzymanie (w przybliżeniu), stanu ρ_{key} z jak największym podukładem AB (k kubitowym). C_D jest zdefiniowany jako największy możliwy do otrzymania stosunek $\frac{k}{n}$ w granicy dużych n.

... są sobie równe w najgorszym kryptograficznie scenariuszu

Następnie zajmujemy się najgorszym przypadkiem scenariuszu LOPK, kiedy ρ_{ABE} jest *stanem czystym*. W tym przypadku Ewa ma najwięcej informacji o stanie, który mają Alicja i Bob. Wykazujemy, że:

$$C_D(|\psi_\rho\rangle_{ABE}) = K_D(\rho_{AB}), \tag{4}$$

gdzie $|\psi_\rho\rangle_{ABE}$ jest *puryfikacją* - dopełnieniem ρ_{AB} do trójukładowego stanu czystego, tj. po wyśladowaniu podukładu E stanu $|\psi_\rho\rangle_{ABE}$, otrzymujemy stan ρ_{AB} który mają Alicja i Bob.

Powyższy wynik oznacza, że klasyczny destylowalny klucz w najgorszym przypadku scenariusza LOPK jest równy mierze splątania. Otrzymujemy zatem

- ilościowy związek między kwantową kryptografią i teorią splątania.

Wynik ten pozwolił zbadać bezpieczną zawartość stanów duukładowych wykorzystując podejście znane w teorii splątania. Pokazujemy, że jedna z miar splątania zwana (zregularyzowaną) *względną entropią splątania* E_r^∞ [VPRK97], jest ograniczeniem górnym[3] na wielkość klucza kryptograficznego K_D:

$$K_D \leq E_r^\infty. \tag{5}$$

[3]Wynik ten został niedawno uogólniony w [CEH$^+$07].

W **Rozdziale 5** pokazujemy, podając przykłady, że pewne stany dwuukładowe ρ spełniają:

$$K_D(\rho) > 0 \ \& \ E_D(\rho) = 0, \tag{6}$$

to znaczy są stanami o związanym splątaniu, i mimo tego, mają destylowalny klucz. Oznacza to, że

- możliwość otrzymania *czystego splątania* jest tylko dostatecznym, ale nie koniecznym warunkiem posiadania bezpieczeństwa kwantowego.

Wynik ten ma istotne znaczenie, gdyż implikuje, że

- w pewnych sytuacjach, można komunikować bezpieczne bity, mimo że nie można wysyłać wiernie kubitów.

Niektóre ze stanów o związanym splątaniu, które mają niezerowy klucz destylowalny, są specyficznymi mieszankami dwóch stanów bezpiecznych.

W **Rozdziale 6** rozważamy scenariusz rozróżniania stanów za pomocą operacji LOKK. Ograniczamy się głównie do przypadku, w którym Alicja i Bob otrzymują stan wejściowy, który z równym prawdopodobieństwem jest jednym ze stanów: stan bezpieczny γ, lub γ, którego część klucza pomierzyła Ewa (γ zaatakowany). Następnie pytamy się ile kopii stanu wejściowego potrzeba aby otrzymać prawodpodobieństwo sukcesu w rozróżnianiu bliskie 1. Podajemy przykład rodziny stanów bezpiecznych parametryzowanej wymiarem d, dla których liczba ta skaluje się **eksponencjalnie** w stosunku to liczby kubitów, które te stany zajmują. Ponieważ w podanym przykładzie γ zaatakowany nie jest stanem splątanym, otrzymujemy, że

- Niektóre stany bezpieczne są trudno odróżnialne za pomocą operacji LOKK, od pewnych stanów niebezpiecznych.

W **Rozdziale 7** podsumowujemy wyniki, prezentując głównie centralną rolę stanów bezpiecznych, jak również owocną wzajemną relację między teorią splątania i kwantową kryptografią.

Zawartość rozprawy jest głównie owocem współpracy z J. Oppenheimem oraz M. i P. Horodeckimi, jak również z Ł. Pankowskim. Bazuje ona na następujących pracach:

1. K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94:160502, 2005. quant-ph/0309110 [HHHO05b]

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]

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].

