# University of Warsaw

## Faculty of Mathematics, Informatics and Mechanics

Jakub Derbisz

# Access structures and elliptic curve cryptosystems

*PhD dissertation*

Supervisor

**dr hab. Jacek Pomykała**

Institute of Mathematics

University of Warsaw

May 2013

## 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*                                                           *Jakub Derbisz*

## Supervisor's declaration:

the dissertation is ready to be reviewed.

......................................                    ..............................................

*date*                                                           *dr hab. Jacek Pomykała*

# Abstract

We develop the theory of access structures and include elliptic curve based cryptosystems applications. Shown are results concerning methods of encrypting monotonic access structures basing on logical formulae and our proposed, extended method with an abstract function, basing on set-theoretic approach. Introduced is an idea of hierarchy in any general access structure and shown are results related to security with respect to the hierarchy. Given are multivariate extensions of secret sharing schemes. Included are considerations on threshold sharing with a multivariate polynomial and a setting for generalized secret sharing. They are based on generalized Chinese Remainder Theorem in multivariate polynomial ring and use methods of the theory of Gröbner bases. Given are elliptic curve based applications in a form of general access structure based signature schemes. The considerations extend to the general access structure based decryption schemes. General access structure in these applications could be given by, apart of method related to a generalized Asmuth-Bloom sequence, by a method based on logical formulae, a method based on extended Blakley's scheme and our method based on plain set-theoretic approach with an introduced abstract function. The bilinear pairings which are appropriate for the designs of our schemes are for instance modified Weil pairing or modified Tate-Lichtenbaum pairing.

## Keywords

# Streszczenie

Rozwijamy teorię struktur dostępu uwzględniając kryptograficzne zastosowania oparte na teorii krzywych eliptycznych. Uzyskano wyniki związane z metodami szyfrowania monotonicznych struktur dostępu, opartymi na formułach logicznych oraz zaproponowaną przez nas, uogólnioną metodą opartą na podejściu teorio-mnogościowym korzystającą z abstrakcyjnej funkcji. Wprowadzone jest pojęcie hierarchii w dowolnej ogólnej strukturze dostępu i uzyskano wyniki związane z bezpieczeństwem dotyczącym hierarchii w naszym ujęciu. Podane zostały rozszerzenia schematów dzielenia sekretu na wiele zmiennych. Możemy zaliczyć tutaj rozważania dotyczące rozdzielania progowego wykorzystującego wielomian wielu zmiennych oraz w podobnym duchu, rozdzielania w ogólnej strukturze dostępu. Oparte są one na uogólnionym Chińskim Twierdzeniu o Resztach w pierścieniu wielomianów wielu zmiennych i używają metod z teorii baz Gröbnera. Podane zostały zastosowania wykorzystujące krzywe eliptyczne w postaci schematów podpisu w ogólnej strukturze dostępu. Rozważania te przenoszą się na schematy deszyfrowania w ogólnej strukturze dostępu. Ogólna struktura dostępu w zastosowaniach tych może być zadana, obok metody związanej z uogólnionym ciągiem Asmutha-Blooma także przez metodę opartą na formułach logicznych, metodę opartą na rozszerzonym schemacie Blakley'a oraz naszą metodę opartą na czystym teorio-mnogościowym podejściu z wprowadzoną funkcją abstrakcyjną. Iloczynem dwuliniowym, użytecznym w konstrukcjach naszych schematów jest zmodyfikowany iloczyn Weila lub zmodyfikowany iloczyn Tate'a-Lichtenbauma.

## Słowa kluczowe

struktura dostępu, podział sekretu, formuły logiczne, rodzina zbiorów bazowych, rodzina zbiorów anty-bazowych, metoda teorio-mnogościowa, hierarchia, uogólnione CRT, bazy Gröbnera, krzywe eliptyczne, kryptografia oparta na iloczynie dwuliniowym, kryptosystem grupowy, grupowy schemat podpisu

## Klasyfikacja AMS

94A60, 94A62, 14G50, 14H52, 68P25

# Acknowledgements

I would like to thank my advisor Jacek Pomykała for sharing ideas and organizing research seminars. I am also grateful to Konrad Durnoga and Bartosz Źrałek for well spent time during the research seminars.

# Contents

# Introduction

Access structure is a tuple $(\Sigma, \Gamma, \Lambda)$, where $\Sigma$ is a secret sharing scheme (further called simply sharing scheme), $\Gamma$ a monotonic structure and $\Lambda$ an anti-monotonic structure, where a monotonic structure forms a family of privileged (qualified) sets, and anti-monotonic structure forms a family of unqualified sets. Having only family of basis sets of certain monotonic structure $\Gamma$, that is minimal sets generating $\Gamma$, or just the family of anti-basis sets, that is maximal sets generating certain anti-monotonic family $\Lambda$, there exist a unique access structure modulo perfect sharing schemes $\Sigma$. Showing this result allows us to describe an access structures in terms only of basis sets or anti-basis sets having in mind certain fixed perfect sharing scheme (it is shown that in both cases there exist appropriate perfect sharing schemes). This is the basic preliminary fact related to the terminology we use, and basic concepts in our thesis.

One can identify a sharing scheme $\Sigma$ with a method of distributing a secret (more precisely parts of the secret) among entities in a certain set. Having an access structure with such $\Sigma$, a monotonic structure $\Gamma$ is a family of these subsets, that are able to reconstruct the secret, and $\Lambda$ are these subsets that can not.

Starting from giving the adequate definitions, using as a basis set-theoretic and probabilistic type terminology we achieve results making use of set-theoretic, combinatorial and logic related reasoning, through Gröbner bases methods in constructing multivariate polynomial based secret sharing schemes, and constructions based on theory of elliptic curves over finite fields related to bilinear pairings such as modified Weil or Tate-Lichtenbaum pairings. Making use of a group where Computational Diffie Hellman Problem is hard while Decision Diffie Hellman Problem is easy, due to the existence of bilinear pairing, we propose a general access structure based signature scheme. A similar construction can lead to a general access structure based group decryption scheme.

In chapter with preliminaries for the thesis, basic approaches to constructing perfect sharing schemes for general (monotonic) access structures are given. Later, in the following chapter, given is a generalization into abstract situation with a function satisfying certain set-theoretic conditions. There are presented two examples of such functions. The abstract function has in its domain a family of sets, the set of values is also a family of sets, and satisfies such conditions that giving any of its realizations results in different methods of encrypting monotonic access structure. This generalized method, besides others that are presented during the thesis, finds its application in the final chapter, in the construction of general access structure based signature scheme.

In the thesis appropriately to the set-theoretic and probabilistic terminology, described are classical ideal sharing schemes as Shamir's and Blakley's schemes. In this terminology also presented is a sharing scheme we refer to as extended Blakley's scheme and which originates from [10]. The description of these schemes is unified, making a use of notion of polynomials in the basis of each. This later extends in the third chapter to an attempt to constructing schemes that are somehow more general than sharing schemes presented in the literature so far and have in its base a multivariate polynomial. This new in the literature approach makes use of elements of the theory of Gröbner bases. Introduced technique is based on the algorithm for finding the minimal Chinese Remainder Theorem solution (with respect to certain quasi-order) in multivariate polynomial ring. The algorithm comes from [4]. We also use the fact that it allows to find the form of all CRT-solutions.

In presented related sharing schemes, shares of the participants could be multivariate polynomials. With every participant it is associated his public ideal of a multivariate polynomial ring. Presented is a theoretical framework for realization of threshold sharing schemes based on multivariate polynomial. In the thesis given are also some examples of such realization. The approach allows to give a proposition of realization of $(t, t)$ threshold secret sharing scheme basing on multivariate polynomial whose degree is a priori not known to the participants. That perspective on sharing schemes is also relevant for the construction of generalized secret sharing scheme to share a multivariate polynomial or a value in its chosen argument. In contrary to the theoretical abstract framework for the construction of threshold scheme, it can be realized in certain access structures just from its exposition in the thesis. As a result we get an interesting proposition with several advantages. One of them is that the shares, when being non-constant polynomials, allow to send participants hidden messages by

publicly announcing argument-points (the sender of hidden messages is an entity who has encrypted in the form of shares the multivariate polynomial).

Part of the thesis, from second chapter, deals with the comparison of two ways of encrypting monotonic access structure. First of them is well known. It was proposed by Benaloh and Leichter in [7]. It is related to the possibilities of encrypting monotonic access structure when given is a monotonic logical formula. The second way, already mentioned, is our extended method of encrypting monotonic access structure that is based on set-theoretic approach. There, starting from a family of basis or anti-basis sets, with a use of special function, one gets a secret sharing scheme.

Shown are dependencies between those two methods. We prove the following theorems, which are called that rather because of their importance in access structures theory, not their difficulties in proof:

**Theorem 2.2.1** *Let $F$ be any monotonic logical formula defining a monotonic structure $\Gamma$. Converting $F$ into disjunctive normal form and making reductions such that there are no clauses contained as sets of literals in other clauses, sets made of indices of clauses define a basis of $\Gamma$.*

and the dual version:

**Theorem 2.2.2** *Let $F$ be any monotonic logical formula defining a monotonic structure $\Gamma$. Writing $F$ in a conjunctive normal form which is reduced such that there are no clauses contained as sets of literals in other clauses, sets forming an anti-basis are constructed by choosing a clause of the formula and extracting all indices omitting these indexing the chosen clause.*

We refer to the end of Section 1.3 to see how monotonic logical formula defines a monotonic structure.

Idea of hierarchy in a general access structure is presented. It is not the idea of the known in the literature hierarchical access structure. We rather present our definition of hierarchy which is meant to be intuitive. We want to have a concept of hierarchy in any general access structure by specifying the participants that are intuitively more desirable for an adversary to be corrupted. We however do not concentrate on the theoretical aspects of that kind of definition, but rather take into consideration practical aspects of sharing a secret which are related to hiding places that an entity takes in

13

a hierarchy intuitively understood this way. By doing this our aim is to prevent an adversary from being able to distinguish, for instance, the participant who is the highest or very important in some general access structure, from the least important. We present the relevant sharing scheme for hiding places of entities in the hierarchy. We deal with some specific issues related to the security in this topic, and show for example:

**Theorem 2.3.1** *For a family of basis sets $\boldsymbol{B}$ of the monotonic access structure such that no entity can reconstruct the secret by himself, it can be guaranteed that subsets $S_i$ related to the entities, in a process of distributing the shares basing on approach with anti-basis, are not contained in one another.*

Sets $S_i$ that are here considered are related to our construction based on abstract function $f$, which realizations implie secret sharing schemes. $f(S_i)$ is a set that is a share of $i$-th participant.

Finally presented are bilinear pairing on elliptic curves over finite fields based constructions for general access structures. The bilinear pairings that can be the base of the constructions are for instance modified Weil pairing or modified Tate-Lichtenbaum pairing. We show how with different methods of encrypting monotonic access structure to construct general access structure based signature schemes. We remark that it is possible to transfer the ideas from signature schemes into general access structure based decryption schemes. The methods of encrypting a structure that we consider are: first based on CRT-Ore algorithm that makes use of a generalized Asmuth-Bloom sequence. Signature scheme with that method was considered by Pomykała. Second based on extended Blakley's scheme. Third based on logical formulae, and eventually fourth based on our abstract plain set-theoretic approach.

Even though cryptography is naturally related to applications we find pleasant the part of theoretical mathematical ideas and theories that are being developed alongside. Thus our presentation, being theoretical, encloses explicit and computationally efficient constructions adequate to further applications.

# Chapter 1

# Secret sharing in a distributed system

In this chapter we give preliminaries being known basic definitions and concepts used throughout our work. We define a *monotonic structure*, an *anti-monotonic structure*, give a definition of *secret sharing scheme* and the meaning of $\Gamma$-reconstruction and $\Lambda$-privacy. We define the basic concept of *access structure* and give the definitions of schemes being *perfect* and *ideal*. Having them, using as a basis probabilistic notation based on random polynomials, written are formally the classical Shamir's and Blakley's schemes. It is shown that the Blakley's scheme is an instance of the scheme originating from [10], which is written accordingly to formalization we use, and to which we will later refer to as extended Blakley's scheme. We introduce *basis of the structure* and *anti-basis of the structure*. With them we show the known elementary methods of constructing perfect schemes for general access structures. We prove Lemma 1.3.1 stating how to uniquely determine an access structure. At last basing on [7] we present a method of using monotonic logical formulae as a possiblity to define monotonic access structures. Summarizing, we are showing the concepts related to the known terminology and its logical structure.

Distributed systems in our context are part of cryptographic systems, where storing parts of cryptographic keys in distinct localizations is performed to increase security of secret keys themselves. It allows to minimalize the probability of intercepting the key by an adversary and hence reduces the possibility of compromising the cryptosystem. In general, the idea is realized by secret sharing protocols. The secret key of a cryptographic system is created from shares generated in distinct localizations. Secret sharing protocols are the basis of access structures. A family of privileged sets is constructed and participants have an access to information or can authorize it if and only if they are

cooperating within the privileged group. This concept originates from two independent and known papers of Blakley and Shamir from 1979 (see [9], [47]). Ito, Seito, Nishizeki in their work [36] from 1987 described a general method of distributing a secret such that only previously chosen, privileged subsets can reconstruct it. Later continued in [7] where Benaloh and Leichter propose their way of sharing a secret in a general, monotonic access structure. Now we introduce the idea of general secret sharing.

## 1.1. Monotonic access structures

We begin with preliminaries, definitions and elementary concepts.

$X = \{1, 2, ..., n\}$ is the set of entities, we also refer to it as to set of participants.

**Definition 1.1.1.** *Monotonic structure (family) on $X$ is a collection $\Gamma \neq 2^X$ of subsets of $X$ that satisfies the following conditions:*

1. *$X \in \Gamma$*
2. *If $A \in \Gamma$ and $A \subseteq B \subseteq X$ then $B \in \Gamma$.*

There is a dual idea.

**Definition 1.1.2.** *Anti-monotonic structure (family) $\Lambda$ on $X$ is a collection of subsets of $X$ such that if $A \in \Lambda$ and $B \subseteq A$ then $B \in \Lambda$.*

Consider the probability space $(\Omega, \mu)$, $|\Omega| < \infty$. Let $S : \Omega \to X$ be a random variable. By abuse of notation we shall denote by $S$ the set of values of a random variable $S$. Induced probability distribution on $S$ is denoted $p_S(s) = p_S(S = s) = \mu(S^{-1}(s))$. Therefore we regard $(S, p_S)$ as a corresponding probability space. Let $(S_i, p_{S_i})$, $i = 1, ..., n$ be a collection of corresponding probability spaces to random variables $S_i$, $i = 1, ..., n$ respectively, defined on $(\Omega, \mu)$. Taking $S_0 = S_1 \times ... \times S_n$ we define joint probability space as a pair $(S_0, p_0)$, where for any $(s_1, ..., s_n) \in S_0$ we put:

$$p_0((s_1, ..., s_n)) = \mu(S_1^{-1}(s_1) \cap ... \cap S_n^{-1}(s_n))$$

We notice that

$$p_0(\pi_i^{-1}(S_i = s_i)) = p_i(S_i = s_i) \text{ for } i = 1, 2, ..., n,$$

where $\pi$ is the projection of $S_0$ onto the $i-th$ component. We say that $S_1, ..., S_n$ are jointly distributed, $p_0$ is their joint probability distribution and correspoinding random variable we denote as $S_0 = S_1...S_n$.

Let $S_1$, $S_2$ be random variables defined on $(\Omega, \mu)$ and $S_0 = S_1 S_2$ have joint probability distribution $p_{S_0}$. Assume that $prob(S_2 = s_2) > 0$. Then conditional probability is:

$$prob(S_1 = s_1 | S_2 = s_2) = \frac{p_{S_0}((s_1, s_2))}{p_{S_2}(S_2 = s_2)}$$

If $S_1, ..., S_n$ are random variables defined on $(\Omega, \mu)$, for a non-empty set $A = \{i_1, ..., i_k\} \subseteq X = \{1, 2, ..., n\}$ we define $S_A$ to be a joint probability distribution of $S_{i_1} S_{i_2}...S_{i_k}$. Moreover let $S_A$ denote the corresponding subsequence of $(S_1, ..., S_n)$.

Now we give some significant for us definitions.

