

On Secret Sharing Schemes

Svetla Nikova[†], Venzislav Nikov

[†]ESAT/COSIC, Katholieke Universiteit Leuven, Belgium

Email: svetla.nikova@esat.kuleuven.be, vnikov@mail.com

Abstract

The concept of *secret sharing* has been introduced independently by Shamir and Blakley, as a tool to protect a secret from getting exposed or from being lost. It allows a so-called *dealer* to share a secret among the members of a set \mathcal{P} , which are usually called *players* or *participants*, in such a way that only certain specified subsets of players are able to reconstruct the secret while smaller subsets have no information about this secret at all. Since then the research on this topic has been extensive.

In this paper we are going to present an overview of some approaches for building secrets sharing schemes based on well studied objects like matroids and error-correcting codes on one hand. We will start with introducing the Shamir's polynomial scheme. Then we will talk about the relations between ideal Secret Sharing, matroids and error-correcting codes. On the other hand we will introduce linear SSS for general access structures and we will explain the approach by Cramer, Damgard and Maurer based on Monotone Span Programs. We will complete by considering error-set codes as a generalization of the notion of codes.

1. Introduction

1.1. Access Structures

To study *secret sharing schemes* (SSS) we first need to introduce some notation. Denote the *participants* (players) of the scheme by P_i , $1 \leq i \leq n$, the set of all *players* by $\mathcal{P} = \{P_1, \dots, P_n\}$ and the set of all subsets of \mathcal{P} (i.e. the power set of \mathcal{P}) by $P(\mathcal{P})$. Denote the *dealer* of the scheme by P_0 . As usual let us call the groups which are allowed to reconstruct the secret *qualified* (authorized) and the groups which should not be able to obtain any information about the secret *forbidden* (unqualified). The set of qualified groups is denoted by Γ ($\Gamma \subseteq P(\mathcal{P})$) and the set of forbidden groups by Δ ($\Delta \subseteq P(\mathcal{P})$). The set Γ is called *monotone increasing* if for each set A in Γ also each superset of A is in Γ . Similarly, Δ is called *monotone decreasing*, if for each set B in Δ also each subset of B is in Δ . A monotone increasing set Γ can be efficiently described by the set Γ^- consisting of the *minimal elements (sets)* in Γ , i.e. the elements in Γ for which no proper subset is also in Γ . Similarly, the set Δ^+ consists of the *maximal elements (sets)* in Δ , i.e. the elements in Δ for which no proper superset is also in Δ . The tuple (Γ, Δ) is

called an *access structure* if $\Gamma \cap \Delta = \emptyset$. It is obvious that (Γ^-, Δ^+) generates (Γ, Δ) . If the union of Γ and Δ is equal to $P(\mathcal{P})$ (so, Γ is equal to Δ^c , the complement of Δ), then it is said that the access structure (Γ, Δ) is *complete* and denote it just by Γ . From now on Γ will be used to denote complete access structures, whereas (Γ, Δ) will be used to denote (incomplete) access structures.

Sometimes the monotone decreasing sets Δ are referred to as *monotone structures* [12, 17]. The simplest access structure is called (k, n) -threshold, denoted by $T_{k,n}$, if all subsets of \mathcal{P} with at least $k + 1$ participants are qualified and any subset of up to k players is forbidden. Access structure (Γ, Δ) is called *connected* if every player is in at least one minimal qualified set [13, 10]. Let us define the *dual access structure* $(\Gamma^\perp, \Delta^\perp)$ for (Γ, Δ) [10]. The tuple $(\Gamma^\perp, \Delta^\perp)$ is defined on \mathcal{P} as follows

$$\Gamma^\perp = \{A : A^c \in \Delta\} \quad \text{and} \quad \Delta^\perp = \{A : A^c \in \Gamma\}.$$

For a complete access structure the dual access structure [13] could therefore be defined as follows. The *dual access structure* Γ^\perp of an access structure Γ , defined on \mathcal{P} , is the collection of sets $A \subseteq \mathcal{P}$ such that $\mathcal{P} \setminus A = A^c \notin \Gamma$ (i.e. $A^c \in \Delta$). Note that $(\Gamma^\perp)^\perp = \Gamma$ and $(\Delta^\perp)^\perp = \Delta$.

For any two monotone *decreasing* sets Δ_1, Δ_2 the operation \uplus and called *element-wise union* [21, 12] is defined as follows: $\Delta_1 \uplus \Delta_2 = \{A = A_1 \cup A_2; A_1 \in \Delta_1, A_2 \in \Delta_2\}$. It is easy to check that $\Delta_1 \uplus \Delta_2$ is monotone decreasing.

1.2. Adversary Structures

A common model for dealing with cheaters is to consider an *adversary* \mathcal{A} who may corrupt some of the players. The adversary is additionally characterized by a particular subset $\Delta_{\mathcal{A}}$ of Δ [12], which is itself monotone decreasing structure. The set $\Delta_{\mathcal{A}}$ is called *adversary structure* while the set Δ is called *privacy structure*. The players which belong to Δ are *curious* but execute the protocol correctly, while players which belong to $\Delta_{\mathcal{A}}$ are *corrupt* and may not follow the protocol.

In general one distinguishes between *passive* and *active* corruption. When the adversary obtains the complete information which the corrupt players possess, but the players still execute the protocol correctly, that is called *passive* corruption and the players are called curious. In contrast, *active* corruption means that the adversary takes complete control over the corrupt players. Obviously active corruption is strictly stronger than passive corruption. Another classification is whether the adversary is *static* or *adaptive*. By *static* is meant that the set of corrupt players is chosen by the adversary once and for all before the protocol starts, whereas *adaptive* means that the adversary can at any time during the protocol choose to corrupt additional player as long as the total set of corrupt players is in $\Delta_{\mathcal{A}}$.