Większość ze wspomnianych wyników została uzyskana w [HHHO05b] oraz [HHHO05a]. W porównaniu z [HHHO05a], są dwie różnice w prezentacji wyników:

1. Dowód Twierdzenia 2 [HHHO05a], (Twierdzenie 3.2 w rozprawie), które podaje charakteryzację stanów mających bezpośrednio dostępny klasyczny klucz, jest zmieniony, tak, że nie wykorzystuje pojęcia wkręcenia. Rozdział 3

2. Podajemy bardziej bezpośredni dowód faktu, że istanieją stany PPT-KD (Twierdzenie 10 w [HHHO05a], Twierdzenie 5.7 w rozprawie). Konstrukcja stanów, które są istotne dla tego twierdzenia, podana w [HHHO05a], jest przedstawiona w Sekcji 5.5.

W [HPHH05], podajemy eksplicite przykłady stanów, o związanym splątaniu, które mają niezerowy destylowalny klucz. Niektóre z wyników nie zostały jeszcze opublikowane. Zawartość rozdziału 6 prezentuje rezultaty, które zostaną rozszerzone w [Hor08]. Ponadto, Sekcje 3.6, 4.4.2 i 5.5.4 oraz Obserwacja 5.5 są prezentowane po raz pierwszy w omawianej rozprawie. Jak wyróżniliśmy w tekście, niektóre fakty jedynie nadmienione, zostaną przedstawione bardziej eksplicite w [PHHH08] oraz [BHH$^+$08].

3 Dalsze wyniki dotyczące stanów bezpiecznych i problemy otwarte

Przedstawione pokrótce wyniki, były rozwijane w ostatnich latach. W rozprawie opisujemy krótko niektóre z nich. Między innymi, pojęcie stanów bezpiecznych zostało wykorzystane w uproszczeniu dowodów bezpieczeństwa [RS07]. Analogiczne rezultaty do zaprezentowanych, jak również pewne nowe efekty otrzymano dla scenariusza z większą

liczbą osób niż 2 [Aug08]. Miary splątania są ograniczeniem górnym na klucz, jeśli spełniają pewne aksjomaty [CEH$^+$07]. Destylowalność stanów dwuukładowych była badana częściowo zarówno w ramach przedstawionego schematu [CCK$^+$07, Koa07], jak również w ramach schematu kwantowego rozdzielania klucza [HHH$^+$07]

Pozostało wciąż wiele problemów otwartych, niektóre z nich przytaczamy w rozprawie. Między innymi problem czy *koszt klucza*, tj. liczba stanów bezpiecznych potrzebna do wytworzenia danego stanu, jest równa kluczowi destylowalnemu. Odpowiedź na to pytanie wymaga dalszego badania klasy stanów bezpiecznych. W szczególnośći nie zostały scharakteryzowane stany bezpieczne, które są *nieredukowalne*, tj. spełniają $K_D(\gamma^{(d)} = \log d$. Jednym z nich jest następujące fundamentalne pytanie:

- Czy wszystkie stany splątane mają niezerowy destylowalny klucz ?

Mamy nadzieję, że owocna interakcja między teorią kwantowego splątania i kwantową kryptografią doprowadzi do odpowiedzi na powyższe jak i na wiele innych istotnych pytań dotyczących obu teorii.

Literatura

[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.

[BBM92] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[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.

[BHH$^+$08] P. Badziag, P. Horodecki, K. Horodecki, M. Nowakowski, and Ł. Pankowski, 2008. in preparation.

[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.

[CK78] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE*, 24:339–348, 1978.

[CLL04] 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.

[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.

[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.

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[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.

[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.

[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. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94:160502, 2005, quant-ph/0309110.

[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.

[Koa07] M. Koashi. Complementarity, distillable secret key, and distillable entanglement. 2007, arXiv:0704.3661.

[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.

[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE*, 39:773–742, 1993.

[May01] D. Mayers. Unconditional security in quantum cryptography. *J. Assoc. Computing Machinery*, 48:351–406, 2001, quant-ph/9802025.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press,Cambridge, 2000.

[PHHH08] Ł. Pankowski, K. Horodecki, M. Horodecki, and P. Horodecki. On the private states, 2008. In preparation.

[RS07] J. M. Renes and G. Smith. Noisy processing and distillation of private quantum states. *Phys. Rev. Lett.*, 98:020502, 2007, quant-ph/0603262.

[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.

[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.

[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.

[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.

[Wie83] S. Wiesner. Conjugate coding. *Sigact news*, 15:1:78–88, 1983.

[Wyn75] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54:1355–1387, 1975.