**Definition 1.1.3.** *A secret sharing scheme $\Sigma$ for a set $X = \{1, ..., n\}$ is a tuple $(S, S_1, ..., S_n)$ satisfying the following conditions:*

*1. $prob(S = s) = \frac{1}{|S|}$ for all $s \in S$.*
*2. If $prob(S_X = s_X) > 0$ then there is a unique $s \in S$ that $prob(S = s | S_X = s_X) = 1$.*

*The values taken by $S$ are called secrets while the values taken by $S_i$ for $i = 1, ..., n$ are called shares. $X = X(\Sigma)$ is called either the set of entities or the set of participants.*

We move to reconstruction and privacy requirements for monotonic structures. Consider a monotonic structure $\Gamma$ consisting of all subsets $B$ of $X$ that would be able to reconstruct the secret $s$ - it will be called reconstruction property. On the other hand there is an anti-monotonic structure $\Lambda$ consisting of subsets $A$ of $X$ which are not able to derive any information about the secret $s$ - it will be called $\Lambda$-privacy condition. Formally:

**Definition 1.1.4.** *A sharing scheme $\Sigma = (S, S_1, ..., S_n)$ satisfies $\Gamma$-reconstruction property if for all $B \in \Gamma$ distribution $S_B$ determines $s$ uniquely i.e. if $prob(S_B = s_B) > 0$ then there exists a unique $s \in S$ such that $prob(S = s | S_B = s_B) = 1$.*

**Definition 1.1.5.** *A sharing scheme $\Sigma = (S, S_1, ..., S_n)$ satisfies $\Lambda$-privacy condition if for all $A \in \Lambda$, where $A \neq \emptyset$, $S_A$ gives no information on $S$ i.e. $prob(S_A = s_A) > 0$ implies that for all $s \in S$ $prob(S = s | S_A = s_A) = \frac{1}{|S|}$.*

17

In what follows we consider the tuple $(\Sigma, \Gamma, \Lambda)$. We call this triple an access structure if $\Gamma = \Gamma(\Sigma)$ and $\Lambda = \Lambda(\Sigma)$ satisfy the maximality condition. More precisely:

**Definition 1.1.6.** *The access structure is a triple $(\Sigma, \Gamma(\Sigma), \Lambda(\Sigma))$, where $\Gamma(\Sigma)$ is the maximal monotonic structure $\Gamma$ such that $\Sigma$ satisfies $\Gamma$-reconstruction, while $\Lambda(\Sigma)$ is the maximal anti-monotonic structure $\Lambda$ such that $\Sigma$ satisfies $\Lambda$-privacy. Elements of $\Gamma(\Sigma)$ are called privileged or qualified sets, elements of $\Lambda(\Sigma)$ are called unprivileged or unqualified sets.*

We define perfect schemes and ideal schemes in the following way:

**Definition 1.1.7.** *Scheme $\Sigma$ is called perfect if $\Gamma(\Sigma) \cup \Lambda(\Sigma)$ are all subsets of $X$. If additionally $S_1 = S_2 = ... = S_n = S$ then $\Sigma$ is called ideal.*

We see that if the scheme is perfect then a set of participants could either reconstruct a secret or can not deduce any information about the secret. In ideal schemes, additionaly, equal are all sets of (possible) shares for the participants and set of (possible) secrets.

For all monotonic structures $\Gamma$ there exists a perfect secret sharing scheme $\Sigma$ such that $\Gamma(\Sigma) = \Gamma$. It means that for a given $\Gamma$ one can describe a way of distributing shares to the participants (i.e. describe random variables $S_i$, $i = 1, ..., n$) and a way of choosing a secret (i.e. a random variable $S$), such that sets of participants able to reconstruct the secret (i.e. those sets $B \subseteq X$ which distribution $S_B$ determines a secret uniquely, as in definition of $\Gamma$-reconstruction) are exactly the sets from $\Gamma$. Other sets can not deduce anything about the secret. In the following sections we will explicitly see the construction of perfect sharing schemes for a given $\Gamma$.

On the other hand, as it is shown in [7], there are access structures for which there is no ideal sharing scheme. Discussion on ideal secret sharing can for instance be found in [8], [10], [11].

## 1.2. Formal constructions of ideal schemes related to threshold structures

The answer to the question of how to distribute a secret among a group of participants such that only certain subgroups, called privileged, could reconstruct it was firstly given in 1979, independently by Blakley [9] and Shamir [47]. Threshold schemes that were introduced in those papers, with the threshold $t$, allow to distribute a secret field element

$s$ to $n$ participants, such that any $t$ or more entities can reconstruct it, and less than $t$ participants can not deduce any information about the secret, meaning every potential secret is for these groups equally probable. The Shamir's scheme is typically realized using a polynomial $f$ of degree $t-1$ over $\mathbb{F}_q$, a finite field of $q$ elements. The free term (usually) represents the secret value $s$, and the shares of $n$ participants are nodes of the form $(x, f(x))$, or rather just $f(x)$ while publicly available $x$ is participant's identity. With $t$ of these nodes one can reconstruct the polynomial since the corresponding system of equations has a unique solution. Thus, in particular one can read the free term. The $(t, n)$ Blakley's scheme is similar. Here, instead of $f$ being a univariate polynomial, it is a polynomial of degree 1 from $\mathbb{F}_q[X_0, ..., X_{t-1}]$ which has the free term equal to zero, so $f = \sum_{i=0}^{t-1} a_i X_i$. The coefficient of chosen variable (for example coefficient of $X_0$) represents the secret value $s$. The shares of the participants are (argument, value) nodes. We could also, as share, just take the value, then the argument is an identity of the participant. We notice, that the idea has a natural geometric interpretation, which is used commonly while characterizing Blakley's scheme. A participant having the share $s_i$ and his vector of identity $(x_{i0}, ..., x_{it-1})$ has an equation with the variables $(a_0, ..., a_{t-1})$ of the form $a_0 x_{i0} + ... + a_{it-1} x_{it-1} = s_i$ which simply is an equation of an affine hyperplane in $\mathbb{F}_q^t$.

In both schemes identities of entities, which are arguments of the polynomials above, has to be chosen in a proper way, so the schemes are really $t$-threshold sharing schemes (for example, in Shamir's scheme the secret, instead of free term, could be at some other coefficient, and then the choice of identities is not trivial). Discussion on allocation of the identities can be found in [50], [10], [47], [54], [39].

We show a formal construction of sharing schemes. We extend our work in [24] which was using ideas of [18]. The random polynomial based terminology would lead to the new perspective on polynomial methods, proposed in Chapter 3.

For Shamir's scheme, let $K = \mathbb{F}_q$ where $q$ is greater than the number of entities $n$ (in applications $q$ is appropriately large due to the security reasons). Let $x_1, \ldots, x_n$ be pairwise different nonzero elements of the field $\mathbb{F}_q$. That would be public identities of the participants.
Take $S = S_1 = \cdots = S_n = K$, $\Gamma = \{B \subseteq X : |B| \geqslant t\}$ and $\Lambda = \{A \subseteq X : |A| \leqslant t - 1\}$. We define the probabilistic space $(\Omega, \mu) = (K^t, \mu)$ where $\mu(\mathbf{k}) = \frac{1}{|K|^t}$ for any $\mathbf{k} \in K^t$. Now let $f = f(X) = a_0 + a_1 X + \cdots + a_{t-1} X^{t-1} \in K[X]$ be selected randomly, i.e. each

$a_i \in K$ is selected uniformly and independently from $K$. The secret $s$ is defined as the value $f(0) = a_0$. The shares given to the participants are the elements $s_j = f(x_j)$ for $j = 1, ..., n$. We define the random variable $S_i$ so that: $S_i$ takes value $s_i \iff f(x_i) = s_i$, thus:

$$prob(S_i = s_i) = \frac{\#\{f : (x_i, s_i) \in \text{Graph } f\}}{|K|^t} = \frac{|K|^{t-1}}{|K|^t} = \frac{1}{|K|} = \frac{1}{q} \ .$$

Probability distribution of $S$ is defined by: $S$ takes value $s \iff f(0) = s$, and similarly

$$prob(S = s) = \frac{1}{q} \ .$$

In a similar fashion by taking $A = \{i_1, \ldots i_k\}$, we obtain

$$prob(S_A = s_A) = prob(S_{i_1} = s_{i_1}, \ldots, S_{i_k} = s_{i_k}) = \frac{1}{q^k} \ , \ \text{if } k \leqslant t$$

$$\text{if } prob(S_A = s_A) > 0 \ \text{ then } \ prob(S_A = s_A) = \frac{1}{q^t} \ , \ \text{for } k > t.$$

which is easily seen looking at the linear equation system

$$\begin{pmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_k} & \cdots & x_{i_k}^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} s_{i_1} \\ \vdots \\ s_{i_k} \end{pmatrix},$$

where for $k \leqslant t$ the rows of nonsingular Vandermonde matrix are independent and we can transform the matrix to reduced row echelon form which gives that $t - k$ variables $a_i$ are free. We could say as well, similarly as will be in Proposition 1.2.1, that from theorem of Kronecker-Capelli the dimension of solution space $W$ of the corresponding homogeneous system is $t - k$ and the set of all solutions is $\alpha + W$, where $\alpha$ is one of the solutions, which of course exists. Then one can take any $t - k$ coefficients of chosen base vectors of $W$ to write a solution with a given $\alpha$ and the basis.

Now, for $|A| \leqslant t - 1$, taking $k = |A|$

$$prob(S = s | S_A = s_A) = \frac{p_{SS_A}((s, s_A))}{p_{S_A}(s_A)} =$$

$$= \frac{prob(f(0) = s, f(x_{i_1}) = s_{i_1}, \ldots, f(x_{i_k}) = s_{i_k})}{prob(f(x_{i_1}) = s_{i_1}, \ldots, f(x_{i_k}) = s_{i_k})} = \frac{q^{-(k+1)}}{q^{-k}} = \frac{1}{q} \ .$$

On the other hand for any $B$ such that $|B| \geqslant t$ and $p_{S_B}(s_B) > 0$, there is a unique $s$ such that:

$$prob(S = s | S_B = s_B) = \frac{p_{SS_B}((s, s_B))}{p_{S_B}(s_B)} = \frac{q^{-t}}{q^{-t}} = 1 \ .$$

which ends analysis of Shamir's sharing scheme. We see it is perfect. It also satisfies the condition required for being ideal.

Extended Blakley's scheme. Before formally describing Blakley's scheme, we show a scheme that we will call extended Blakley's scheme. It originates from [10] by Brickel, where we give a slight generalization. We consider:

$$f = f(X_0, X_1, \ldots, X_{t-1}) = a_0 X_0 + a_1 X_1 + \cdots + a_{t-1} X_{t-1} \in K[X_0, \ldots, X_{t-1}] \ ,$$

selected randomly choosing coefficients. The identities of the participants are vectors $\mathbf{x}_1 = (x_{10}, x_{11}, \ldots, x_{1t-1}), \ldots, \mathbf{x}_n = (x_{n0}, x_{n1}, \ldots, x_{nt-1})$. The secret $s$ is defined as $f(\mathbf{v}) = s$ for publicly known vector $\mathbf{v} \in \mathbb{F}_q^t$. The shares given to the participants are $s_j = f(\mathbf{x}_j)$ for $j = 1, \ldots, n$. Random variable $S_i$ takes value $s_i \iff f(\mathbf{x}_i) = s_i$. Random variable $S$ takes value $s \iff f(\mathbf{v}) = s$. Without giving any restriction on vectors of identities we have an access structure which form is implied by the proposition that originates from proposition from [10]. We however give a proof based on our setting.

**Proposition 1.2.1.** *A subset of participants in extended Blakley's scheme is privileged if and only if the corresponding set of identities spans the subspace containing $\boldsymbol{v}$.*

**Proof.** Let $C$ be the set of participants and $U = \{\mathbf{x}_{i_1}, \ldots, \mathbf{x}_{i_k}\}$ be the corresponding set of identities. If $\mathbf{v}$ lies in the subspace spanned by $U$, if $p_{S_C}(s_C) > 0$ then there is a unique $s$ such that

$$prob(S = s | S_C = s_C) = \frac{prob(f(\mathbf{v}) = s, f(\mathbf{x}_{i_1}) = s_{i_1}, \ldots, f(\mathbf{x}_{i_k}) = s_{i_k})}{prob(f(\mathbf{x}_{i_1}) = s_{i_1}, \ldots, f(\mathbf{x}_{i_k}) = s_{i_k})} = 1 \ ,$$

since having $\mathbf{v} = \sum_{j=1}^{k} c_{i_j} \mathbf{x}_{i_j}$ there is

$$f(\mathbf{v}) = f(\sum_{j=1}^{k} c_{i_j} \mathbf{x}_{i_j}) = \sum_{j=1}^{k} c_{i_j} f(\mathbf{x}_{i_j}) = \sum_{j=1}^{k} c_{i_j} s_{i_j} \ ,$$

which could be taken for $s$. That means $C$ is a privileged set.

If the subspace spanned by $U$ does not contain $\mathbf{v}$ then from the theorem of Kronecker–Capelli, for the linear system $f(\mathbf{x}_{i_j}) = s_{i_j}$, $j = 1, ..., k$, solutions of the corresponding homogeneous system span the subspace that has one more vector in its basis than the subspace spanned by solutions of homogeneous system related to linear system: $f(\mathbf{x}_{i_j}) = s_{i_j}$, $j = 1, ..., k$ and $f(\mathbf{v}) = s$. It is simply because the rank of the matrix having for rows $\mathbf{x}_{i_j}$, $j = 1, ..., k$ is one less than the rank of the extended matrix by a vector $\mathbf{v}$. Hence, if $p_{S_C}(s_c) > 0$, meaning a solution of the linear system $f(\mathbf{x}_{i_j}) = s_{i_j}$, $j = 1, ..., k$ exists, which also implies that the linear system with additional $f(\mathbf{v}) = s$ has a solution (since one could see that, ranks of matrices of linear system and corresponding homogeneous system are equal, which from the theorem of Kronecker-Capelli is equivalent for a solution to exist), we have:

$$prob(S = s | S_C = s_C) = \frac{prob(f(\mathbf{v}) = s, f(\mathbf{x}_{i_1}) = s_{i_1}, \ldots, f(\mathbf{x}_{i_k}) = s_{i_k})}{prob(f(\mathbf{x}_{i_1}) = s_{i_1}, \ldots, f(\mathbf{x}_{i_k}) = s_{i_k})} = \frac{1}{q} \; .$$

Thus $C$ is an unqualified set.

$\square$

We note that the generalized situation, related to more general than threshold, monotonic family of sets $\Gamma$, may be linked to the considerations on placing the secret and problem of distributing the identities to the participants in paper [50] of Spież, Srebrny and Urbanowicz, where the authors give conditions for the construction of threshold schemes. Further in our thesis we often consider general access structures.

For the formal construction of Blakley's scheme we use the setting from extended Blakley's scheme with a vector $\mathbf{v}$ equal for instance to $(1, 0, ..., 0) \in \mathbb{F}_q^t$, where we guarantee the two following conditions on choosing the identities. Eventually, we can perform an analysis of Blakley's scheme, which is essentially the same as in the case of Shamir's scheme. For the scheme to be $t$-threshold scheme it is enough that vectors of identities satisfy the following conditions:
1) any subset of $t$ vectors of identities is linearly independent
2) adding vector $\mathbf{v}$ to any subset of $t - 1$ vectors of identities gives linearly independent set of vectors

To show this, we look at the Proposition 1.2.1.

**Remark 1.2.1.** *In the presented schemes, if the Trusted Authority wants to make the specified secret key $s_0 \in \mathbb{F}_q$ to be reconstructed by the privileged groups, he publishes $s_1 = s_0 - s$. An unprivileged group having $s_1$ knows that some element $s$ has to be added to reconstruct the key $s_0$. Because all $s \in \mathbb{F}_q$ seems for this group equally likely, then all elements of $\mathbb{F}_q$ for $s_0$ are equally probable. Privileged groups can reconstruct $s$ and add it to $s_1$, which yields $s_0$.*

What we could see in this section, having polynomials in the base of each of presented schemes, the idea of sharing a secret introduced by Blakley and Shamir comes from an interpolation of a polynomial of one variable or more. Interpolation in Shamir's scheme is the Lagrange interpolation. It is similar when interpolating multivariate polynomial in Blakley's scheme. One could think of different interpolation methods that are already known, as Hermite interpolation, Birkhoff interpolation (as it was noticed in [52]) or using some special functions or multivariate interpolations (such as from survey article [34], see also [53]). The difference may be simply in meaning of shares. Some of them may be derivatives of polynomials in certain points, where the intuition (used in [52]) is that lower derivative orders carry more information than higher ones. That is why the methods with derivatives were appropriate to the known in the literature hierarchical systems.

Looking at the Lagrange interpolation from the perspective of algebra, it can be treated as an instance of the Chinese remainder theorem in the principal ideal domain of $K[X]$, where one searches for the polynomial belonging to the sets intersection $\bigcap_{i=1}^{t} (r_i + (X - c_i))$, where $(X - c_i)$, $i = 1, ..., t$ are ideals of $K[X]$. It is a special case of generalized CRT (see [4]), which gives the generalization of CRT algorithm for PID as $K[X]$ to CRT algorithm in multivariate polynomial ring $K[X_1, ..., X_l]$. New in the literature applications to sharing schemes which use that language to give their generalization to multivariate case are shown in this work in Chapter 3.

# 1.3. Approaches to constructing perfect schemes for monotonic structures

There are known two basic approaches to the construction of perfect secret sharing scheme for any general access structure (we recall that a general access structure has not necessairly threshold monotonic family). One is related to the family of all minimal qualified sets of $X$, which we will call a family of basis sets. The other is related to the family of maximal non-qualified sets, an anti-basis. The methods presented here will be the subject of further generalizations, given in the second chapter. We prove our Lemma 1.3.1 relating the family of basis sets or the family of anti-basis sets to the construction of an access structure. This allows us to say, while considering triple $(\Sigma, \Gamma, \Lambda)$ being an access structure, only about a monotonic structure $\Gamma$ or only about an anti-monotonic structure $\Lambda$. In that case we have in mind certain fixed sharing scheme $\Sigma$ which, as we present, can always be constructed.