An $(\Delta, \Delta_{\mathcal{A}})$ -adversary is an adversary who can (adaptively) corrupt some players passively and some players actively, as long as the set A of actively corrupt players and the set B of passively corrupt players satisfy both

$$A \in \Delta_{\mathcal{A}} \quad \text{and} \quad (A \cup B) \in \Delta.$$

This model is known as the *mixed adversary* model. In case $\Delta_{\mathcal{A}} = \Delta$ one simply says a $\Delta_{\mathcal{A}}$ -adversary. Note that in case of secret sharing schemes one has $\Delta_{\mathcal{A}} = \emptyset$. For verifiable secret

sharing schemes adversaries are classified according to whether they cheat actively or passively, i.e. the adversary is called *passive* if $\Delta_A = \emptyset$ and *active* otherwise. In the threshold case it is usual to shorten the notation (Δ, Δ_A) -adversary to (k, k_a) -adversary.

1.3. Linear Algebra Background

An $m \times d$ matrix M over a field \mathbb{F} defines a map from \mathbb{F}^d to \mathbb{F}^m by taking a vector $\mathbf{v} \in \mathbb{F}^d$ to the vector $M\mathbf{v} \in \mathbb{F}^m$. Associated with $m \times d$ matrix M (or linear map) are two natural subspaces, one in \mathbb{F}^m and the other in \mathbb{F}^d . The *kernel* of M (denoted by $\ker(M)$) is the set of vectors $\mathbf{u} \in \mathbb{F}^d$, such that $M\mathbf{u} = \mathbf{0}$. The *image* of M (denoted by $\text{im}(M)$) is the set of vectors $\mathbf{v} \in \mathbb{F}^m$ such that $\mathbf{v} = M\mathbf{u}$ for some $\mathbf{u} \in \mathbb{F}^d$.

For an arbitrary matrix M over \mathbb{F} , with m rows and for an arbitrary non-empty subset A of $\{1, \dots, m\}$, let M_A denote the restriction of M to the rows i with $i \in A$. If $A = \{i\}$ we write M_i . Similarly for any vector $\mathbf{k} \in \mathbb{F}^m$ and an arbitrary non-empty subset A of $\{1, \dots, m\}$, let $\mathbf{k}_A \in \mathbb{F}^{|A|}$ denote the restriction of \mathbf{k} to the coordinates $i \in A$. If $A = \{i\}$ we write \mathbf{k}_i . In the sequel \mathbf{v}^i will denote a vector but \mathbf{v}_i stands for the i -th coordinate of vector \mathbf{v} .

With the standard inner product $\langle \mathbf{v}, \mathbf{w} \rangle = \sum \mathbf{v}_i \mathbf{w}_i$, we write $\mathbf{v} \perp \mathbf{w}$, when $\langle \mathbf{v}, \mathbf{w} \rangle = 0$. For an \mathbb{F} -linear subspace \mathcal{V} of \mathbb{F}^d , \mathcal{V}^\perp denotes the collection of elements of \mathbb{F}^d , that are orthogonal to all of \mathcal{V} (the orthogonal complement). It is again an \mathbb{F} -linear subspace. For all subspaces \mathcal{V} of \mathbb{F}^d one has $\mathcal{V} = (\mathcal{V}^\perp)^\perp$. Other standard relations are $(\text{im}(M^T))^\perp = \ker(M)$, and $\text{im}(M^T) = (\ker(M))^\perp$, as well as $\langle \mathbf{v}, M^T \mathbf{w} \rangle = \langle M\mathbf{v}, \mathbf{w} \rangle$.

An $n \times (k + 1)$ matrix with the i -th row of the form $(1, \alpha_i, \dots, \alpha_i^k)$, where $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ are distinct elements, is called an $(n, k + 1)$ -Vandermonde matrix (over \mathbb{F}) generated by $\alpha_1, \dots, \alpha_n$. It is well known that any square Vandermonde matrix, i.e. $k + 1 = n$, has non-zero determinant. If M is an $(n, k + 1)$ -Vandermonde matrix over \mathbb{F} and A is a non-empty subset of the rows $\{1, \dots, n\}$, then the rank of M_A is maximal. In particular the rank is equal to $k + 1$, or equivalently, $\text{im}(M_A^T) = \mathbb{F}^{k+1}$ if and only if $|A| \geq k + 1$. Let $\boldsymbol{\varepsilon}$ denote the column vector $(1, 0, \dots, 0)^T \in \mathbb{F}^{k+1}$ and let M be an $(n, k + 1)$ -Vandermonde matrix generated by distinct non-zero elements $\alpha_1, \dots, \alpha_n$. Then stronger property holds, namely $|A| \leq k$ if and only if $\boldsymbol{\varepsilon} \notin \text{im}(M_A^T)$, i.e. there is no $\boldsymbol{\lambda} \in \mathbb{F}^{|A|}$ such that $M_A^T \boldsymbol{\lambda} = \boldsymbol{\varepsilon}$.

As usual for any vector \mathbf{v} the *support* of \mathbf{v} is defined as the set of nonzero coordinates (denoted by $\text{sup}(\mathbf{v})$) and for any two vectors \mathbf{x}, \mathbf{y} the set $\delta(\mathbf{x}, \mathbf{y})$ is defined as $\delta(\mathbf{x}, \mathbf{y}) = \{i : \mathbf{x}_i \neq \mathbf{y}_i\}$. Considering the properties of the support of a vector, we point out some similarities to the properties of a norm [23].