**First approach**

We show a method which for 'an input' being a monotonic family of sets, constructs a sharing scheme (a way of distributing shares, parts of a secret, to the participants) such that participants from a given set from the monotonic family, from shares that they will receive, are able to reconstruct the secret. Other sets of participants are unqualified, meaning their shares do not provide them any information about the secret. It will be described using the family of all minimal sets in a monotonic access structure. These sets define the monotonic structure.

Firstly, assume that $\Gamma = X$. In this case we may apply either Shamir's secret sharing or the simpler, additive secret sharing scheme as follows:

Let $s_0 \in K$ ($K = \mathbb{F}_q$) be the secret to be distributed among the set of entities $X$. Fix $j_0 \in X$. For each $j \in X \setminus \{j_0\}$ we select independently and uniformly a random $r_j \in K$ and define $s_j = r_j$ while

$$s_{j_0} = s_0 - \sum_{j \in X \setminus \{j_0\}} r_j \;.$$

We can also think here in terms of extended Blakley's scheme for the random polynomial $f = f(X_0, X_1, \ldots, X_{t-1}) = a_0 X_0 + a_1 X_1 + \cdots + a_{t-1} X_{t-1}$. We take the identities $\mathbf{x}_i = \mathbf{e}_i = \underbrace{(0, ..., 0, 1, 0, ..., 0)}_{i} \in \mathbb{F}_q^t$ for $i = 1, ..., t$ and secret $s = f((1, 1, \ldots, 1))$. This

gives the scheme corresponding to described and, as pointed in Remark 1.2.1, making public $s_1 = s_0 - s$ allows reconstruction of chosen $s_0$ by the privileged groups.

Now let $\Gamma = < B_1, ..., B_m >$ be any monotonic structure, where writing in this manner we understand sets $B_j$, $j = 1, ..., m$ as minimal that generate $\Gamma$ (i.e. for all $j = 1, ..., m$ any proper subset of $B_j$ is not in $\Gamma$, and $\Gamma$ is the family of supersets of $B_j$, $j = 1, ..., m$).

**Definition 1.3.1.** *Family of minimal sets that generate a monotonic structure $\Gamma$ is called basis of the structure $\Gamma$ and we denote it $\boldsymbol{B}$.*

For $\Gamma = < B_1, ..., B_m >$, for each basis element $B_j \in \Gamma$ we independently distribute additively the secret $s$, i.e.

$$s = \sum_{i \in B_j} s_i^{(j)} \ .$$

Finally the share of the $i - th$ entity is equal $s_i = \{s_i^{(j)}, j \in \{1, ..., m\} \ : \ i \in B_j\}$ i.e. each $B_j$ that $i$ is a member of contributes one $s_i^{(j)}$ to the $i - th$ share.

Formally, similarly as before, we can think here of $m$ multivariate polynomials $f_j(X_0, ..., X_{k_j-1})$ from extended Blakley's scheme, where $k_j = |B_j|$, which coefficients $a_{jk}$ for $k = 0, ..., k_j - 1$, are given to the members of $B_j$. We receive the corresponding scheme by making public $s - f_j((1, ..., 1))$ for $j = 1, ..., m$, which is the field element related to $B_j$.

**Second approach**

We show a method which for 'an input' being an anti-monotonic family of sets, constructs a sharing scheme (a way of distributing shares, parts of a secret, to the participants) such that sets of participants that can not reconstruct the secret, are exactly the sets from our anti-monotonic family. These sets can not decude any information about the secret. Other sets, from shares of their participants, are able to reconstruct the secret. The distribution of shares in this method is related to the family of maximal non-qualified sets in an anti-monotonic family. Such sets generate an anti-monotonic family.

Let $\Lambda = < A_1, ..., A_l >$ be anti-monotonic structure generated by maximal sets in $\Lambda$ (i.e. for any $i = 1, ..., l$ adding an element of $X \setminus A_i$ to $A_i$ creates a set that is not in $\Lambda$, moreover subsets of $A_i$ for all $i = 1, ..., l$ create $\Lambda$).

**Definition 1.3.2.** *Family of maximal sets that generate an anti-monotonic structure $\Lambda$ is called anti-basis of the structure $\Lambda$ and we denote it $\boldsymbol{N}$.*

For $\Lambda = <A_1, ..., A_l>$, we choose randomly $s_1, s_2, ..., s_l \in K$ such that $\sum s_j = s$ (formally, we can think of a multivariate polynomial). Now any participant $j \notin A_1$ obtains the value $s_1$, any $j \notin A_2$ obtains the value $s_2$, ... , any $j \notin A_l$ obtains the value $s_l$. We can see that, for all $j = 1, ..., l$, in a set $A_j$ the value $s_j$ is missing, hence this is really non-qualified set. Taking any set $S \notin \Lambda$, it is not contained in any of $A_1, ..., A_l$, so its participants have together all the shares $s_1, ..., s_k$. That means $S$ is privileged. We have constructed a sharing scheme $\Sigma$ for which $\Lambda = \Lambda(\Sigma)$.

Now we can write the following lemma, for the sake of terminology. It allows us to write only about basis or anti-basis sets, while considering an access structure, which was defined as a triple $(\Sigma, \Gamma, \Lambda)$.

**Lemma 1.3.1.** *One can determine access structure on $X$ with perfect sharing scheme by providing only a basis of the monotonic structure $\Gamma$ or by giving only an anti-basis of anti-monotonic structure $\Lambda$, then families of privileged and unprivileged sets are determined uniquely.*

**Proof**. While having basis it uniquely determines $\Gamma$. We can construct, as in the first approach, a perfect secret sharing scheme $\Sigma$ such that $\Gamma = \Gamma(\Sigma)$. Since the scheme is perfect we have

$$\Gamma(\Sigma) \cup \Lambda(\Sigma) = P(X) ,$$

where $P(X)$ is a family of all subsets of $X$. Since there is $\Gamma(\Sigma) \cap \Lambda(\Sigma) = \emptyset$ we can write $\Lambda(\Sigma) = X \setminus \Gamma(\Sigma)$ which is a corresponding family of unqualified sets. We have constructed an access structure $(\Sigma, \Gamma, \Lambda)$.

While having anti-basis it uniquely determines $\Lambda$. We can construct, as in the second approach, a perfect secret sharing scheme $\Sigma$ such that $\Lambda = \Lambda(\Sigma)$. Rest of the reasoning is similar as before.

$\square$

We have shown that for a given basis of $\Gamma$ (or anti-basis of $\Lambda$) there exists a perfect sharing scheme $\Sigma$ which determines the triple $(\Sigma, \Gamma, \Lambda)$ - an access structure. The construction is unique 'modulo perfect sharing schemes' since having same basis of $\Gamma$ (or anti-basis of $\Lambda$) one could use some other method of distributing a secret resulting in perfect sharing scheme $\Sigma'$ (for instance methods from first and second approach can be used dually since monotonic and anti-monotonic families are dual concepts), yielding

26

$\Gamma(\Sigma') = \Gamma$ and $\Lambda(\Sigma') = \Lambda$. In that case $(\Sigma', \Gamma, \Lambda)$ is the corresponding access structure. From now on, considering monotonic (or anti-monotonic structure), we also use terms privileged (or unprivileged sets), having in mind certain fixed access structure with perfect sharing scheme.

Instead of determining an access structure by giving a basis one can also as Benaloh and Leichter in [7] use a method with a logical formula consisting only of conjunctions and disjunctions (without negations).

**Definition 1.3.3.** *Monotonic logical formulae are formulae that consist only of conjunctions and disjunctions.*

Such formulae define monotonic structures in a way described in the following definition:

**Definition 1.3.4.** *For a monotonic logical formula $F$ with the variables indexed by the elements of a set $X$, the monotonic structure $\Gamma$ defined by $F$ is created by these subsets $S$ of $X$, for which $F$ is true when the variables indexed by $S$ have logical values one, and others are set to zero.*

For example for a formula $(a_1 \lor a_2) \land a_3$ we have $X = \{1, 2, 3\}$ and the family of base sets of access structure defined by this formula is $\{\{1, 3\}, \{2, 3\}\}$.

If we have the family of privileged sets $\Gamma$ implied by the logical formula $F$, we can also use the form of the formula (which could be nested) for the construction of sharing scheme related to the $\Gamma$-family. That kind of construction was proposed by Benaloh and Leichter in [7]. This subject is related to the considerations in the following chapter. We give there generalizations of sharing models proposed in this section. We will present facts and prove proper theorems to show the dependencies between the method of Benaloh and Leichter and our generalizations.

This ends the chapter of preliminaries.

# Chapter 2

# Encrypting monotonic access structures

First, we introduce broader definitions for basic concepts which will be further used.

Unprivileged (unqualified) sets will now be these sets of participants, that in 're-asonable' time are not able to reconstruct the secret (earlier they could not derive any information about the secret). Thus, now unprivileged sets in an access structure are these sets of participants that can not reconstruct a secret in practice, due to probabilistic, computational bounds. For instance, when $q$ is appropriately large and participants from a certain set know that any element from $\mathbb{F}_q$ is equally probable to be a secret, then as in previous meaning, they form an unprivileged set.

Sharing scheme on a set of participants $X$ is understood similarly as before, as a method of distributing a secret such that all elements from secrets domain are equally probable to be a secret, and there is a unique secret reconstructed by all participants from their shares.

Access structure is a triple $(\Sigma, \Gamma, \Lambda)$, where $\Lambda$ is an anti-monotonic family, being unprivileged sets in our meaning that we have just given, and $\Gamma = 2^X \setminus \Lambda$ is a family of sets that can reconstruct the secret.

In the literature, perfect sharing schemes are schemes (as we defined it in previous chapter) in which participants form sets that either can reconstruct the secret, or can not deduce any information about the secret. Now considered schemes, at least in general, are not perfect in that sense, since some subsets of participants in $\Lambda$ may have some partial information concerning the secret. However, looking at new definitions of $\Gamma$ and $\Lambda$, if in the scheme we consider they overlap the previous definitions, the scheme

will be perfect, since now there is always $\Gamma(\Sigma) \cup \Lambda(\Sigma) = 2^X$. For instance, perfect will be the scheme of Benaloh and Leichter (now, we consider it only over a large ring $\mathbb{Z}_q$).

By monotonic access structure we mean an access structure that is implied by giving any monotonic (or anti-monotonic) family of sets. As we have previously shown, any basis (or equivalently any monotonic family of sets) leads to an access structure with perfect sharing scheme. Similarly for an anti-basis and anti-monotonic structure. In this section we will consider some other methods of encrypting monotonic access structures, that is different ways of distributing a secret as shares to the participants. They may result in non-perfect schemes, which are secure accordingly to our introduced broader definitions.

We present ideas on the possibilities of sharing a secret in a monotonic access structure. That is, ideas related to sharing schemes in a monotonic family of sets. Shown are relations which occur between a method of encrypting a monotonic access structure using a family of sets, and a method based on a logical formula from [7].

We discuss the problem of security. There are included aspects of security of a hierarchy in the structure and our idea of hierarchy is being defined. This definition is new in the literature, not related to known hierarchical systems. We introduce the hierarchy in any general access structure. However, we do not concentrate on aspects related to the definition and treat it rather intuitively. We focus on practical aspects related to the possible corruption of entities by an adversary.

Methods of encrypting a monotonic access structure basing on a family of basis sets or a family of anti-basis sets are described generally. Discussed are aspects of using the method based on a logical formula. Any general access structure can be encrypted by each of those methods, however as it is shown, a specified method is chosen to achieve desirable level of security and appropriate time complexity.

## 2.1. Characterization of schemes

We briefly present a method of distributing a secret for a monotonic family given by a logical formula proposed by Benaloh and Leichter in [7]. Then we show our generalized method based on a family of basis sets or a family of anti-basis sets. Actually, it is based on family of anti-basis sets, but having a basis, there is a unique anti-basis by taking a complement of a family of monotonic sets in $2^X$. Then one gets anti-monotonic family and finds the anti-basis. Similarly the other way, uniqueness, starting from anti-basis.

As we have already mentioned, in our schemes we always consider these two, monotonic and anti-monotonic families, that sum up to the whole $2^X$. Next in our work considered here methods of distributing a secret are compared and shown are dependencies between them. We will also draw attention to their practical aspects.

A method of sharing a secret proposed in [7] uses a monotonic logical formula which could be nested. Having the formula, if $s$ is a secret value that is going to be shared, the distribution is done by getting into more and more detailed parts of the formula until we reach each participant. In particular, when there is a disjunction, all of its components receive the same part of actually distributed part of the secret. When there is a conjunction, performed is a random division of local part of the secret $s^{(l)}$ into the sum of $s^{(l)} = \sum_i s_i$ and each of the components related to participants in the conjunction receives $s_i$. In this method of distributing a secret it is possible to use threshold distribution, that is for disjunction use a threshold scheme with threshold 1 and for conjunction of $k$ components use a threshold scheme with threshold $k$. In that case we have in mind the following remark which could be important in some practical aspects of the scheme.

**Remark 2.1.1.** *In the process of reconstruction when using the threshold distribution, to solve the linear system the authority needs participants' identities which is not required for instance while using secure channels.*

As for example, we will distribute in $\mathbb{F}_q$ a secret $s \in \mathbb{F}_q$ to entities $\{1, 2, 3\}$ with a structure defined by the formula $(a_1 \wedge a_3) \vee (a_2 \wedge a_3)$.
Firstly, for the disjunction, $s$ is distributed to $a_1 \wedge a_3$ and to $a_2 \wedge a_3$. Now looking at $a_1 \wedge a_3$ there is random division of $s$ into two parts $s_1$, $s_2$ such that $s_1 + s_2 = s$ and parts $s_1$ is given to the entity 1 and $s_2$ to the entity 3. Similarly getting $s_3$ and $s_4$ such that $s_3 + s_4 = s$ there is then a distribution of them to entities 2 and 3 respectively.

Formula $((a_1 \vee a_2) \wedge a_3) \vee (a_1 \wedge (a_2 \vee a_3) \wedge a_4)$ defines an access structure, where firstly $s$ is distributed to both components of disjunction, then in the first component it is divided into appropriate $s_1$ and $s_2$ where $s_1$ is given to entities 1 and 2, $s_2$ to entity 3. Here instead of participating $s$ into two parts we could use a Shamir's scheme with threshold 2. In the second component of the formula $s$ is divided randomly into $s_3$, $s_4$ and $s_5$ which are distributed: $s_3$ to entity 1, $s_4$ to entities 2 and 3 and $s_5$ to entity 4. Here we could also use a Shamir's scheme, with threshold 3.

We notice that for the formula $(a_1 \vee a_2) \wedge (a_3 \vee a_4) \wedge \ldots \wedge (a_{2n-1} \vee a_{2n})$ each entity receives only one number, hence the related scheme is ideal.

Now, we would present our generalized method of creating a monotonic access structure from a family of basis sets or a family of anti-basis sets (one family is implied by the other). We use here a special, abstract function, satisfying certain set-theoretic conditions. Each of its realization results in a sharing scheme. We are interested in realizations for which implied scheme is secure. The distribution of shares is based on reasoning as in anti-monotonic based approach in Section 1.3.

Consider set of entities $X = \{P_1, \ldots, P_n\}$ and a monotonic family $\Gamma$. Assume a family of anti-basis sets of have a cardinality $k$, that is an anti-basis $\mathbf{N} = \{N_1, \ldots, N_k\}$. We can think of it as it is given and it determines the family of basis sets $\mathbf{B}$, or first there was a family of basis sets, which determined $\mathbf{N}$.

We distribute, with the use of special function $f$ subsets $S_i$ of $S = \{a_1, \ldots, a_k\}$ to the participants. It means that entity $P_i$ receives as his share the value $f(S_i)$. This value is a set, such that there is a requirement: function $f$ is chosen such that the following condition holds:

$$f\left(f(A) \cup f(B)\right) = f(A \cup B)$$

where $A = S_i \subseteq S$, $B = S_j \subseteq S$ are any subsets that would be related, with $f$, to shares of the participants $f(S_i)$, $f(S_j)$ respectively. Again, $S_i$ and $S_j$ are only related, meaning there is one to one correspondence, such that $S_i$ and $S_j$ are used to construct the shares $f(S_i)$ and $f(S_j)$. Participants do not need to know those sets (and as we would see often that is the case).

Notice that examples of functions for which this condition holds and could be taken for $f$ are identity on subsets of $S$ or $f$ being the least common multiple ($LCM$), when $S$ is a set of pairwise coprime numbers and least common multiple is understood as a function that takes on the input a set and returns the singleton consisting of an element being the least common multiple.

We notice that these kind of functions, satisfying our set-theoretic condition, 'forget the repeated terms in inputs' (see for instance when $f = LCM$) and can be used for sharing a secret, by giving to participants for shares the values of $f$ in certain chosen arguments i.e. chosen sets. We will show the details.