- (1) $\text{sup}(\mathbf{x}) = \emptyset$ if and only if $\mathbf{x} = \mathbf{0}$,
- (2) $\text{sup}(j\mathbf{x}) = \text{sup}(\mathbf{x})$ if $j \neq 0$, and
- (3) $\text{sup}(\mathbf{x} + \mathbf{y}) \subseteq \text{sup}(\mathbf{x}) \cup \text{sup}(\mathbf{y})$.

In their paper Fehr and Maurer [12] noticed that $\delta(\mathbf{x}, \mathbf{y})$ behaves like a metric, as for all vectors $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}^N$ one has that

- (1) $\delta(\mathbf{x}, \mathbf{x}) = \emptyset$,

(2) $\delta(\mathbf{x}, \mathbf{y}) = \delta(\mathbf{y}, \mathbf{x})$ (symmetry), and

(3) $\delta(\mathbf{x}, \mathbf{z}) \subseteq \delta(\mathbf{x}, \mathbf{y}) \cup \delta(\mathbf{y}, \mathbf{z})$.

Recall that for any two vectors $\mathbf{x} = (x_0, x_1, \dots, x_n)$ and $\mathbf{y} = (y_0, y_1, \dots, y_n)$ in \mathbb{F}^n the *Hamming distance* between them is given by $d(\mathbf{x}, \mathbf{y}) = |\delta(\mathbf{x}, \mathbf{y})|$. We will consider a generalization of δ and sup as defined by Van Dijk.

Definition 1.1 [10] Consider a vector $\mathbf{v} \in \mathbb{F}^N$. The coordinates in \mathbf{v} , which belong to player P_i are collected in a sub-vector denoted by \mathbf{v}^i and the coordinates that correspond to the secret, i.e. to the dealer P_0 are collected in a sub-vector denoted by \mathbf{v}^0 or in other words $\mathbf{v} = (\mathbf{v}^0, \mathbf{v}^1, \dots, \mathbf{v}^n)$ where $\mathbf{v}^i \in \mathbb{F}^{p_i}$. The \mathcal{P} -support of vector \mathbf{v} , denoted by $\text{sup}_{\mathcal{P}}(\mathbf{v})$, is defined as the set of coordinates i , $0 \leq i \leq n$ for which $\mathbf{v}^i \neq \mathbf{0}$, i.e.

$$\text{sup}_{\mathcal{P}}(\mathbf{v}) = \{i : \mathbf{v}^i \neq \mathbf{0}\}.$$

For two vectors $\mathbf{x} = (x^0, x^1, \dots, x^n)$ and $\mathbf{y} = (y^0, y^1, \dots, y^n)$ in \mathbb{F}^N define the set

$$\delta_{\mathcal{P}}(\mathbf{x}, \mathbf{y}) = \{i : \mathbf{x}^i \neq \mathbf{y}^i\}. \quad (1)$$

Hence $\delta_{\mathcal{P}}(\mathbf{x}, \mathbf{y}) = \text{sup}_{\mathcal{P}}(\mathbf{x} - \mathbf{y}) \subseteq \{0, \dots, n\}$. Note that the properties for sup and δ also hold for \mathcal{P} -support and for $\delta_{\mathcal{P}}(\mathbf{x}, \mathbf{y})$.

1.4. The Model

Consider a finite set \mathcal{K} (the set of *secrets*), n finite sets $\mathcal{S}_1, \dots, \mathcal{S}_n$, where \mathcal{S}_i is the set of possible *shares* for player P_i , and let \mathcal{Z} be their Cartesian product $\mathcal{Z} = \mathcal{S}_1 \times \dots \times \mathcal{S}_n$. The elements of \mathcal{Z} are called *sharing*.

Players and Communication Model:

Each player is connected to a common broadcast medium. Also between every two players as well as between every player and the dealer there are secure channels, also called bilateral channels. We assume that the system is synchronized, i.e. the players can access a common global clock. We also assume that each player has a local source of randomness. This communication model is called *secure-channel* and was introduced in [6, 9].

The Adversary Model:

The adversary can passively corrupt a group of players at any time as long as this group is from the set of forbidden players. The corrupt players are assumed to execute the protocol correctly, i.e. the adversary is passive but adaptive.

Definition 1.2 A secret sharing scheme based on an access structure (Γ, Δ) is a pair (Share, Reconstruct) of protocols (phases) namely, the sharing phase, where dealer P_0 shares to the players a secret $s \in \mathcal{K}$, and the reconstruction phase, where the players try to reconstruct s , such that the following two properties hold:

- *Privacy: The players of any set $B \in \Delta$ learn nothing about the secret s as a result of the sharing phase.*
- *Correctness: The secret s can be computed by any set of players $A \in \Gamma$.*

A complete access structure Γ is called *ideal* if there is an SSS for Γ , such that any participant has only one share with size equal to the size of the secret. Recall that the SSS is called *perfect* if and only if $\Delta^c = \Gamma$. An SSS is *linear* (denoted by LSSS) if the dealer uses only linear operations to share (to reconstruct) the secret amongst the participants.

Now we present an example of SSS, namely the Shamir's (k, n) -threshold SSS [24] (see Fig. 1). It is easy to see that this scheme is linear.