Value of $f$ in the sum of all sets used for the construction of shares is the secret that is going to be distributed among participants. In applications, for some functions $f$ and

for some monotonic structures, this value could be the secret, and reconstructing the secret, is finding that actual value. We call that kind of situation a 'method with plain set-theoretic approach' or simply 'Plain Set-Theoretic method'. For example, when the set of participants $X$ is not too large, for $f = LCM$, if our set $S$ satisfies the threshold condition, i.e. when all coprime numbers in $S$ are greater than certain, appropriately large threshold natural number $t \in \mathbb{N}$, security of the scheme, being a scheme on the natural numbers $\mathbb{N}$, is related to choosing appropriately large threshold constraint $t$.

Otherwise for final sharing scheme, we could moreover make use of some other constructions, as again for $f = LCM$, of based on Asmuth-Bloom sequence [1] construction that uses CRT-Ore algorithm [45]. It is then similar to regular Chinese Remainder Theorem based sharing scheme, but where participants have their CRT moduls such that only privileged sets are able, from their shares (constructed as in regular CRT scheme) to reconstruct the secret. The moduls for the participants forming an Asmuth-Bloom sequence could be chosen exactly with a method of distributing the shares with $f = LCM$ that we present. This specific application, i.e. application of least common multiply, was used by Pomykała while constructing general access structure based signature scheme, see Section 4.2.

Function $f$ is publicly known and security issues are dependent on the choice of the function. Reconstructing the secret is performed by taking values as in the left hand side of the equation that $f$ satisfies. Notice, for visualisation, that connecting $f(A \cup B)$ with a share $f(C)$ of a certain participant we compute $f\left(f(A \cup B) \cup f(C)\right) = f(A \cup B \cup C)$ and so on as we wanted for the process of reconstruction.

Distributing the shares to the participants is based on the second approach from Section 1.3. For each $N_i \in \mathbf{N}$, $i = 1, ..., k$ relate $a_i$ with every entity of $X$ except those which are in $N_i$. Hence, for $j = 1, ..., n$ some subset $S_j \subseteq S$ was related to a participant $P_j$. After computing the value $f(S_j)$ that value is given to the participant $P_j$ as his share. Participants from a selected privileged set $H \in \Gamma = 2^X \setminus < N_1, ..., N_k >$ can reconstruct the secret, since $H$ is not contained in any of $N_1, ..., N_k$. We have

$$f(\bigcup_{P_i \in H} f(S_i)) = f(\bigcup_{P_i \in H} S_i) \text{ , and } \bigcup_{P_i \in H} S_i \text{ is the whole set of distributed elements,}$$

(we sum up sets related to appropriate participants).

Since neither participant from a set $N_i \in \mathbf{N}$ has received $a_i$ it could be used to set up security conditions for sharing scheme that depends on the chosen $f$. Consider special

case with $f = LCM$ forming a scheme on the natural numbers $\mathbb{N}$, where the set $S$ satisfies a threshold condition of elements being larger than some fixed value.

## 2.2. Dependencies

The methods of determining a monotonic structure from a family of basis sets and determining it by a monotonic logical formula (as it was introduced at the end of Section 1.3) are related and any access structure can be defined using each of them.

**Theorem 2.2.1.** *Let $F$ be any monotonic logical formula defining a monotonic structure $\Gamma$. Converting $F$ into disjunctive normal form i.e. equivalent formula which is a disjunction of conjunction of the literals and making reductions of a type $(a \vee b) \wedge a \Leftrightarrow a$ such that there are no clauses contained as sets of literals in other clauses, sets made of indices of clauses define a basis of $\Gamma$.*

As an example, the formula $(a_1 \vee a_2) \wedge a_3$ is equivalent to $(a_1 \wedge a_3) \vee (a_2 \wedge a_3)$ and so we can read the basis $\{\{P_1, P_3\}, \{P_2, P_3\}\}$.

**Proof**. Let **B'** be a family of sets that were formed from the reduced disjunctive normal form, as described in the theorem. We will show that **B'** $=$ **B**, where **B** is the family of basis sets of $\Gamma$.

For any $B \in$ **B** setting variables indexed by elements of $B$ to 1 and others to 0 gives a value of $F$ equal to 1. Hence, we conclude that there exists $B' \in$ **B'** such that $B' \subseteq B$ and since sets from **B'** are also in the monotonic structure $\Gamma$ we have $B' = B$, which shows that **B** $\subseteq$ **B'**.

Now, we take any $B' \in$ **B'**. As we know, it is in the monotonic structure and we will show that it does not contain properly any set from $\Gamma$. However, this is true since **B'** is constructed from reduced formula. This shows that $B' \in$ **B**, hence **B'** $\subseteq$ **B**.

$\square$

Dual theorem for maximal unprivileged sets:

**Theorem 2.2.2.** *Let $F$ be any monotonic logical formula defining a monotonic structure $\Gamma$. Writing $F$ in a conjunctive normal form i.e. logical formula which is a conjunction of disjunction of the literals, that is reduced with $(a \wedge b) \vee a \Leftrightarrow a$ such that there are no clauses contained as sets of literals in other clauses, sets forming an anti-basis $\boldsymbol{N}$ are constructed by choosing a clause of the formula and extracting all indices omitting these indexing the chosen clause.*

As an example, the formula $(a_1 \lor a_2) \land (a_1 \lor a_3)$ implies anti-basis $\{\{P_3\}, \{P_2\}\}$.

**Proof**. Let $\mathbf{N'}$ be a family of sets constructed as stated in the theorem. We will show that $\mathbf{N'} = \mathbf{N}$, where $\mathbf{N}$ is the family of anti-basis sets of $\Lambda = 2^X \setminus \Gamma$.

Take any set $N' \in \mathbf{N'}$. Let $C$ be the clause selected for the construction of $N'$. Setting variables indexed by $N'$ to 1, and others to 0 gives a value of $F$ equal to 0 since clause $C$ takes the value 0. Any proper superset of $N'$ is in $\Gamma$ since it has a participant related to the variable in $C$, and any clause other than $C$ contains a variable that is not in $C$, becasue $F$ is reduced. That shows that $\mathbf{N'} \subseteq \mathbf{N}$.

Now, we take any $N \in \mathbf{N}$. The formula $F$ is false when setting all variables indexed by $N$ to 1 and others to 0. That means certain clause has to have value 0, so there are no variables indexed by $N$ in that clause. Because of $N$ being maximal all other indices apart of those indexing mentioned clause are in $N$ so $N$ is in $\mathbf{N'}$.

$\square$

We observe that having a basis $\mathbf{B}$ it is easy to construct a logical formula that defines the same monotonic structure, similarly for a family of maximal unprivileged subsets. These results indicate for instance, that after encoding the monotonic structure using one of considered methods it is possible to encode it using the other (with respect to computational constraints).

Sometimes it is much easier to give a monotonic structure using a logical formula. For example if we have a group of $n$ pairs of entities of the form $(2i - 1, 2i)$ for $i = 1, 2, \ldots, n$ and want to construct such structure, that for reconstruction of distributed value $s$ it is required at least one entity from each pair, then we can describe it shortly by a formula:

$$(a_1 \lor a_2) \land (a_3 \lor a_4) \land \quad \ldots \quad \land (a_{2n-1} \lor a_{2n})$$

The family of basis sets consists of $2^n$ elements. In each there is exactly one element of each pair. On the other hand, the description by the family of maximal unprivileged sets, which has $n$ elements, is simple again.

In the methods of distributing a secret in a monotonic access structure that were considered, the numbers from above are relevant. The number of basis sets, number of anti-basis sets (that directly imply the number of distributing elements in a method with abstract function) and, on the other hand, the number of nested parts from which the logical formula consists. They are associated with the time needed and practical

aspects in the distribution of shares. As we would see in further sections, it is significant in applications. We can also relate considerations on methods of describing monotonic structures to Section 2.4, where Trusted Authority, responsible for constructing the structure, chooses the way of giving the information about the structure to the public.

**Remark 2.2.1.** *While using logical formulae, shares have a strictly specified meaning, and in the process of reconstructing the secret one needs to use related to them information about the access structure. For instance, which of distributed elements that one has received, should one use, for various groups of entities, to reconstruct the secret. This extra information (as is presented in the two following sections) may be taken as an advantage by the third party. An adversary, having the information, gains knowledge about the access structure. We do not have that problem while using our abstract function based approach when the shares are of the form $f(S_i)$ and these whole sets take part in the reconstruction, as it was presented, without requirement of additional information.*

## 2.3. Idea of hierarchy in a general access structure

In the literature, there are ways of thinking about hierarchical access structure, see [10], [48], [52]. The definition from [27] that covers all the definitions considered so far is as follows:

**Definition 2.3.1.** *Let $\Gamma$ be a monotonic family of sets. We say that the participant $P_1 \in X$ is hierarchically superior to the participant $P_2 \in X$, if $A \cup \{P_1\} \in \Gamma$ for every subset $A \subseteq X \setminus \{P_1, P_2\}$ with $A \cup \{P_2\} \in \Gamma$. An access structure is said to be hierarchical if all participants are hierarchically related.*

Our approach is however different. It is more general in the sense that every access structure has hierarchy, and it is intuitive for many practical considerations. It comes from the observation that in every monotonic family we may try to point out the participants that are somehow more desirable, from adversary's point of view, to be corrupted. We make the following definition:

**Definition 2.3.2.** *The place of an entity in a hierarchy depends on the number of privileged subsets of $X$ which contain that entity, such that the participant $P_1 \in X$ is hierarchically superior to the participant $P_2 \in X$, if the cardinality of the family $\boldsymbol{F}_1 = \{A \in \Gamma : P_1 \in A\}$ is greater or equal to the cardinality of $\boldsymbol{F}_2 = \{A \in \Gamma : P_2 \in A\}$.*

We will concentrate on those aspects of constructing monotonic access structures that allow to hide the places that entities take in our definition of hierarchy. It is relevant especially in applications. From now on we assume, that while writing about hierarchy we think of it as it is in our definition.

Let us look from mentioned perspective at the sharing schemes.
Appropriate, as we will see, for hiding places of entities, would be our generic sharing scheme where the function $f$ is our Least Common Multiple (LCM), and for the set $S$ of distributed values related to entities, we take a subset of prime numbers or pairwise coprime numbers (it is a Plain Set-Theoretic method, as we called it). Thus, $f = LCM$ is the subject of our further investigations.

Security of the hierarchy in that case is based on the computational problem, that it is hard to determine how many distinct prime divisors or distinct coprime parts does a composite number have. It is considered to be comparatively difficult to the problem of factorization of a composite number which is a hard computational problem assumption. The prime or coprime parts that we are here considering, come from the process of distributing the shares. A share, as we will see, is the number that an adversary would want to know from how many parts it has been constructed.

Each entity $P_i$, intuitively is the more important in the hierarchy, the larger is his set $S_i$ of distributed numbers, related to his share (the smaller is the number of maximal unqualified sets that contain him). It is not always true that to entities higher in the hierarchy, related are larger sets $S_i$, as for instance in the situation with anti-basis $\mathbf{N} = \{\{P_1, P_2\}, \{P_3\}\}$. Here, $P_3$ is the highest in the hierarchy and each participant have one element in his related set. However, in many practical instances of general access structures it is true (look also at the Example 2.3.1).

Assume that an adversary knows the family of privileged sets in the access structure. Then, while gaining information about the position of certain entity in the hierarchy, which we assume for this access structure could be deduced from number of shares he has received, apart of knowing the position of the entity, he is able to plan further corruption to eventually reconstruct the secret. We want to prevent this circumstances.

Recall, we investigate a method with $f = LCM$. The share of $P_i$ is the least common multiple of elements of $S_i$, not the set $S_i$ itself. When distributing the prime numbers we have the problem of identifying how many distinct prime divisors does a composite number have. Distributing coprime parts instead of prime numbers is in that

case even better. In both cases we can modify sizes of eventually received shares by making some modifications in sizes of distributed elements that construct sets $S_i$. For security reasons one has to guarantee the adequate size of shares to prevent possible deductions of number of parts from which they are constructed, or comparisions of two gained shares. One has to guarantee that shares are not divisible by one another. It can be achieved by appropriate modification of the family of basis sets with the use of auxiliary entity that preserves the original family of qualified sets, as presented below.

We assume there is no entity that is able to reconstruct the secret by himself (which is a natural assumption while sharing a secret).

**Theorem 2.3.1.** *For a family of basis sets $\mathbf{B}$ of the monotonic access structure such that no entity can reconstruct the secret by himself, it can be guaranteed that subsets $S_i$ related to the entities, in a process of distributing the shares basing on approach with anti-basis, are not contained in one another.*

**Proof**. Let $\Gamma$ be the monotonic structure determined by the family of basis sets $\mathbf{B}$. Looking at the elements of sets from the family $\mathbf{B}$, if two entities $P_j$ and $P_k$ are both contained in a certain basis set, then their corresponding subsets $S_j$ and $S_k$ would not be contained in one another since in the family of maximal unprivileged sets $\mathbf{N}$ there would be a set that contains entity $P_j$ and does not contain the entity $P_k$, and the other set for which the opposite is true. On the other hand, if for entities $P_j$ and $P_k$ there is no basis set which contains that both entities, then by adding a new auxiliary entity $P_l$ to the set of entities we create a new privileged set of $\{P_j, P_k, P_l\}$. The family $\mathbf{B}$ with additional set forms a new basis, since the sets that previously were in $\mathbf{B}$ still do not contain, as proper subsets, basis elements. The only new sets in $\Gamma$ are those that contain the new basis set. All previous relations between entities has been preserved. The additional entity is only auxiliary. After performing described procedure for all such pairs of entities, a new basis $\mathbf{B'}$ is created. After receiving from $\mathbf{B'}$ the family of maximal unprivileged sets $\mathbf{N'}$ and distributing the shares, the condition from the theorem is fulfilled.

$\square$

**Example 2.3.1.**

Consider the set of entities $X = \{P_1, P_2, P_3, P_4\}$ and the family of basis sets
$\mathbf{B} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_4\}\}$.
It can be easily seen that related family of maximal unprivileged sets (anti-basis) is
$\mathbf{N} = \{\{P_1\}, \{P_2, P_4\}, \{P_3, P_4\}\}$.
The most privileged entity (the highest in the hierarchy) is $P_1$. He can reconstruct the secret cooperating with any other entity. Number of qualified subsets that contain $P_1$ is the largest (it is 7, while for $P_2$ and $P_3$ it is 6, for $P_4$ it is 5). The least privileged entity is $P_4$ since he can reconstruct the secret only with $P_1$. Number of qualified sets containing $P_4$ is smallest. In our sharing scheme with $P_1$ would be related two numbers, and with $P_4$ only one. In our approach we want to hide this dependency.

**Example 2.3.2.**

It can be noticed that in the setting from previous example after performing steps described in the proof of the Theorem 2.3.1, since pairs of entities $P_2$ and $P_4$, similarly $P_3$ and $P_4$ are not the elements of any basis sets, we receive the following sets:
$\mathbf{B'} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_4\}, \{P_2, P_4, P_5\}, \{P_3, P_4, P_5\}\}$
and related anti-basis
$\mathbf{N'} = \{\{P_1, P_5\}, \{P_2, P_4\}, \{P_2, P_5\}, \{P_3, P_4\}, \{P_3, P_5\}, \{P_4, P_5\}\}$,
where $P_5$ is the auxiliary entity. Now in the scheme with $f$ being $LCM$ after distribution of shares with respect to $\mathbf{N'}$, shares (as numbers) are not divisible by one another and if we forget about $P_5$ family of privileged sets remains unchanged.

## 2.4. Revealing information

We will pay here attention to applications of monotonic access structures. The considerations and possibilities can be examined during the phase of construction of structure, accordingly to the practical needs. We describe the settings for the Trusted Authority, who is the entity that constructs the monotonic access structure, to share the information about the structure with the participants. In relation to the previous section we include the practical aspects of security of the hierarchy. We consider here hierarchy of a monotonic access structure as it was previously introduced.

Apart of making the sets forming monotonic structure $\Gamma$ publicly available to everyone, there are the following possibilities for distributing information about $\Gamma$:

1) The information about the possible groups of entities that can reconstruct the secret is publicly available for every entity in the structure.

2) Every entity has the information only about the groups of participants with whom that entity is able to reconstruct the secret.

3) The information about the possible privileged groups is given to a certain trusted external entity and the participants obtain incomplete information about privileged groups that are constructed.

4) The information about the possible privileged groups is given to a certain trusted external entity and every participant receives incomplete information about the privileged groups that participant is an element of.

First method is the simplest. The information about the basis sets is publicly known by participants what makes it also the least secure. Adversary, after corrupting any entity, possess the whole information about the hierarchical structure in the access structure. This information, from practical point of view, helps him to choose the best for him 'path' of corruption (sequence of the participants to corrupt), which after being performed allows him to reconstruct the secret. For instance, let us look, in previous section, at the Example 2.3.1. Assume every entity is treated equally, that is everyone could be corrupted with the same probability. For example, every entity could be met in a place and circumstances favorable for corruption while moving randomly, everyone same frequent. The entity whom the adversary would like to corrupt in the first place is the highest in the hierarchy $P_1$, since corrupting any other entity allows him to reconstruct the secret. In a similar manner the less desirable in that sense is $P_4$.

In the second method, entity has only partial information about the hierarchy in the structure, hence strategies of an adversary after corrupting an entity are limited.