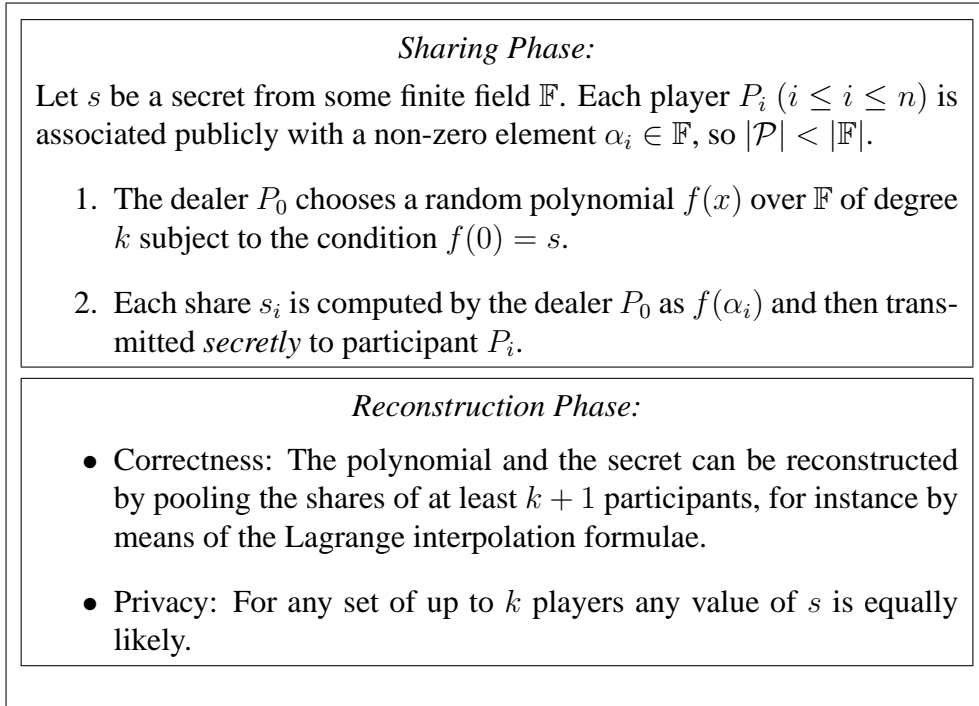


Figure 1: Shamir's Secret Sharing Scheme [24]

2. Ideal Secret Sharing Schemes

2.1. Ideal LSSS and Matroids

Matroids have been introduced by Whitney [25]. We first recall some basic facts, but refer to [26] for a more comprehensive introduction into the subject. A *matroid* $\mathfrak{M} = (\mathcal{S}, \mathcal{I})$ is a finite set \mathcal{S} and a collection \mathcal{I} of subsets of \mathcal{S} (called the *independent sets*) such that (I1) – (I3) are satisfied:

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $X \in \mathcal{I}$ and $Y \subseteq X$, then $Y \in \mathcal{I}$.

(I3) If $U, V \in \mathcal{I}$ with $|U| = |V| + 1$, there exists $x \in U \setminus V$ such that $V \cup \{x\} \in \mathcal{I}$.

A subset of \mathcal{S} not belonging to \mathcal{I} is called *dependent*. The maximal independent subsets of \mathcal{S} are called the *bases*, while the minimal dependent subsets are called *circuits*. The collection of bases is denoted by \mathcal{B} . A matroid \mathfrak{M} is uniquely defined by \mathcal{B} . The following theorem, known as the augmentation theorem, gives as a consequence that all bases in \mathfrak{M} have the same cardinality.

Theorem 2.1 [26] *Suppose that $X, Y \in \mathcal{I}$ and that $|X| < |Y|$. Then there exists $Z \subseteq Y \setminus X$ such that $|X \cup Z| = |Y|$ and $X \cup Z \in \mathcal{I}$.*

A matroid can also be uniquely defined by its *rank function*

$$\rho : P(\mathcal{S}) \rightarrow \mathbb{Z} : \rho(A) = \max\{|X| : X \subseteq A, X \in \mathcal{I}\}, \quad \forall A \subseteq \mathcal{S}.$$

The *rank of the matroid* is the rank of the bases. Consequently, if C is a circuit then $\rho(C) = |C| - 1$ and every proper subset of a circuit is independent. If for $x \in \mathcal{S}$, $A \subseteq \mathcal{S}$, $\rho(A \cup x) = \rho(A)$ it is said that x *depends* on A and it is denoted by $x \sim A$. If every set of cardinality l is a base in \mathcal{S} with $1 \leq l \leq n$ where n is the number of elements of \mathcal{S} , the matroid is said to be *uniform*, denoted by $\mathfrak{M}_{l,n}$. With any matroid, one can associate its dual.

Definition 2.2 [26] *If $\mathcal{B} = \{B_i : i \in I\}$ is the set of bases of a matroid \mathfrak{M} . Then the dual matroid \mathfrak{M}^* of a matroid \mathfrak{M} is defined by the set of bases $\mathcal{B}^* = \{\mathcal{S} \setminus B_i : i \in I\}$.*

It is said that a matroid \mathfrak{M} is *connected* or *non-separable* if for every pair of distinct elements x and y of \mathcal{S} there is a circuit of \mathfrak{M} containing x and y . Moreover, a matroid \mathfrak{M} is connected if and only if its dual \mathfrak{M}^* is connected. It appears that if a matroid \mathfrak{M} is connected then we do not need to know the full set of circuits of \mathfrak{M} in order to be able to specify the matroid completely.

Theorem 2.3 [26] *Let \mathfrak{M} be a connected matroid on \mathcal{S} and let x be a fixed element of \mathcal{S} . The collection of circuits of \mathfrak{M} which contains x uniquely determines \mathfrak{M} .*

A matroid is said to be representable over a field \mathbb{F} if there exists a vector space V over \mathbb{F} together with a map $\phi : \mathcal{S} \rightarrow V$ which represents the rank. However, the representability problem for matroids is still not completely solved. See, for instance, [26, Chapter 9] for some results on this problem.

Brickell and Davenport were the first to point out the relation between ideal LSSS and matroids over the set $\mathcal{S} = \{0, 1, \dots, n\} = \{P_0\} \cup \mathcal{P}$.

Definition 2.4 [4] *Consider an ideal SSS and define the set*

$$D = \{A \subseteq \mathcal{P} : \exists y \in A \text{ such that } y \sim A \setminus y\}.$$

Theorem 2.5 [4, 13, 11] *Let Γ be an ideal connected access structure on \mathcal{P} with $\Gamma^- = \{C_i, i \in I\}$. Then the sets $\{P_0\} \cup C_i, i \in I$ are all circuits through P_0 of a unique matroid (by Theorem 2.3) defined on $\mathcal{S} = \{P_0\} \cup \mathcal{P}$. This matroid is called to be induced by Γ , and denoted by $\mathfrak{M}(\Gamma)$. The set D is the set of the dependent sets of the connected matroid.*

The opposite relation is also true.

Theorem 2.6 [4] *Let $\mathfrak{M} = (\mathcal{S}, \mathcal{I})$ be a connected representable matroid and let $P_0 \in \mathcal{S}$. Then there exists a connected ideal SSS on $\mathcal{P} = \mathcal{S} \setminus \{P_0\}$ with a dealer P_0 such that $D = \mathcal{I}$.*

A relation between the dual access structures and matroids also holds.

Theorem 2.7 [13, 11] *Let Γ be a connected ideal access structure that induces a matroid $\mathfrak{M}(\Gamma)$. Then the dual access structure Γ^\perp induces a matroid $\mathfrak{M}(\Gamma^\perp)$ and*

$$\mathfrak{M}(\Gamma)^* = \mathfrak{M}(\Gamma^\perp).$$

Theorem 2.8 [13, 11] *Let Γ be an ideal access structure that induces a matroid $\mathfrak{M}(\Gamma)$. Then Γ is connected if and only if $\mathfrak{M}(\Gamma)$ is connected.*

2.2. Ideal LSSS and Error-Correcting Codes

Let \mathbb{F} be a finite field and let the set of secrets be $\mathcal{K} = \mathbb{F}^{p_0}$. We will consider only the case $p_0 = 1$. Associate with each player P_i ($1 \leq i \leq n$) a positive integer p_i such that the sets of possible shares for player P_i , is a linear subspace $\mathcal{S}_i = \mathbb{F}^{p_i}$. Analogously p_0 is associated with the dealer P_0 . Denote by $p = \sum_{i=1}^n p_i$ and by $N = p_0 + p$. Then the sharing space $\mathcal{Z} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_n = \mathbb{F}^p$ and $\mathcal{K} \times \mathcal{Z} = \mathbb{F}^N$. From now on we will consider only connected access structures. However when we speak about error-correcting codes we always will assume that $p_i = 1$ for all $0 \leq i \leq n$ (i.e. ideal case), hence $p = n$ and $N = n + 1$ hold.

Now we will give some notions from the theory of error-correcting codes. Any non-empty subset \mathcal{C} of \mathbb{F}^N is called a *code* and the parameter N is called the *length* of the code. Each vector in \mathcal{C} is called a *codeword* of \mathcal{C} . Define the *minimum distance* of a code \mathcal{C} as the smallest of all (Hamming) distances between different codewords in \mathcal{C} . It follows from this definition that a code with minimum distance d_{min} can correct $\lfloor (d_{min} - 1)/2 \rfloor$ errors, since spheres with this radius are disjoint (see [19]). If d_{min} is even the code can *detect* $d_{min}/2$ errors, meaning that a received word cannot have distance $d_{min}/2$ to one codeword and distance less than $d_{min}/2$ to another one. It may however have distance $d_{min}/2$ to more codewords.

Something more actually can be said. Code \mathcal{C} can decode errors and *erasures* simultaneously. An erasure is an ambiguously received coordinate (the value is undecided), thus the erasures can be considered as errors in known positions. Let \mathcal{C} be a code of length N with minimum distance d_{min} and let $e = \lfloor (d_{min} - 1)/2 \rfloor$. Then the code can correct b errors and c erasures as long as $2b + c < d_{min}$. In other words, the transmitted codeword should be retrievable if during the transmission at most c of the symbols in the word are erased and at most b received symbols are incorrect.

If \mathcal{C} is a T -dimensional subspace of \mathbb{F}^N , then the code \mathcal{C} is *linear* and its characteristic parameters are given by $[N, T, d_{min}]$. The set \mathcal{C}^\perp is an $(N - T)$ -dimensional linear subspace of \mathbb{F}^N and is called the *dual code* of \mathcal{C} .

There are two methods to define a linear code \mathcal{C} : a *generator matrix* and a *parity check matrix*. A *generator matrix* of a linear code \mathcal{C} is any $T \times N$ matrix G whose rows form a basis for \mathcal{C} . A generator matrix H of \mathcal{C}^\perp is called a *parity check matrix* for \mathcal{C} . Clearly, the matrix

H is of size $(N - T) \times N$. It follows that $\mathbf{x} \in \mathcal{C}$ if and only if $H\mathbf{x}^T = \mathbf{0}$, or in other words $HG^T = GH^T = 0$ holds.

The following relation between representable matroids and error-correcting codes is well known. Considering the columns of the generator matrix of a linear code \mathcal{C} , they define a representable (over \mathbb{F}) matroid \mathfrak{M} on the set of points $\mathcal{S} = \{P_0\} \cup \mathcal{P}$. All generator matrices of the code \mathcal{C} define the same matroid \mathfrak{M} , and hence the matroid is said to be associated to the code \mathcal{C} and is denoted by $\mathfrak{M}(\mathcal{C})$. In addition it is said that the code \mathcal{C} is a representation of the matroid $\mathfrak{M}(\mathcal{C})$. Note that while a unique matroid is associated to a linear code, different codes can be represented by the same matroid. The matroid that is associated with the dual code \mathcal{C}^\perp is the dual matroid $\mathfrak{M}(\mathcal{C})^*$, i.e, $\mathfrak{M}(\mathcal{C})^* = \mathfrak{M}(\mathcal{C}^\perp)$.