The third method uses an entity, who knows the whole family of basis sets. Entities even during the independent meetings (after the meeting a participant has the same information about the secret as he had before) with attempts to reconstructing the secret are not able to identify which privileged groups were formed (unless it is a meeting of such group and it reconstructs the secret). This method has also advantages

related to protection against the corruption of entities. Here, corrupted entities do not have the whole information about the other entities that should be corrupted to reconstruct the secret.

In the fourth method each entity has even less knowledge about the family of basis sets. Planning the corruption of entities in the structure is therefore more difficult.

The third and fourth methods made use of an additional, external entity. Corrupting this entity (if possible) reduces the situation to the situation in the first method. Introducing such entity, leads to the new possibilities in using such system, which may be interesting from the practical point of view. At some point of time, the additional entity may adjudge that it is required to reveal to certain group of entities the hidden information, that this group is able to reconstruct the secret.

# Chapter 3

# Multivariate extensions of sharing schemes

Shamir's $(t, n)$ threshold scheme is based on univariate polynomial of degree $t - 1$. Blakley's or extended Blakley's schemes, as was presented in Section 1.2, are based on multivariate polynomial of degree one. The natural question is the construction of sharing schemes based on multivariate polynomials. We propose an approach for constructing such schemes. We give a possible framework for the constructions of threshold scheme and show a construction of sharing scheme for general access structure. The approach gives a new theoretical perspective in general on polynomial based sharing schemes. It is based on generalized Chinese Remainder Theorem in multivariate polynomial ring and use methods of the theory of Gröbner bases. Shares of the participants in the scheme for general access structure are multivariate polynomials.

We note that here, during the exposition, we use a broader definition of an access structure, same as it was presented at the beginning of previous chapter. In particular, privileged sets of participants forming monotonic family $\Gamma$ are those sets that are able to reconstruct the secret. Unprivileged sets in $\Lambda$, on the other hand, are those sets that are not able to reconstruct it in 'reasonable' time due to probabilistic, computational bounds. Sharing scheme $\Sigma$ is a way of distributing the secret, as always. Thus, for a set of participants $X$, we have an access structure $(\Sigma, \Gamma, \Lambda)$ where $\Gamma \cup \Lambda = 2^X$. Since sharing scheme does not have to be perfect, we will see in the practical applications in this chapter, that one has to guarantee the indepednence of meetings of groups of participants. We mean here that even though unprivileged sets, in practice do not

reconstruct the secret, they can gain some information about it while attempting to reconstruct. A remedy for this is using in applications a third party, that performs the calculation on shares and returns if the secret was reconstructed or not. For example a secure device that solves generalized CRT problem (as we will further see), from shares that are sent by the participants.

It is possible to use multivariate polynomials of degree 1, as we did in our previous considerations, or greater than 1. That is the polynomials of the form

$$f = f(X_1, \ldots, X_l) = \sum a_{\alpha_1 \ldots \alpha_l} X_1^{\alpha_1} \ldots X_l^{\alpha_l}$$

find their applications related to access structures. As an example take a setting where for a chosen set of identities of the participants being vectors in $K^l$, one would like to check what groups of entities do exist. We can think of an environment where entities may disappear with certain probabilities, like transmitters that could be damaged. It may be possible to find the groups of entities as these able to reconstruct the secret similarly as in the setting of Proposition 1.2.1. Then we test different vectors $\mathbf{v}$ for possibility of group reconstruction, in that case if it is in a subspace spanned by set of vectors of identities. One can then take monic monomials in place of single variables in polynomial from extended Blakley's scheme, send monic monomials to participants (or the multivariate polynomial that is formed by taking their sum) and test reconstruction possibility in a similar manner, by searching for 'monomial vectors' that span a subspace containing $\mathbf{v}$ (for instance $X_1^2 + \ldots + X_l^2$ gives vector $(X_1^2, \ldots, X_l^2)$ which masks the difference between $(x_1, \ldots, x_l)$ and $(\pm x_1, \ldots, \pm x_l)$). One can test polynomial inequalities.

There exist ([30], [37]) propositions for public key cryptosystems that make use of the ring $R = K[X_1, \ldots, X_l]$ and Buchberger's algorithm for Gröbner bases computation ([5], [14], [29]). We however, having in mind our definitions, present approaches to the construction of secure sharing schemes related to that subject which use the generalized CRT algorithm from [4] being generalization of CRT algorithm for PID, as $K[X]$ in the univariate case.

## 3.1. Computational aspects of the ring $K[X_1, \ldots, X_l]$

We will give the preliminaries. When writing about monomials we would think about monic monomials. Considering computations in the ring of multivariate polynomials $R = K[X_1, \ldots, X_l]$ for our use, firstly we state the division theorem ([14], [5]) for a

total order on a set of monomials such that when $X^\alpha \leqslant X^\beta$ then $X^{\alpha+\gamma} \leqslant X^{\beta+\gamma}$, and it is always $X^\alpha \geqslant 1$. We mean here $X^\delta = X_1^{\delta_1}...X_l^{\delta_l}$, that is $\delta$ is a multi-index. In the literature this order is called admissible order, however we refer to it simply as monomial order, since we consider only that kind of order on monomials. Examples of monomial orders are degree lexicographic order or lexicographic order. Assuming axiom of choice, we can have a well order on a field $K$ such that 0 is the minimal element (of course we are usually working in finite fields). Thus, we can naturally extend a monomial order and consider a term order (a term understood as monomial multiplied by a coefficient). We notice that for a given polynomial $g$ leading term in $g$ is a leading monomial in $g$ multiplied by its coefficient.

**Theorem 3.1.1.** *For a given term ordering and a set of polynomials $\{f_1, ..., f_k\}$, every $f \in R$ can be written as*

$$f = a_1 f_1 + ... + a_k f_k + r \ ,$$

*where $a_i, r \in R$ and either $r = 0$ or $r$ is a $K-$linear combination of monomials, none of which is divisible by $lt(f_1), ..., lt(f_k)$, where $lt(f_i)$ is the leading term of $f_i$.*

This is known in the theory of Gröbner bases result. Its proof implies an algorithm for dividing a polynomial modulo certain set of polynomials with a given term ordering, which would be referred to as reducing the polynomial modulo given set. Gröbner bases are those sets of polynomials, divided modulo which, for any given polynomial there is exactly one remainder $r$ related to that polynomial.
From now we fix certain term ordering.

**Definition 3.1.1.** *Gröbner basis for an ideal $I$ of $R$ is a finite collection $G$ of generators of $I$ such that every nonzero $f \in I$ has leading term that is divisible by the leading term of some polynomial from $G$. We call a finite set of polynomials a Gröbner basis if it is a Gröbner basis of an ideal generated by this set.*

For a Gröbner basis $G = \{g_1, ..., g_k\}$ for $I$ there is then an equality of ideals

$$(lt(I)) = (lt(g_1), ..., lt(g_k)) \ ,$$

where $(lt(I))$ is the ideal generated by leading terms of polynomials from $I$.
It is easy to see the uniqueness of remainders modulo fixed Gröbner basis, since a monomial lies in a monomial ideal if and only if it is divided by one of monomial generators of the ideal. Thus, for a Gröbner basis $G = \{g_1, ..., g_k\}$, writing from division

theorem $f = \sum a_i g_i + r_1$ and $f = \sum a'_i g_i + r_2$, if $r_1 \neq r_2$ we have $r_1 - r_2 \in I$ so $lt(r_1 - r_2) \in (lt(I))$, hence one of the terms in $r_1$ or in $r_2$ is divisible by $lt(g_i)$ for some $i$, so there has to be uniqueness.

Similarly, we could notice that there is the following useful and known proposition:

**Proposition 3.1.1.** *If $G_1$ and $G_2$ are Gröbner bases for an ideal $I$ of $R$ then remainder from a reduction of any polynomial modulo $G_1$ is the same as remainder modulo $G_2$.*

The definition of reduced Gröbner basis is as follows:

**Definition 3.1.2.** *Gröbner basis $\{g_1, ..., g_k\}$ for an ideal $I$ of $R$ is called reduced if its elements are monic polynomials and if any term in $g_i$ is not divisible by $lt(g_j)$ for $j \neq i$.*

An ideal has a unique reduced Gröbner basis.

It is possible to algorithmically decide the membership of a polynomial in the ideal i.e. reduced form modulo Gröbner basis $G$ of $f$ equals 0 iff $f \in I$. It is possible to check the equality of the ideals by calculating reduced Gröbner bases and checking if they are the same. One can also algorithmically calculate ideals intersections or solve systems of multivariate polynomial equations.

Calculation of Gröbner basis depends on the ordering of monomials that one chooses and in general could be computationally expensive. However, both standard and reduced Gröbner bases are often computable in practice ([29]). In the setting when the Trusted Authority is choosing in precomputation phase the ideals for which the calculations would be executed, for instance when there is a given general access structure, as we will see in our proposal for a generalized sharing scheme, abovementioned methods could find their practical use. In our theory, in general, we could think of a black box providing for the participants such calculations related to Gröbner bases so that generalized CRT algorithm from [4] is fast. We will present the adequate constructions.

## 3.2. Theoretical framework for threshold scheme

We set up a theoretical, abstract framework for a $t$ threshold sharing scheme for $n$ participants having in its base multivariate polynomial interpolation. We show how to securely share a multivariate polynomial among $n$ participants such that $t$ or more of participants can reconstruct it. While considering an appropriately large base field $K$, less than $t$ participants would not be able to extract the chosen polynomial in practice,

since as we will see, there would be at least $|K|$ equally probable possibilities for the polynomial that is being reconstructed.

Assume that for $(t, n)$ there is a set of points $S \in K^l$ of cardinality $n$ and a class of polynomials $\mathcal{P} \subseteq R$, such that for any $t$ points from $S$, any $t$ values from $K^l$, there is a unique polynomial from $\mathcal{P}$ that on the chosen points takes the chosen values respectively.

We give a simple example of a setting in which our assumption can be fulfilled. However, the sharing schemes that are based on this setting overlap schemes already known in univariate case. We call that kind of settings trivial.

Assume the Trusted Authority succeeds in finding vectors for $S$ in the following situation ($S$ will be the set of identities in our scheme). For $\mathcal{P}$ take the polynomials of degree not greater than $m$ in $K[X_1, ..., X_l]$. There are $\binom{m+l}{m}$ possible monic monomials in a polynomial from $\mathcal{P}$, that is we can write it as a sum of $\binom{m+l}{m}$ terms:

$$f(X_1, \ldots, X_l) = \sum_{\alpha_1 + \ldots + \alpha_l \leqslant m} a_{\alpha_1 \ldots \alpha_l} X_1^{\alpha_1} \ldots X_l^{\alpha_l} .$$

By taking $t = \binom{m+l}{m}$ and $n \geqslant t$ the Trusted Authority in precomputation phase finds $n$ vectors from $K^l$ for elements of $S$ such that nonsingular are all of $\binom{n}{t}$ matrices, where each considered matrix has in a row all possible monic monomials in an argument being one of the $t$ chosen vectors.

Explicit examples of such vectors for identities that satisfie the conditions from above can be found. It is also possible to relate the problem of finding all the possible vectors for identities to searching for solutions of systems of multivariate polynomial equations. They arise from calculating discriminants of all $\binom{n}{t}$ matrices of values of monic monomials in vectors, assuming we are looking for vectors of the form $(x_{i1}, ..., x_{il})$, $i = 1, ..., n$. We want to find for each matrix, all the vectors that give zero discriminant, as these vectors that are not allowed. It is then related to Gröbner bases methods, for finding solutions of polynomial systems of equations. This in general, are however mostly theoretical considerations.

Now, having our assumption, we continue theoretical description of the sharing scheme. We can think of having abstract 'non-trivial' $\mathcal{P}$ and $S$, where for example $\mathcal{P}$ has more complicated structure than mentioned polynomials with a bound for the degree.

We randomly choose the multivariate polynomial $g \in \mathcal{P}$ assuming existence of the procedure allowing to choose every polynomial in $\mathcal{P}$ with the same probability. We give $i$-th participant the identity (identities are always public): a point $(c_{i1}, ..., c_{il}) \in S$. Then we give him a share $g(c_{i1}, ..., c_{il}) = r_i$. We treat $\mathcal{P}$ as publicly available. Because of our assumption, we see that every $t$ participants are related by their shares to the chosen polynomial $g$. We show a possibility to algorithmically reconstruct it with the algorithm from [4] that finds minimal CRT solution (being minimal can be an asset), instead of making attempts to solve linear system to find coefficients of the polynomial. Its degree may be a priori not known to the participants. Representing $g$ in the Theorem 3.1.1, taking a set of polynomials $\{X_1 - c_{i1}, ..., X_l - c_{il}\}$, we get that remainder is a constant, and so it is equal to $r_i$. Hence, a participant's share $r_i$ can be interpreted as the remainder from the publicly known ideal, meaning that the participant has $r_i + (X_1 - c_{i1}, ..., X_l - c_{il})$. By the generalized CRT algorithm from [4] that is based on the computation of Gröbner bases it is possible to find all the polynomials that exist which give chosen remainders by the ideals.

We state the appropriate theorem that originates from [4].

Fix any (admissible) monomial order on $R$ (so the term order is implied).

**Theorem 3.2.1.** *For ideals $I_1, ..., I_m$ of $R$ and polynomials $f_1, ..., f_m \in R$, sets intersection $\bigcap_{j=1}^m (f_j + I_j)$, if non-empty, is equal to $f' + \bigcap_{j=1}^m I_j$, where constructable $f' \in R$ is minimal in $\bigcap_{j=1}^m (f_j + I_j)$ with respect to quasi-order on polynomials in $R$ induced from term ordering in $R$. Moreover for any polynomial $g \in R$, its reduced form modulo certain constructable Gröbner basis is $f'$ if and only if $g \in \bigcap_{j=1}^m (f_j + I_j)$.*

**Remark 3.2.1.** *We can take quasi-order above as being induced from degree lexicographic order or induced from lexicographic order on monomials in $R$ (induced quasi-order is an ordering that comes from comparing leading terms, if equal, comparing 'next' leading terms and so on).*

**Remark 3.2.2.** *Constructions of constructable elements above can be done by algorithms in [4] (we could fix any monomial order on $K[X_1, ..., X_l] = K[\boldsymbol{X}]$ since in [4] for arbitrary monomial order $\leqslant_{\boldsymbol{X}}$ on $K[\boldsymbol{X}]$ and any monomial order $\leqslant_{\boldsymbol{Y}}$ on $K[\boldsymbol{Y}]$ we define $\leqslant$ on $K[\boldsymbol{X}, \boldsymbol{Y}]$ as $X^{\alpha_1} Y^{\beta_1} \leqslant X^{\alpha_2} Y^{\beta_2} \iff Y^{\beta_1} <_{\boldsymbol{Y}} Y^{\beta_2} \vee (Y^{\beta_1} = Y^{\beta_2} \wedge X^{\alpha_1} \leqslant_{\boldsymbol{X}} X^{\alpha_2})$.*

**Remark 3.2.3.** *Terminology: even though $f'$ clearly depends on a set of polynomials and a set of ideals, we write just $f'$ having in mind appropriate sets.*

Gröbner bases methods can be used to calculate the intersection of the ideals (in our situation, however, ideals are coprime, hence the intersection is the product of the ideals). They are also used in the CRT algorithm from [4] to calculate the reduced form $f'$, which added to the calculated intersection gives the appropriate set of polynomials, CRT solutions, that is

$$f' + \bigcap_i ((X_1 - c_{i1}), ..., (X_l - c_{il})) .$$

Looking at $t$ participants, they know that in their CRT-solution set, which is $f' + \bigcap_i^t ((X_1 - c_{i1}), ..., (X_l - c_{il}))$ (numbered without loss of generality) there is a unique element from $\mathcal{P}$. They also know that $f'$ is minimal in that set. If the knowledge of the form of every possible solution implied by the form of CRT-solutions, combined with the knowledge of $\mathcal{P}$ allows them to extract that element, they reconstructed the secret. Less than $t$ participants can not reconstruct the polynomial because for every of the remaining points, for any value from $K$, in $\mathcal{P}$ there is a polynomial that takes this value at that point while keeping the values received by participants in their points. From our assumption any of these polynomials could have been chosen from $\mathcal{P}$ with the same probability. It is then, with respect to the possible extraction of the solution by privileged sets, as in our broader definition of an access structure.

The scheme works for trivial settings and we now give two so called trivial examples (we will see why the name).

In the situation from our example of setting we called trivial: we have $\mathcal{P}$ as a class of multivariate polynomials of degree not greater than $m$ and $t = \binom{m+l}{m}$. Identities are found such that appropriate matrices (as it was in previous example) are nonsingular. Our assumption is then fulfilled. We fix degree lexicographic order. It induces quasi-order in $R$. The generalized CRT algorithm finds minimal polynomial and there is a unique polynomial of degree not greater than $m$ for $t$ given values. After randomly choosing $f \in \mathcal{P}$, accordingly to the scheme procedure, $t$ or more participants reconstruct as $f'$ the correct polynomial. It is since $deg(f') \leqslant deg(f)$ because $f$ is in CRT-solution set for every $t$ participants (we have $f(c_{i1}, ..., c_{il}) = r_i \iff f \in r_i + (X_1 - c_{i1}, ..., X_l - c_{il})$ so taking any $t$ participants $f \in \bigcap_{i=1}^t (r_i + (X_1 - c_{i1}, ..., X_l - c_{il}))$, with respect to the

numbering of $t$ participants, and $f'$ is also in this set so it takes the same values as $f$ on $t$ corresponding points). As we see, in that case, the participants could use the information about $\mathcal{P}$, that this is a set of polynomials of degree $\leqslant m$, to derive that one solution from the set $\mathcal{P}$, which appeared to be $f'$.