For any $[N, T, d_{min}]$ code, the following inequality known as the *Singleton bound* holds, $d_{min} \leq N + 1 - T$. In particular, if $d_{min} = N + 1 - T$ then the $[N, T, d_{min}]$ code is called *maximum distance separable* (MDS). MDS codes, in particular Reed-Solomon codes, have interesting properties which are often used in cryptography and particularly in secret sharing schemes. The following property of MDS codes is well known.

Lemma 2.9 [19] *Let \mathcal{C} be a $[N, T, d_{min}]$ code. Then the following statements are equivalent:*

1. \mathcal{C} is an $[N, T, N + 1 - T]$ MDS code,
2. any T columns of a generator matrix of \mathcal{C} are linearly independent,
3. \mathcal{C}^\perp is an $[N, N - T, T + 1]$ MDS code.

McEliece and Sarwate [18] reformulated Shamir's scheme in terms of Reed-Solomon codes instead of polynomials, improving it by adding error-correcting capabilities. The general relationship between linear codes and secret sharing schemes was established by Massey [16], Blakley and Kabatianskii [7]. In fact, the coding theoretic approach can be reformulated as the vector space construction, which was introduced by Brickell in [3]. This approach was generalized to the so-called generalized vector space construction by Van Dijk [10]. Two approaches to the construction of secret sharing schemes based on linear codes could be distinguished. These two types of approaches can be described as follows.

The first approach uses an $[n, k + 1, d_{min}]$ linear code $\overline{\mathcal{C}}$. Let \overline{G} be a generator matrix of $\overline{\mathcal{C}}$, so it is a $(k + 1) \times n$ matrix. The dealer P_0 chooses a random information vector $\mathbf{x} \in \mathbb{F}^{k+1}$, subject to $\mathbf{x}_1 = s$ – the secret. Then he calculates the codeword \mathbf{y} corresponding to this information vector as $\mathbf{y} = \mathbf{x}\overline{G}$, ($\mathbf{y} \in \mathbb{F}^n$). Then the dealer P_0 gives y_j to player P_j to be his share.

The secret sharing schemes based on linear codes with respect to the first approach were considered by Shamir, in terms of polynomials. In terms of vector spaces, Brickell studied it and a generalization was given by Van Dijk. As we will see in the next section the monotone span program approach could also be considered as an approach of this kind.

Theorem 2.10 [3] *Let \overline{G} be a generator matrix of an $[n, k + 1, d_{min}]$ linear code. In a secret sharing scheme based on \overline{G} as described above a set of shares belonging to players $A \subset \mathcal{P}$ determines the secret s if and only if the vector $\boldsymbol{\varepsilon}$ is a linear combination of the columns in the generator matrix \overline{G} with indices in A . Furthermore, the secret-sharing is perfect.*

The second approach uses an $[N = n + 1, k + 1, d_{min}]$ linear code $\tilde{\mathcal{C}}$. Let \tilde{G} be a generator matrix of $\tilde{\mathcal{C}}$, so it is $(k + 1) \times (n + 1)$. The dealer P_0 calculates the codeword \mathbf{y} as $\mathbf{y} = \mathbf{x}\tilde{G}$, ($\mathbf{y} \in \mathbb{F}^N$), from a random information vector $\mathbf{x} \in \mathbb{F}^{k+1}$, subject to $y_0 = s$ – the secret. Then the dealer P_0 gives y_j to player P_j to be his share.

Theorem 2.11 [16] *Let \tilde{G} be a generator matrix of an $[n+1, k+1, d_{min}]$ linear code. In a secret sharing scheme based on \tilde{G} with respect to the second approach a set of shares belonging to players $A \subset \mathcal{P}$ determines the secret s if and only if the first column in \tilde{G} is a linear combination of the columns with indices in A . Furthermore, the secret-sharing is perfect.*

Secret sharing schemes based on codes with respect to the second approach were considered by Massey. The two approaches seem different but they are related. In the first approach all the shares form a *complete* codeword of the code, while in the second one all the shares form only part of a codeword. But as Van Dijk [10] proved one can simply transform the matrices of the codes, setting $\tilde{G} = (\varepsilon \mid \overline{G})$. Hence one can consider the code $\overline{\mathcal{C}}$ to be obtained from the code $\tilde{\mathcal{C}}$ by *puncturing* i.e. by deleting a coordinate [19].

We will illustrate the error correcting influence to SSSs by the following example, given by McEliece and Sarwate.

Theorem 2.12 [18] *Consider an $k + 1$ -dimensional MDS code \mathcal{C} of length $N = n + 1$ over \mathbb{F} and select at random any of the $|\mathbb{F}|^k$ codewords $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_n)$ with $\mathbf{c}_0 = s$ (s is the secret to be shared). The dealer gives c_i as a share to participant i , $1 \leq i \leq n$.*

If $k + 1 + 2k_a$ or more participants pool together their shares, and at most k_a of these values are incorrect, then the secret s can be recovered correctly and the lying participants can be identified.

If $k + 2k_a$ or less participants pool together their shares, and precisely k_a of these values are incorrect, then the secret s cannot be recovered correctly. In fact, each value of s is equally likely.

To prove this theorem, it is sufficient to interpret the missing shares as erasures and use the theory above. By making use of Reed-Solomon codes, the authors showed that recovery of the secret can in fact, be done efficiently.