In this case, however, the reconstruction of polynomial $f$ from shares $r_i$ can be performed using the classical method of Gaussian elimination. We have vectors of identities of the form $(c_{i1}, ..., c_{il})$. We put them as arguments in all possible monomials of degree $\leqslant t$ forming a vector in the row of matrix. Using $r_i$, similarly as in the classical schemes, $t$ participants find a solution, which is a vector of coefficients of $f$. That is why we called this situation trivial.

Another, so called trivial example, comes from looking at randomly chosen univariate polynomial $f \in K[X]$ of degree not greater than $t - 1$, as in Shamir's scheme. Let $f(c_i) = r_i$ for $i = 1, ..., n$ be the shares of the participants. Hence, participants have $r_i + (X - c_i)$. Our scheme gives an algorithm for finding Shamir's polynomial. Here $\mathcal{P}$ is the class of all polynomials of degree not greater than $t - 1$ and set of identities $S$ is a subset of $K$ of cardinality $n$. The generalized CRT algorithm for $t$ participants gives CRT-solution set $f' + \bigcap_{i=1}^{t}(X - c_i)$ which is equal to

$$f' + (\prod_{i=1}^{t}(X - c_i))$$

and since Shamir's polynomial $f$ is of degree not greater than $t - 1$ it has to be $f'$.

We can, in similar terms, construct a sharing scheme that is not based on our theoretical framework. In the case of $n = t$, in $(t, t)$ threshold scheme we can share multivariate polynomial as in the following construction:
Participant's identities would be vectors of the form $\mathbf{c} = (c_{j1}, ..., c_{jl})$ for $j = 1, ..., t$. Now we do not need a uniqueness condition:

Assume that all $t$ vectors of identities are such that for any $t$ values there is a polynomial in $K[X_1, ..., X_l]$ that in chosen vectors takes those values respectively. The existence of such a polynomial can be guaranteed by the following procedure: Trusted Authority chooses a set of $t$ vectors for identities:

For a fixed set of identities Trusted Authority by Gaussian elimination proceeds as follows: he chooses multivariate polynomial by writing a sum $\sum X_1^{\alpha_1}...X_l^{\alpha_l}$ of ap-

propriately many chosen monomials to check, if independent are monomial-id-rows of matrix, that is rows having all chosen monomials, that take their values in vectors of identities (every row is related to one vector of identity as the argument). The procedure of choosing monomials may be randomized or some adequate to chosen identities. If he succeeds in an appropriate for him time, he proceeds further. If not he chooses different set of identities. If he succeeds we denote the multivariate polynomial being the sum that he found by $f$ and by $\mathbf{f}$ the vector of monomials that form the sum. Let $k$ be the number of terms in $f$, so also it is the length of $\mathbf{f}$. Let $M$ be related matrix formed by monomial-id-rows in the identities that were found. Let $\mathbf{a}$ denote a vector of length $k$ (it would be vector of coefficients related to $f$).

For example set $\{(i, ..., i) : i \in \{1, ..., t\}\}$ is always good to be the set of identities in the procedure, because of Shamir's univariate polynomial. Trusted Authority could in that case take for instance $\sum_{i=0}^{t-1} X_1^i$. We allow more general situations. We also notice that Trusted Authority could firstly start from sum of monomials and then search for vectors of identities.

In practice, assuming the Trusted Authority found vectors of identities as above, it gives the following secure scheme with an interesting property.
The Trusted Authority randomly chooses $r_j \in K$, $j = 1, ..., t$ and distributes as shares to the participants. We look at $r_j + I_j$, $j = 1, ..., t$, where $I_j = (X_1 - c_{j1}, ..., X_l - c_{jl})$ is an ideal in $R$ which is public (i.e. $(c_{j1}, ..., c_{jl})$ is a vector of identity) related to the $j$-th participant. From the construction of the Trusted Authority in preliminary phase, we know that there is at least one element in sets intersection $\bigcap_{j=1}^{t}(r_j + I_j)$. It is since $M\mathbf{a} = \mathbf{r}$ has a solution in $\mathbf{a}$, where $\mathbf{r} = (r_1, ..., r_t)$, so that element in the sets intersection could be $g = \mathbf{f} \cdot \mathbf{a}$, because the element $g$ satisfies $g(c_{j1}, ..., c_{jl}) = r_j$, $j = 1, ..., t$, and $g(c_{j1}, ..., c_{jl}) = r_j \Leftrightarrow g \in r_j + I_j$, since writing from Theorem 3.1.1 $g = \sum_{i=1}^{l} a_i(X_i - c_{ji}) + r$ we get that $r$ is constant and so, equal to $r_j$. We know from Theorem 3.2.1 that one can calculate $f'$ which is minimal in $\bigcap_{j=1}^{t}(r_j + I_j)$ with respect to quasi-order on polynomials induced from monomial ordering which can be chosen. Trusted Authority chooses the monomial ordering, calculates $f'$ with generalized CRT algorithm and treats $f'$ as a secret polynomial to be reconstructed. He publishes term ordering that was chosen.

All $t$ participants, knowing $r_j$ and $I_j$ for $j = 1, ..., t$, can reconstruct $f'$ from generalized CRT, as it was done by the Trusted Authority.

Less than $t$ participants, say having shares $r_1, ..., r_{t-1}$, can not find $f'$ since for every

possible $r_t$ that could have been randomly chosen, there is one corresponding $f'$ such that $f'(c_{t1}, ..., c_{tl}) = r_t$, which gives a one to one relation. It is what we wanted to show to have an access structure.

**Remark 3.2.4.** *Notice that the participants do not know a priori the degree of $f'$.*

At the end we comment that one can construct a simple ideal $(t, n)$ threshold scheme, which makes use of a multivariate polynomial. It is only an extension of the well known linear constructions. We proceed as follows:

Using the notation from above, Trusted Authority finds as previously $k = t$ monomials forming a vector $\mathbf{f}$, and vectors of identities for $n$ participants, such that any set of $t$ vectors forms a non-singular, related monomial-id matrix (rows are monomial-id-rows related to those $t$ vectors). Then he publishes a vector $\mathbf{f}$. Trusted Authority randomly chooses a vector of coefficients $\mathbf{a}$. Knowing $g = \mathbf{a} \cdot \mathbf{f}$ he distributes the shares as values of $g$ in vectors of identities. Then he chooses a vector $\mathbf{u}$ such that $\mathbf{f}(\mathbf{u})$ is not in any subspace spanned by $t - 1$ monomial-id-rows (equivalently a matrix having these $t - 1$ monomial-id-rows and additional row of $\mathbf{f}(\mathbf{u})$ is nonsingular). The scheme, where $g(\mathbf{u})$ is the secret and $\mathbf{u}$ is publicly given (so $\mathbf{f}(\mathbf{u})$ is public), is then secure, where the proof is as of Proposition 1.2.1. Since, we recall, in a scheme where $\mathbf{x}_i$ is a vector known by $i$-th participant, having a publicly known vector $\mathbf{v}$ and a secret $\mathbf{v} \cdot \mathbf{a}$ for some random vector $\mathbf{a}$, if $\mathbf{x}_i \cdot \mathbf{a} = s_i$ are shares, then participants from certain set can reconstruct from their shares $\mathbf{v} \cdot \mathbf{a}$ iff vectors $\mathbf{x}_i$ that are known to participants of this set span a subspace which contains $\mathbf{v}$. Comparing to extended Blakley's scheme, the case here is that all vectors of identities form related rows of matrices with a use of $\mathbf{f}$. These monomial-id-rows are vectors $\mathbf{x}_i$ from above, and vector $\mathbf{v} = f(\mathbf{u})$.

**Remark 3.2.5.** *Looking at the number of variables the Trusted Authority used while constructing $\boldsymbol{f}$ we notice that a vector of identity of (general) length $l$ is related to a row of matrix of the length $t$.*

## 3.3. Proposition for generalized secret sharing

For the generalized secret sharing, we present the considerations, where proposed is a scheme for a general access structure, to securely reconstruct a multivariate polynomial, or securely reconstruct a value at publicly known point.

In the setting, the share of each participant is a polynomial $f_j$, where $f_j$ is reduced form modulo Gröbner basis for an ideal $I_j$ of certain chosen polynomial $f$. Publicly known ideals $I_j$ assigned each to participant are such that there is a distinguished ideal $I$ that is a proper subset of $I_j$ for every $j$. What is more $\bigcap I_j = I$ whenever intersected are ideals of participants from the privileged group. The set of all general CRT solutions of privileged set would be $f' + I$ for certain constructable polynomial $f'$. We can take $f(a)$ as the secret for certain element $a \in K$ that would be given. Ideals $I_j$ assigned to the participants are constructed as in the following approach.

For certain monotonic family $\Gamma$ and related to it, family of maximal unprivileged sets proceed as follows, as in Section 1.3 in anti-monotonic family based approach. Distribute appropriately large set of non-associated irreducible polynomials $g_1, ..., g_k$, that would form the generators of $I$, to the participants such that privileged sets of participants have all the polynomials $g_j$ for $j = 1, ..., k$ and participants of an unprivileged set do not have certain polynomial (at least one) related to that set. The set $\{g_{\sigma_1}, ..., g_{\sigma_s}\}$ related to the participant in a process of distribution forms an ideal $I_m = (g_{\sigma_1}...g_{\sigma_s})$ which is assigned to the participant. Polynomials $g_1, ..., g_k$ can be publicly known. Since $R$ is unique factorization domain every irreducible element is prime and we have

$$I_m = (g_{\sigma_1}...g_{\sigma_s}) = (g_{\sigma_1}) \cap ... \cap (g_{\sigma_s}).$$

Now any subset of participants, from their shares can calculate $f' + \bigcap I_j$ knowing that one of the representatives is $f$. Privileged sets can calculate $f' + I$. We can take

$$f = f_0 + \sum_{1 \leqslant i_1 < ... < i_{k-1} \leqslant k} c_{i_1...i_{k-1}} g_{i_1}...g_{i_{k-1}} \ ,$$

where $deg(f_0) < deg(g_1...g_k)$ (or just $f_0 = 0$) and constants $c_{i_1...i_{k-1}}$ are chosen at random with respect to uniform distribution on $K$.

Assume that we took such polynomial $f$. In this case we work with the degree lexicographic order, hence the quasi-order on polynomials in $R$ is induced from it. We use Theorem 3.2.1.

The participants of a privileged set have the information that $f \in f' + I$, that is $f = f' + hg_1...g_k$ for certain $h \in R$ and $f'$ is minimal in $f' + I$ with respect to quasi-order, hence in particular $deg(f') \leqslant deg(f)$. Writing $f - f' = hg_1...g_k$, since the degree of $f - f'$, gives $h = 0$ and the polynomial $f'$ calculated by the privileged set is $f$.

On the other hand, looking at an unqualified set, every of its participants does not

have a polynomial, without loss of generality say $g_k$ in the product that generates his related ideal $I_j$. Hence, having as his share $f$ reduced modulo Gröbner basis for $I_j$ he has no information about $c_{1...k-1}$ since for any constant $c$ both $f$ and $f_c = f + cg_1...g_{k-1}$ give the same reduced forms modulo $I_j$ (uniqueness of remainder modulo Gröbner basis in Theorem 3.1.1). Hence, for these participants equally $f$ and $f_c$ could be chosen as the secret polynomial, which is what we wanted to show. Looking at field $K$, if the Trusted Authority ensures that for $a \in K$ that he chooses there is $g_i(a) \neq 0$ for all $i = 1, ..., k$, then as in our case $cg_1(a)...g_{k-1}(a)$ could be any element of $K$ with same probability so unqualified set of participants does not have any information about $f(a)$.

**Remark 3.3.1.** *We have an advantage, which is that when participants have as their secret shares nonconstant polynomials, the Trusted Authority who was responsible for constructing the shares and securely sent them to the participants, is also able to secretly give information to the participants. For that he, knowing the polynomial of specific participant, chooses the point for that participant and announces it. The participant can read the information by calculating at that point the value of the polynomial.*

**Remark 3.3.2.** *Notice, while having publicly known ideals of the participants in the access structure, everyone can encrypt a polynomial of the described form by calculating appropriate reduced forms and sending them respectively to participants. Accordingly to our (broader) definition of an access structure, the privileged sets in the structure are able to reconstruct it, and unprivileged are not.*

**Remark 3.3.3.** *After an entity sent an encoded polynomial as shares in the group, he is able to choose the values for $a$ related to the secret value $f(a)$. That gives another method for the dynamism of the secret itself when the shares were already given (another way is to announce $s_0 - f(a)$ for some chosen $s_0$).*

We comment that considerations in Section 1.3 also imply a basic secure scheme for sharing a single polynomial in a general access structure, where shares are sets of polynomials. For that take a polynomial $f = f_1 + ... + f_k$ as the secret, where $f_i$ for $i = 1, ..., k$ are randomly chosen polynomials appropriately distributed among the participants as in the approach based on anti-monotonic structure ($k$ is an appropriate number of elements to be distributed). Then the entities in a privileged set have all the shares, that is the set $\{f_1, ..., f_k\}$, and participants from given unprivileged set do not have certain polynomial $f_s$ for $s \in \{1, ..., k\}$. This simple method is obviously secure.

We will give an example of our construction for already considered monotonic structure from Example 2.3.1.

**Example 3.3.1.**

Let the set of entities $X = \{P_1, P_2, P_3, P_4\}$ and the family of basis sets
$\mathbf{B} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_4\}\}$.
The related anti-basis is
$\mathbf{N} = \{\{P_1\}, \{P_2, P_4\}, \{P_3, P_4\}\}$.
Let $N_1 = \{P_1\}$, $N_2 = \{P_2, P_4\}$, $N_3 = \{P_3, P_4\}$.
We will share a multivariate polynomial from $\mathbb{F}_q[X_1, ..., X_l]$.
First we construct public ideals for participants with a method based on approach with anti-basis:
We choose $g_1, g_2, g_3$, non-associated irreducible polynomials (3 since $|\mathbf{N}| = 3$). Accordingly to the method of distribution, we give $g_1$ to every participant except those in $N_1$, then $g_2$ to everyone except the participants in $N_2$, then $g_3$ to everyone except those who are in $N_3$. After all:
$P_1$ receives the set $\{g_2, g_3\}$ and his related ideal is $I_1 = (g_2 g_3) = (g_2) \cap (g_3)$,
$P_2$ receives the set $\{g_1, g_3\}$ and his related ideal is $I_2 = (g_1 g_3) = (g_1) \cap (g_3)$,
$P_3$ receives the set $\{g_1, g_2\}$ and his related ideal is $I_3 = (g_1 g_2) = (g_1) \cap (g_2)$,
$P_4$ receives the set $\{g_1\}$ and his related ideal is $I_4 = (g_1)$.
Let $I = (g_1 g_2 g_3)$.
We choose a polynomial that we want to share, it has a form

$$f = f_0 + c_1 g_1 g_2 + c_2 g_1 g_3 + c_3 g_2 g_3,$$

where $c_i$, $i = 1, 2, 3$ are chosen randomly from $\mathbb{F}_q$, and $f_0$ is any polynomial we like, that has degree less than $deg(g_1 g_2 g_3)$. We choose $a \in \mathbb{F}_q$ such that $g_i(a) \neq 0$, $i = 1, 2, 3$ and make it public.
Shares:
We find $f_j$ which is a reduced form of $f$ modulo Gröbner basis of $I_j$ and give $f_j$ to participant $P_j$ as a share, for $j = 1, 2, 3, 4$.
That means $f_j$ is a remainder in the division theorem, i.e. Theorem 3.1.1 for $f$ modulo Gröbner basis of $I_j$. Our situation is simple since $I_j$ is principal and its generator

is a Gröbner basis for $I_j$ (it is easy to show, since if $J = (h)$ we get the equality $(lt((h))) = (lt(h))$ as was required for $h$ to be a Gröbner basis).

Take

$$h_1 = g_2g_3, \ h_2 = g_1g_3, \ h_3 = g_1g_2, \ h_4 = g_1 \ .$$

We have $I_j = (h_j)$, $j = 1, ..., 4$.

Writing from the Theorem 3.1.1

$$f = a_jh_j + f_j \ .$$

The polynomial $f_j$ is the share of participant $I_j$.

We show that participants from sets of $\mathbf{B}$, from their shares, can reconstruct $f$.

Let us look for example at the participants $P_1$ and $P_2$.

There is

$$I_1 \cap I_2 = (g_2) \cap (g_3) \cap (g_1) \cap (g_3) = (g_1) \cap (g_2) \cap (g_3) = (g_1g_2g_3) = I \ .$$

In the Theorem 3.2.1 we fix monomial order as degree lexicographic. Then quasi-order on polynomials is induced from it.

Next in the Theorem 3.2.1, for the ideals $I_1$ and $I_2$ and set of polynomials $f_1$, $f_2$, we have that set $(f_1 + I_1) \cap (f_2 + I_2)$ is non-empty because $f$ is in the intersection (it can be seen where we wrote $f$ from Theorem 3.1.1).

We find $f'$ with generalized CRT algorithm. We know that

$$f' + I_1 \cap I_2 = (f_1 + I_1) \cap (f_2 + I_2) \ .$$

So $f' + I = (f_1 + I_1) \cap (f_2 + I_2)$. We know about $f'$ that it is minimal in $(f_1 + I_1) \cap (f_2 + I_2)$. Since $f$ is also an element of that set, it means that $f'$ is smaller than $f$ with respect to quasi-order induced by degree lexicographic order on monomials. That implies $deg(f') \leqslant deg(f)$. Our $f$ was chosen such that $deg(f) < deg(g_1g_2g_3)$.

Thus, we also have, $deg(f - f') < deg(g_1g_2g_3)$.

Since $f \in f' + I$ we can write $f = f' + hg_1g_2g_3$. Then $f - f' = hg_1g_2g_3$. So $h = 0$ and $f' = f$, they reconstructed $f$. They can read $f(a)$. For other sets in $\mathbf{B}$ it is similar.

We will show that participants of an unprivileged set can not reconstruct $f$.

We take for example $N_3 = \{P_2, P_4\}$.

Both $P_2$ and $P_4$ haven't received $g_2$ and their ideals $I_2 = (g_1 g_3)$ and $I_4 = (g_1)$.

From their shares $f_2$ and $f_4$, they know nothing about the part $c_2 g_1 g_3$ that is in

$$f = f_0 + c_1 g_1 g_2 + c_2 g_1 g_3 + c_3 g_2 g_3.$$

It is because $f_c = f + c g_1 g_3$ would give them the same shares, if chosen (that is if there was chosen different coefficient of $g_1 g_3$ in $f$). It is so, since $g_1 g_3$ is both in $I_2$ and $I_4$.

We show that for example for the participant $P_4$:

We know that $f_4$ is reduced form of $f$ modulo $I_4$, that is $f = a_4 g_1 + f_4$.

Then,

$$f_c = f + c g_1 g_3 = a_4 g_1 + f_4 + c g_1 g_3 = g_1 (a_4 + c g_3) + f_4 .$$

From the uniqueness of remainder in Theorem 3.1.1 for set being Gröbner basis, we have that $f_4$ is also reduced form of $f_c$ modulo $I_4$ (it was before, so we know that it is either 0 or is not divided by leading terms of polynomials in Gröbner basis).

Similarly for participant $P_2$ we get that $f_2$ is reduced form of $f_c$.

That means participants $P_2$ and $P_4$ can not determine randomly chosen part $c_2 g_1 g_3$ in $f$ because they do not have any information about it (if one has chosen different coefficients of $g_1 g_3$ in $f$ then $P_2$, $P_4$ would still have the same shares).

From that reason, since $g_1(a) g_3(a) \neq 0$, they can not determine the value $f(a)$ as well.

In practice, for sharing scheme in a general access structure we could use a third party, as it was said in the beginning of this chapter, so that the meetings of the participants are independent.

# Chapter 4

# Pairing based constructions for general access structures

At the beginning we will introduce notation and elementary concepts. Then we will move to applications based on bilinear pairing for general access structures. Our constructions result in general access structure based signature schemes, that are based on a framework used also by Pomykała, while considering signature scheme using generalized Asmuth-Bloom sequence and CRT-Ore algorithm. We include presentation of this method. In our designs we show that other methods of encrypting monotonic access structure considered in the thesis can be used for the signature scheme. To encrypt a monotonic access structure in the proposal for signature schemes we use the following methods:
- method based on generalized Asmuth-Bloom sequence which uses CRT-Ore algorithm
- method based on extended Blakley's scheme, originating in considerations of Brickell
- method based on logical formulae introduced by Benaloh and Leichter
- method based on plain set-theoretic approach that we have introduced in the thesis. The considerations are meant to be treated as a theoretical proposal.

We remark that considerations presented while designing signature schemes can be applied to the construction of general access structure based group decryption schemes.

The base for the presented constructions are the properties of bilinear pairing on elliptic curve over finite field. In the preliminary section we introduce background for further applications.

## 4.1. Elliptic curves and bilinear pairings

Firstly, we give the preliminaries. Let $K$ be a field, $\overline{K}$ its algebraic closure. An elliptic curve $E$ over $K$ is a smooth projective plane cubic curve with a distinguished point called the point at infinity, denoted by $\mathcal{O}$. It is given, up to a birational transformation, by a non-singular Weierstrass equation

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3 \ .$$

After de-homogenisation we have an affine Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ .$$

If the field characteristics is different from 2 and 3 Weierstrass equation is isomorphic over $K$ to $y^2 z = x^3 + a_4 xz^2 + a_6 z^3$ (a commonly considered affine version of which is $y^2 = x^3 + a_4 x + a_6$) and non-singularity condition is equivalent to $4a_4^3 + 27a_6^2 \neq 0$ in $K$.

If $L$ is any field extension of $K$, by $E(L)$ we denote the set of $L$-rational points of $E$. Together with $\mathcal{O}$ these points form an abelian group, where $\mathcal{O}$ is its identity element. The group of $n$-torsion points of an elliptic curve is $E[n] = \{P \in E(\overline{K}) \mid nP = \mathcal{O}\}$. We also denote $E(K)[n] = \{P \in E(K) \mid nP = \mathcal{O}\}$. By $\mu_n = \{x \in \overline{K} \mid x^n = 1\}$ we denote the group of $n$-th roots of unity in $\overline{K}$. In our considerations we will be interested in curves defined over a finite field of $q$ elements: $\mathbb{F}_q$, and its extensions in a fixed algebraic closure $\overline{\mathbb{F}}_q$.

We present applications for general access structures that are based on bilinear pairings on elliptic curves. In general (as in [31]), for an abelian additive $n$-torsion groups $G_1 = (G_1, +, 0)$ and $G_2 = (G_2, +, 0)$, and a multiplicative group $G_3 = (G_3, \cdot, 1)$, pairing is a mapping

$$e : \ G_1 \times G_2 \to G_3 \ .$$

In our considerations pairings have the following, standard properties:
Bilinearity: For any $P, P' \in G_1$ and any $Q, Q' \in G_2$

$$e(P + P', Q) = e(P, Q)e(P', Q) \text{ and } e(P, Q + Q') = e(P, Q)e(P, Q').$$

Non-degeneracy: For any nonzero $P \in G_1$ there is $Q \in G_2$ such that $e(P, Q) \neq 1$, and also for any nonzero $Q \in G_2$ there is $P \in G_1$ such that $e(P, Q) \neq 1$.

On elliptic curves over finite fields there are two pairings most often considered, the Weil pairing and the Tate-Lichtenbaum pairing. Let $E$ be elliptic curve over $\mathbb{F}_q$. The Weil pairing is a non-degenerate bilinear map:

$$e_n : \; E[n] \times E[n] \to \mu_n \; ,$$

where $n$ is coprime to characteristics of the field over which we consider our curve $E$. The Tate-Lichtenbaum pairing on the other hand is a non-degenerate bilinear map:

$$t_n : \; E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n \; ,$$

where $gcd(n,q) = 1$ , $n \mid \#E(\mathbb{F}_q)$ and $k$ is the embedding degree of $E$ with respect to $q$ and $n$, i.e. the order of $q$ in $\mathbb{Z}_n^*$.

For references related to pairings, one could for example see [31], [33].

In our applications we assume having a setting when pairing $e$ is efficiently computable, which means that there exist an efficient algorithm to compute $e(P,Q)$ for any $P \in G_1$, $Q \in G_2$. Weil pairing and Tate-Lichtenbaum pairing could be efficiently computed with Miller's algorithm [42]. We also assume that the discrete logarithm problems are hard in $G_1$ and $G_2$ and that we are working in a Gap Diffie-Hellman group. We give a notation that is used. Let $G$ be a cyclic additive group of prime order $p$ generated by $P$ and let $a, b, c \in \mathbb{Z}_p$.

**Definition 4.1.1.** *Discrete Logarithm Problem - DLP: Given $P, Q \in G$ find, if exists, an integer $k$ such that $Q = kP$.*

**Definition 4.1.2.** *Computational Diffie-Hellman Problem - CDHP: Given a triple $(P, aP, bP)$ find the element $abP$*

**Definition 4.1.3.** *Decision Diffie-Hellman Problem - DDHP: Given a quadruple $(P, aP, bP, cP)$ decide whether $c = ab$ (mod p).*

**Definition 4.1.4.** *Gap Diffie-Hellman Problems - GDHP: A class of problems where CDHP is hard but DDHP is easy. We call the related group the GDH group.*

Being easy here means that DDHP can be solved in polynomial time, but there is no probabilistic algorithm that can solve CDHP with non-negligible advantage within polynomial time (see also [43], [13], [16]).

Having a bilinear pairing $e$ that for a point $P \in G$ is such that $e(P, P)$ has order $p$, one can solve DDHP by calculating $e(aP, bP)$ and comparing it to $e(P, cP)$, where $(P, aP, bP, cP)$ is a quadruple to be tested. This is often the case, however not for Weil pairing, where for all points $P \in E[n]$ there is $e_n(P, P) = 1$. Tate-Lichtenbaum pairing in cryptography is used more often. However it goes into quotient group and we would rather have specified values instead of cosets. This is resolved by introducing modified (also called reduced) Tate-Lichtenbaum pairing $\tau_n$. We shortly show the idea behind. For embedding degree $k$, there is $\mu_n \subseteq \mathbb{F}_{q^k}^*$. Since $\mathbb{F}_{q^k}^*$ is a cyclic group of order $q^k - 1$, we have a homomorphism defined by taking the power of $(q^k - 1)/n$:

$$\mathbb{F}_{q^k}^* / (\mathbb{F}_{q^k}^*)^n \to \mu_n$$

It is an isomorphism if we known that field extension $\mathbb{F}_q(\mu_n) = \mathbb{F}_{q^k}$, i.e. when $\mathbb{F}_q(\mu_n)$ is not a proper subfield of $\mathbb{F}_{q^k}$. This is fulfilled for example for embedding degree 1. Hence, we define modified (reduced) Tate-Lichtenbaum pairing as:

$$\tau_n = t_n^{(q^k-1)/n} \ .$$

What is more, first isomorphism theorem gives that $E(\mathbb{F}_{q^k})[n]$ has the same cardinality as $E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k})$. Then, for $n = \ell$ being prime number, if in $E(\mathbb{F}_{q^k})$ there are no points of order $\ell^2$, since being isomorphic, we can represent $E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$ as $E(\mathbb{F}_{q^k})[\ell]$ and treat modified Tate-Lichtenbaum pairing similarly as Weil pairing, that is:

$$\tau_\ell : \ E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})[\ell] \to \mu_\ell$$

We also state here related theorem of Balasubramanian and Koblitz [2]:

**Theorem 4.1.1.** *Let $E$ be an elliptic curve over $\mathbb{F}_q$. For $\ell$ prime dividing $\#E(\mathbb{F}_q)$ but not dividing $(q - 1)$, if $gcd(\ell, q) = 1$ it is: $E[\ell] \subseteq E(\mathbb{F}_{q^k}) \iff \ell \mid (q^k - 1)$ .*

Thus, in our case, if embedding degree $k > 1$ and $\ell$ is prime, we can write $E(\mathbb{F}_{q^k})[\ell]$ as $E[\ell]$ in modified Tate-Lichtenbaum pairing domain, just as in the case of Weil pairing.

In our applications we make use of these observations when writing that bilinear pairing $e$, that we take, is given on the product $G \times G$ of finite cyclic groups (for $\ell$ being prime different from the base field characteristics, we can generate $G$ by choosing point of order $\ell$ from $E[\ell]$, and we find one since in that case, $E[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, [55] col. 6.4). Next, if we as mentioned earlier, want our pairing Weil or modified Tate-Lichtenbaum

to satisfy $e(P, P) \neq 1$ for $P$ of prime order $\ell$, we can use endomorphism of $E$. By endomorphisms of elliptic curve $E$ over $\mathbb{F}_q$ we mean homomorphisms from $E(\overline{\mathbb{F}_q})$ to itself given by rational functions. We state appropriate lemma ([31] IX.7.3, after [56]):

**Lemma 4.1.1.** *Let $P \in E(\mathbb{F}_q)$ have prime order $\ell$ and suppose $k > 1$. For $E(F_{q^k})$ not having points of order $\ell^2$, $\phi$ an endomorphism of $E$, we have that if $\phi(P) \notin E(\mathbb{F}_q)$, then $e(P, \phi(P)) \neq 1$.*

For a prime $\ell$ and a point $P \in E(\mathbb{F}_q)[\ell]$, we call a distortion map that kind of endomorphism, that further modify bilinear pairing, so that $e : E[\ell] \times E[\ell] \to \mu_\ell$ is non-degenerate on $P$. If a curve is supersingular, looking at $E(\mathbb{F}_q)[\ell]$, if embedding degree $k > 1$, then for any $P \in E(\mathbb{F}_q)[\ell] \setminus \{\mathcal{O}\}$ a distortion map exist ([33], [56]). In our applications we can use that kind of modified Tate-Lichtenbaum or Weil pairings, on certain supersingular curves which are related to $GDH$ groups (see [16], [3]).

At the end we also notice an asset of bilinear pairing that we make use of. In similar fashion as before when looking at DDHP, they allow to prove that two elements $P'$ and $Q'$ of $G$ are the same multiplicities of group elements $P$ and $Q$ modulo order of $e(P, Q)$ respectively. We calculate and compare $e(P, Q')$ with $e(P', Q)$. This property allows verification of signature shares in signature scheme as will be further presented.

## 4.2. General access structure based signature and decryption schemes

We show an extension of considerations of Pomykała related to general access structure based aggregated signature scheme. Extension allows different methods of encrypting monotonic access structures in the signature scheme. The proposal for signature scheme considered by Pomykała is based on CRT-Ore algorithm [45] and uses the generalized Asmuth-Bloom sequence. From the perspective introduced in this thesis one can notice that it is based on the method of encoding the monotonic structure from Section 2.1 with a function $f$ being $LCM$. We show how to use different presented in this thesis methods of encrypting monotonic access structures, to achieve similar results for the construction of signature scheme. Other considered methods are: method with extended Blakley's scheme which can be found in Section 1.2, method based on logical formulae from Section 2.1, and our plain set-theoretic method based on anti-monotonic approach with an abstract function $f$, introduced also in Section 2.1.

We present the scheme.

First, there is a preparation phase which is performed by the Trusted Authority. The Trusted Authority gives participants their public and private keys.

**Setup**

The Trusted Authority determines the bilinear structure $(G, e, Q, H)$, where $e$ is a bilinear map on the product $G \times G$ of finite cyclic groups of order $q$. Now $q$ that we consider is not related to the number of field elements over which an elliptic curve is defined, as it was previously. In practice, for $q$ being a prime, for a supersingular curve $E(K)$, where $K = \mathbb{F}_r$ for $r$ being some prime power, and $char(K) \neq q$, the bilinear pairing $e$ could be modified Weil or modified Tate-Lichtenbaum pairing on some subgroup $G$ of $q$-torsion points that is nontrivial (i.e. $\neq \{O\}, G$, hence of order $q$), and which is a $GAP$ group. Let $Q$ be generator of $G$ and $H : \{0,1\}^* \to G$ the suitable secure hash function.

To distribute private and public keys of the participants by Elgamal's method [26], the Trusted Authority defines the cyclic group $G'$ of order $q'$ with generating element $Q'$ such that discrete logarithm problem is hard in $G'$. Number of elements $q'$ has to be large enough, so there are enough points in $G'$ to map into $G'$ any possible share of participants, and as we will further see it is enough that $q' \geqslant q$. He also publishes easily invertible injection map $h : \{1, ..., p\} \to G'$ where $p$ is appropriately large to allow transformation of all possible shares into points in $G'$.

The Trusted Authority generates the random private keys $d_j \in \mathbb{Z}_{q'}$ of the group members and publishes the corresponding public keys $D_j = d_j Q'$.

The Manager chooses the monotonic structure $\Gamma$. In relation to it and the method of encrypting $\Gamma$ he publishes necessary public values for the reconstruction as follows:

For the method that uses CRT-Ore algorithm, generalized Asmuth-Bloom sequence and is based on anti-monotonic approach (denote it **[AB]**), he publishes the Asmuth-Bloom sequence $(q, p_1, ..., p_n)$ related to $\Gamma$. He also defines the modulus up to which solutions in CRT-Ore algorithm are equivalent, as $\pi = lcm(p_1, ..., p_n)$.

For the method with extended Blakley's scheme (denote it **[EBS]**), assuming $q$ is prime, after choosing participants vectors with coefficients in $\mathbb{F}_q^t$ forming vectors of identities which define $\Gamma$ with respect to $\mathbf{v} \in \mathbb{F}_q^t$, he publishes $\mathbf{v}$ and all $id$ vectors of participants.

For the method based on logical formulae and chosen additive share distribution method in $\mathbb{Z}_q$ (denote it **[LF]**), he publishes the formula that defines $\Gamma$.