Corollary 2.13 *The secret sharing schemes defined in Theorem 2.12 is a perfect (k, n) -threshold scheme, secure against k_a corrupt (cheating) players ($k_a \leq k$).*

In SSSs, cheaters may disclose incorrect shares causing honest participants to recover a forged secret. This problem is closely related to error-correcting codes. Thus the McEliece and Sarwate result could be restated as follows. For Shamir's (k, n) -threshold scheme a collusion of k_a cheaters can be identified (and the secret recovered) if and only if $k_a \leq \lfloor (d_{min} - 1)/2 \rfloor$, where d_{min} is the minimum distance of the $[n + 1, k + 1, n + 1 - k]$ MDS code \mathcal{C} .

3. General Secret Sharing Schemes

3.1. A Linear Algebra View on LSSS

We start with a formal definition of a monotone span program.

Definition 3.1 [15] A Monotone Span Program (MSP) \mathcal{M} is a quadruple $(\mathbb{F}, M, \varepsilon, \psi)$, where \mathbb{F} is a finite field, M is a matrix (with m rows and $d \leq m$ columns) over \mathbb{F} , $\psi : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ is a surjective (labelling) function and $\varepsilon = (1, 0, \dots, 0)^T \in \mathbb{F}^d$ is called target vector. The size of \mathcal{M} is the number m of rows and is denoted as $\text{size}(\mathcal{M})$.

As ψ labels each row with a number i from $\{1, \dots, m\}$, corresponding to player $P_{\psi(i)}$, one can imagine that each player owns one or more rows from the matrix. Also consider a “function” φ from $\{P_1, \dots, P_n\}$ to $\{1, \dots, m\}$ which gives for every player P_i the set of rows owned by him (denoted by $\varphi(P_i)$). In some sense φ is “inverse” of ψ . For any set of players $B \subseteq \mathcal{P}$ consider the matrix consisting of rows these players own in M , i.e. $M_{\varphi(B)}$. As it is common, we shall shorten the notation $M_{\varphi(B)}$ to just M_B . The reader should stay aware of the difference between M_B for $B \subseteq \mathcal{P}$ and for $B \subseteq \{1, \dots, m\}$.

An MSP is said to compute a (complete) access structure Γ when $\varepsilon \in \text{im}(M_A^T)$ if and only if A is a member of Γ . We denote such an access structure by $\Gamma(\mathcal{M})$. It is said that A is *accepted* by \mathcal{M} if and only if $A \in \Gamma$, otherwise it is said that A is *rejected* by \mathcal{M} . In other words, the players in A can reconstruct the secret precisely if the rows they own contain in their linear span the target vector of \mathcal{M} , and otherwise they get no information about the secret. Hence when a set A is accepted by \mathcal{M} there exists a so-called *recombination vector* (column) λ such that $M_A^T \lambda = \varepsilon$. Using the recombination vector λ it is easy to see that the following relation holds $\langle \lambda, M_A(s, \rho)^T \rangle = \langle M_A^T \lambda, (s, \rho)^T \rangle = \langle \varepsilon, (s, \rho)^T \rangle = s$ for any secret s and any random vector ρ . Notice that the vector $\varepsilon \notin \text{im}(M_B^T)$ if and only if there exists a vector $k \in \mathbb{F}^d$ such that $M_B k = \mathbf{0}$ and $k_1 = 1$. The equivalence follows from the following remark. Recall that $\text{im}(M_B^T) = (\ker(M_B))^\perp$, thus $\varepsilon \notin \text{im}(M_B^T)$ if and only if there exists a vector $k \in \ker(M_B)$ with $\langle \varepsilon, k \rangle \neq 0$, i.e. $k_1 \neq 0$.

In general any non-zero vector can serve as a target vector for the MSP. It is straightforward to construct an MSP $\tilde{\mathcal{M}}$ with a target vector $\mathbf{1}$ (all 1 vector) starting from an MSP \mathcal{M} with a target vector ε (and vice versa) by adding (subtracting) the first column of the matrix M to all other columns of M . In other words there exists a matrix \tilde{D} with $\tilde{M} = M\tilde{D}$. Recall that an SSS is called *ideal* if any participant has only one share. In case an ideal LSSS is induced by an MSP we will call the MSP *ideal*. Let \mathcal{M} be a MSP computing $\Gamma(\mathcal{M})$. We call an MSP the *dual MSP* if it computes $\Gamma(\mathcal{M})^\perp$ and will denote it by \mathcal{M}^\perp . We stress here that

$$\begin{aligned} A \in \Gamma &\iff \exists \lambda \in \mathbb{F}^{|\varphi(A)|} \text{ such that } M_A^T \lambda = \varepsilon \\ B \notin \Gamma &\iff \exists k \in \mathbb{F}^d \text{ such that } M_B k = \mathbf{0} \text{ and } k_1 = 1. \end{aligned} \quad (2)$$

The first property guaranties *correctness* and the second *privacy* of the SSSs, see Definition 1.2. Technically property (2) means that when one considers the restricted matrix M_A for some subset A of \mathcal{P} , the first column is linearly dependent of the other columns if and only if $A \notin \Gamma$. We stress here that the first column in M has different role than the other columns, as we will demonstrate later. Sometimes we will slightly rewrite the first property in the following way:

$$A \in \Gamma \iff \exists \lambda \in \mathbb{F}^m \text{ such that } M^T \lambda = \varepsilon \text{ and } \text{sup}_{\mathcal{P}}(\lambda) \subseteq A. \quad (3)$$

The vector λ in (3) in fact is the same vector as in (2), but expanded with zeroes. Note that for a given access structure Γ there are many MSPs computing it. This fact is analogous to the fact that for a given code there are many generator (and therefore parity-check) matrices.