For the plain set-theoretic method based on anti-monotonic approach with an abstract function $f$ (denote it **[PST]**), he publishes the family of basis sets $\mathbf{B}$. In that case he announces the following chosen operations, so that there were secure operations on shares, and a way of computing them:

For the family $\mathbf{F}$ being the set of values of $f$ (or any family that contains that set),

$$* : \ \mathbf{F} \times G \to G$$

is such that for any set $A$ from the domain of $f$, assuming that set $S$ from the description of $f$ is a subset of $\mathbb{Z}_q$ (so the domain of $f$ is in the power set $2^{\mathbb{Z}_q}$), for any $Q \in G$, there is:

$$f(A) * Q = (\sum_{a_i \in A} a_i)Q$$

and

$$\boxplus : \ G \times G \to G$$

such that for any sets $A, B$ from the domain of $f$, any $Q \in G$, there is:

$$f(A) * Q \boxplus f(B) * Q = f(A \cup B) * Q \ .$$

The Manager selects a key that is the base for the group signature:

**Key generation**

In **[AB]** the element responsible for signature scheme would be, selected by the Manager, random $x \in \mathbb{Z}_q$. We choose randomly an element $a \ mod \ \pi$ such that $s = x + aq < \pi$. The secret key that would be related to the group signature is $s$. The Manager defines the group public key: $S = sQ = xQ$.

In **[EBS]** the secret key would be $s = \mathbf{a} \cdot \mathbf{v}$, where random vector $\mathbf{a}$ comes from taking coefficients of secret polynomial in the scheme description and $\mathbf{v}$ is a vector determining $\Gamma$ as in Proposition 1.2.1. The group public key is: $S = sQ$.

In **[LF]** the secret key is $s \in \mathbb{Z}_q$ that will be distributed to the participants as it was described having an access structure implied by possibly nested logical formula. The group public key is: $S = sQ$.

In **[PST]** the secret key is $s = \sum_{a_i \in U} a_i$, where $U = \bigcup_i S_i$ and we sum all $S_i$, sets related to shares of participants in the description of $f$ (thus $f(U)$ is the secret distributed in the scheme). The group public key is: $S = sQ$

Now there is a phase of shares distribution performed by the Manager:
**Shares Distribution**
The Manager sends shares to chosen set of potential signers $W = \{P_i : i \leqslant l\}$.
We numerate the participants without loss of generality, with possible renumbering. Notice that it can also be $W = X$, the set of all participants, however here it is that additional possibility. He publishes the list

$$L = (V_1, E_1, ..., V_{l'}, E_{l'}) ,$$

where $l' \geqslant l$ and $V_i = s_i Q$ (except in **[PST]** where $V_i$'s are different and their number may be smaller than $E_i$'s). As in Elgamal's method, for randomly chosen $r \in \mathbb{Z}_{q'}$ there is $E_i = (rQ', Q'_i + rD_i)$, where $Q'_i = h(s_i)$ for $i = 1, ..., l'$ is the corresponding point of $G'$. Elements $s_i$ related to shares depend on method of encrypting monotonic structure as follows:

In **[AB]** $l' = l$ and the Manager computes the shares $s_i = s \bmod p_i$ for $i = 1, ..., l$. He also precomputes and publishes CRT-Ore coefficients for those privileged sets $B \in \Gamma$ for which $B \subseteq W$. That is, taking any such $B$, he finds coefficients $a_i, b_i$ for $i = 1, ..., |B|$ related to $B$, such that $(\sum a_i b_i s_i) \bmod \pi = s$, where the sum is over all $i$ related to the participants in $B$.

In **[EBS]** $l' = l$ and the Manager computes the shares $s_i = \mathbf{a} \cdot \mathbf{v}_i$, where $\mathbf{v}_i$ is identity of $i - th$ participant.

In **[LF]** shares, being additive parts of $s$ are distributed as it was written while presenting the scheme. In that case since there is possible need of sending multiple shares to single participant, $l'$ can be larger than $l$. Eventually, all the shares of a participant are sent as different $s_i$'s.

In **[PST]** share of $i$-th participant is a set being the value of $f(S_i)$ and Manager sends with a use of Elgamal's method all the elements of $f(S_i)$. Sent are $V_i = (\sum_{a_k \in S_i} a_k)Q$.

We move to the signing procedure.

**Signing**

Assume that the authorized group $B$ of signers from $\Gamma$, related to the list $L$, wants to sign the messages $m_1, ..., m_k$. Let $M = (m_1, ..., m_k)$. Firstly, every signer from $B$ for every cryptogram dedicated to him, decrypts the cryptogram $E_i$, then by inverting $h$ he receives the share $s_i$. Next:

In **[AB]** he uses related to the group $B$, public coefficients $a_i, b_i$ for $i = 1, ..., |B|$ yielding the signature share

$$\sigma_i(m_j) = a_i b_i s_i H(m_j) \ .$$

The signers broadcast them within the group $B$.

Every member of $B$ checks if $e(\sigma_i(m_j), Q)$ is equal to $e(a_i b_i H(m_j), V_i)$. If so, the signature of the group $B$ is the tuple $[M, B, \sigma]$, where

$$\sigma = \sum_j \sigma(m_j), \quad \text{with} \quad \sigma(m_j) = \sum_i \sigma_i(m_j).$$

In **[EBS]** we know from the construction (Proposition 1.2.1) that vector $\mathbf{v}$ lies in the subspace spanned by vectors of identities of participants in $B$. Then knowing their vectors of identities $\mathbf{v}_i$ for $i = 1, ..., |B|$ they can find elements $c_i \in \mathbb{F}_q$ such that $\sum c_i \mathbf{v}_i = \mathbf{v}$ (so there is also $\sum c_i s_i = \mathbf{a} \cdot \mathbf{v} = s$). Then, after only finding coefficients $c_i$ with a use of the vectors of identities they proceed as follows: the signature shares are

$$\sigma_i(m_j) = c_i s_i H(m_j)$$

which signers broadcast within the group $B$. Every member of $B$ checks if $e(\sigma_i(m_j), Q)$ is equal to $e(c_i H(m_j), V_i)$. If so, the signature of the group $B$ is $[M, B, \sigma]$ defined as before.

In **[LF]** participants from $B$ choose those shares from sets of shares they received that sum up to $s$. We consider here only the additive method, leaving threshold possibilities. However, this can also be generalized allowing threshold distribution similarly as it was shown above, where the coefficient of $s_i$ is 'accumulated', that is multiplied accordingly by other found coefficients from upper parts of the formula (there are publicly distributed $id$'s for reconstruction), so that eventually $\sum c_i s_i = s$, where we sum all $s_i$ that take place in the reconstruction. With additive method there is simply $\sum s_i = s$ (all computations in $\mathbb{Z}_q$). There can be many shares from single participant. Let $\sum_{k \in U_i} s_k$ be the sum of $i$-th participant's shares that take part in the reconstruction in $B$. The $i$-th participant announces the set of indices $U_i$. The signature shares are

$$\sigma_i(m_j) = \left( \sum_{k \in U_i} s_k \right) H(m_j) \ .$$

After broadcast of signature shares within the group $B$ participants check if equal are $e(\sigma_i(m_j), Q)$ and $e(H(m_j), \sum_{k \in U_i} V_k)$. If so, the signature of the group $B$ is $[M, B, \sigma]$ as earlier.

In **[PST]** $i$-th participant has his share $f(S_i)$. The signature shares are then

$$\sigma_i(m_j) = f(S_i) * H(m_j) \ ,$$

where $*$ is the defined operation. Signatures are broadcast within the group $B$, then participants check if $e(\sigma_i(m_j), Q)$ equals $e(H(m_j), V_i)$. If so, the signature of the group $B$ is $[M, B, \sigma]$, where

$$\sigma = \sum_j \sigma(m_j), \quad \text{with} \quad \sigma(m_j) = \sum_i^{\boxplus} \sigma_i(m_j),$$

where $\boxplus$ is an addition operation in the sum $\sum_i^{\boxplus}$.

Verification of the signature:

**Verification**

To verify the signature one checks the validity condition, that is if equal are:

$$e(\sigma, Q) \quad \text{and} \quad \prod_j e(H(m_j), S) \ .$$

**Remark 4.2.1.** *It is possible in a similar fashion, using Elgamal's idea, to propose general access structure based group decryption schemes. Then the privileged groups would be able to decrypt an encrypted message. A sender generates the shares for the decryption group, as in the proposal for signature scheme above, then encrypts the message. Encrypting the message $M$ is performed using Elgamal's method to calculate $(rQ, M + rS)$ with random $r$, where the group public key $S = sQ$ is constructed as above. The group decrypts the message by finding $srQ = rS$ with a use of their shares. We notice that Elgamal's encryption is used in two different ways: to send shares for the participants as in the method above, and to encrypt the message.*

# Bibliography

[1] C. Asmuth, J. Bloom, *A modular approach to key safeguarding*, IEEE Trans. on Information Theory, IT-29(2):208-211, 1983.

[2] R. Balasubramanian, N. Koblitz, *The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm*, J. Cryptology, 11, 141–145, 1998.

[3] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, *Efficient algorithms for pairing-based cryptosystems*, M. Yung (ed.) CRYPTO 2002. LNCS, vol. 2442, 354–368. Springer, Heidelberg 2002.

[4] T. Becker, V. Weispfenning, *The Chinese remainder problem, multivariate interpolation, and Gröbner bases*, Proc. ISSAC'91, Bonn, ACM Press, 64–69, New York 1991.

[5] T. Becker, V. Weispfenning, *Gröbner Bases: A Computational Approach to Commutative Algebra*, Springer-Verlag, 1993.

[6] M. Ben-Or, S. Goldwasser, A. Wigderson, *Completeness theorems for non-cryptographic fault-tolerant distributed computation*, 1-10, Proc. ACM STOC '88.

[7] J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions*, Advances in Cryptology - CRYPTO '88.

[8] A. Beimel and N. Livne, *On matroids and nonideal secret sharing*, IEEE Trans. Inform. Theory, 54(6):2626–2643, 2008.

[9] G. Blakley, *Safeguarding cryptographic keys*, Proceedings of the National Computer Conference 48: 313–317, 1979

[10] E.F. Brickell, *Some ideal secret sharing schemes*, J. Combin. Math. Combin. Comput. 9, 105-113, 1989.

[11] E. Brickell, D. Davenport, *On the classification of ideal secret sharing schemes*, Journal of Cryptology, vol. 4, 123–134, 1991.

[12] D. Boneh, M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in cryptology, Crypto 2001 (Santa Barbara, CA), volume 2139 of Lecture Notes in Comput. Sci., 213-229, Springer-Verlag, Berlin 2001.

[13] D. Boneh, B. Lynn, H. Shacham, *Short Signatures from the Weil Pairing*, Proc. of Asiacrypt '01, Lecture Notes in Computer Sciences, Vol. 2248, Springer-Verlag, 514-532, 2001.

[14] B. Buchberger, *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, N. K. Bose ed. Recent trends in Multidimensional System theory. Dordrecht: Reidel, 184-232, 1985.

[15] B. Buchberger, F. Winkler, *Gröbbner Bases and Applications*, Cambridge University Press 1998.

[16] J.C. Cha, J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, Springer, Heidelberg, 18–30 2002.

[17] D. Chaum, C. Crépeau, I. Damgård, *Multi-party unconditionally secure protocols*, Proc. ACM STOC '88, 11-19.

[18] R. Cramer *Introduction to Secure Computation*, Lectures on Data Security - Modern Cryptology in Theory and Practice, Springer LNCS, vol. 1561, 16-62, 1999.

[19] R. Cramer, I. Damgård, U. Maurer, *General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme*, B. Preneel (Ed.), Advances in Cryptology, EuroCrypt 2000, Lecture Notes in Computer Science, vol. 1807, Springer, 316-334, Berlin 2000.

[20] J. Derbisz, *Methods of encrypting monotonic access structures*, Annales Universitatis Mariae Curie-Skłodowska Sectio AI Informatica XI, 2, 49-60, 2011.

[21] J. Derbisz, *Remarks on the foundations of access structures theory*, submitted.

[22] J. Derbisz, *Multivariate extensions of secret sharing schemes*, submitted.

[23] J. Derbisz, *General access structure based signature and decryption schemes on bilinear pairing*, submitted.

[24] J. Derbisz, J. Pomykała, *Pairing based group cryptosystem with general access structures*, Cyberprzestępczość i ochrona informacji, 329-348, WSM, Warszawa, 2012.

[25] J. Derbisz, J. Pomykała, *Uogólnione rozdzielanie sekretu w systemach rozproszonych*, Cyberprzestępczość i ochrona informacji, 311-328, WSM, Warszawa, 2012.

[26] T. Elgamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, IT-31(4):469–472, 1985.

[27] O. Farràs, C. Padró, *Ideal hierarchical secret sharing schemes*, Seventh IACR Theory of Cryptography Conference, TCC 2010, Lecture Notes in Comput. Sci., vol. 5978, 219–236, 2010.

[28] J.-C. Faugére, *A New Efficient Algorithm for Computing Gröbner Basis (F4)*, Journal of Pure and Applied Algebra 139(1-3), 61–88, 1999.

[29] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, in: ISSAC '02: Proceedings from the International Symposium on Symbolic and Algebraic Computation, pp. 75–83, 2002.

[30] M. Fellows, N. Koblitz, *Combinatorial cryptosystems galore!*, Contemporary Mathematics, 51-61, 1994.

[31] S. D. Galbraith, *Pairings, Advances in elliptic curve cryptography*, London Math. Soc. Lecture Note Ser., vol. 317, Cambridge University Press, Cambridge, 183–213, 2005.

[32] S. D. Galbraith, *Supersingular curves in cryptography*, Asiacrypt'2001, Lecture Notes in Computer Science 2248, 495–513, Springer-Verlag, 2002.

[33] S. D. Galbraith, *Mathematics of public key cryptography*, Cambridge University Press, 2012.

[34] M. Gasca, T. Sauer, *Polynomial interpolation in several variables*, Adv. Comput. Math., 12 (4), 377-410, 2000.

[35] O. Goldreich, S. Micali, A. Wigderson, *How to play any mental game or a completeness theorem for protocols with honest majority*, Proc. ACM STOC '87, 218-229.

[36] M. Ito, A. Saito, T. Nishizeki, Secret Sharing Scheme Realizing General Access Structure, Proc. Glob. Com, 1987.

[37] N. Koblitz, *Algebraiczne aspekty kryptografii*, WNT, Warszawa 2000.

[38] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation, 48, 203–209, 1987.

[39] C.P. Lai and C. Ding, *Several Generalizations of Shamir's Secret Sharing Scheme*, Internat. J. Found. Comput. Sci. 15, 445-458, 2004.

[40] A.J. Menezes, T. Okamoto, S.A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory 39, 1639–1646, 1993.

[41] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology-CRYPTO '85, Lecture Notes in Computer Science, Springer-Verlag, 218, 417–426, 1986.

[42] V. S. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology, 17, 235-261, 2004.

[43] T. Okamoto, D. Pointcheval, *The gap-problems: a new class of problems for the security of cryptographic Schemes*, Proc. of PKC '01, Lecture Nores in Computer Sciences, Vol. 1992, Springer-Verlag, 104-118, 2001.

[44] P.J. Olver, *On multivariate interpolation*, Stud. Appl. Math. 116, 201-240, 2006.

[45] O. Ore, *The general Chinese remainder theorem*, American Mathematical Monthly, 59:365-370, 1952.

[46] T. Sauer, *Polynomial interpolation of minimal degree and Gröbner bases*, Groebner Bases and Applications (Proc. of the Conf. 33 Years of Groebner Bases), eds. B. Buchberger and F. Winkler, London Math. Soc. Lecture Notes, Vol. 251, 483–494 Cambridge University Press, 1998.

[47] A. Shamir, *How to share a secret*, Communications of the ACM 22 (11): 612–613, 1979.

[48] G. J. Simmons: *How to (Really) Share a Secret*, 390-448 CRYPTO 1988.

[49] N. Smart, *Access control using pairing based cryptography*, Joye, M. (ed.) CT-RSA 2003, LNCS, vol. 2612, 111–121, Springer, Heidelberg 2003.

[50] S. Spież, M. Srebrny, J. Urbanowicz, *Remarks on the classical threshold secret sharing schemes*, Annales Societatis Mathematicae Polonae. Series 4: Fundamenta Informaticae, 2012.

[51] D. R. Stinson, *An explication of secret sharing schemes*, Designs, Codes and Cryptography, Vol. 2, 357–390, 1992.

[52] T. Tassa, *Hierarchical Threshold Secret Sharing*, J. Cryptology 20(2): 237-264, 2007.

[53] T. Tassa, N. Dyn, *Multipartite Secret Sharing by Bivariate Interpolation*, ICALP (2), 288-299, 2006.

[54] T. Tassa and J.L. Villar, *On proper secrets, (t; k)-bases and linear codes*, Des. Codes Cryptogr. 52, 129-154, 2009.

[55] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[56] E. Verheul, *Evidence that XTR is More Secure than Supersingular Elliptic Curve Cryptosystems*, Proceedings of Eurocrypt 2001, LNCS 2045, 195–210, Springer-Verlag, 2001.