Beimel *et al.* [5] have observed that the number of columns d in an MSP \mathcal{M} can be increased without modifying the access structure which is computed. However it is always possible to keep the number of columns upper bounded by the size of the program (since one may restrict the matrix to a set of linearly independent columns without modifying the function that is computed). The space generated by the 2-nd up to the d -th column of M cannot contain a non-zero multiple of the first column. It also follows that one can always replace the 2-nd up to the d -th column of M by any set of vectors that generates the same space, without modifying the access structure that is computed.

Now we present the protocol of the linear algebra view on Shamir's SSS as given in [8] (see Fig. 2).

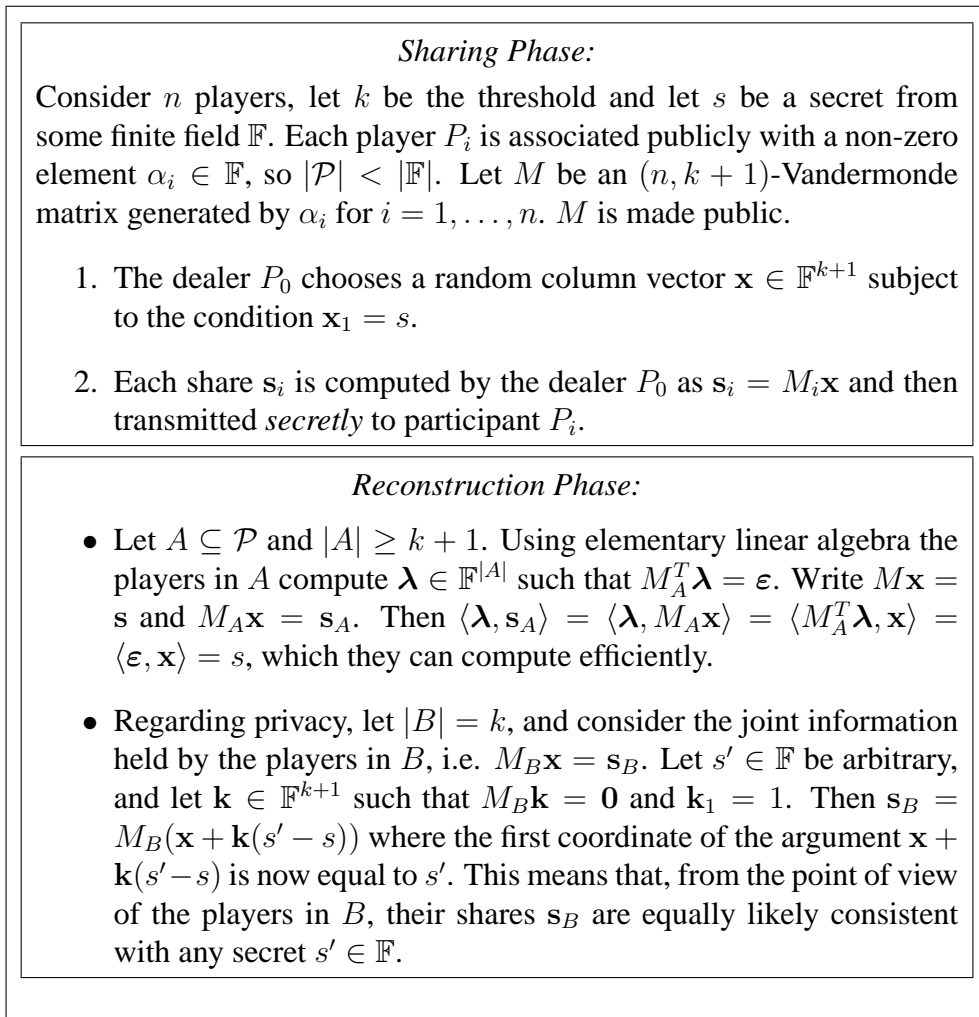


Figure 2: Shamir's Secret Sharing Scheme as an MSP [8]

Definition 3.2 [10] Let $\Gamma^- = \{X_1, \dots, X_r\}$. Then the set of vectors $C = \{\mathbf{c}^i \in \mathbb{F}^m : 1 \leq i \leq r\}$

$r\}$ is said to be suitable for the access structure Γ if C satisfies the following properties:

- $\text{sup}_{\mathcal{P}}(\mathbf{c}^i) = X_i$ for $1 \leq i \leq r$;
- for any vector (μ_1, \dots, μ_r) in \mathbb{F}^r , such that $\sum_{i=1}^r \mu_i \neq 0$, there exists a set $X \in \Gamma = \Delta^c$ satisfying $X \subseteq \text{sup}_{\mathcal{P}}(\sum_{i=1}^r \mu_i \mathbf{c}^i)$.

Lemma 3.3 Let $\Gamma^- = \{X_1, \dots, X_r\}$ be an access structure computed by an MSP \mathcal{M} . Also let $\lambda^i \in \mathbb{F}^m$ be the recombination vector that corresponds to X_i (see (2) and (3)). Then the set of vectors $C = \{\lambda^i : 1 \leq i \leq r\}$ defines a suitable set of vectors for the complete access structure Γ .

In the next theorem Van Dijk provides an important link between a parity check matrix of a code generated as a span of suitable vectors and an MSP matrix.

Theorem 3.4 [10] Let $\Gamma^- = \{X_1, \dots, X_r\}$. Consider a set of vectors $C = \{\mathbf{c}^i : 1 \leq i \leq r\}$. Let H be a parity check matrix of the code generated by the linear span of the vectors $(1, \mathbf{c}^i)$, $1 \leq i \leq r$ and let H be of the form $H = (\varepsilon \mid H')$ (This can be assumed without loss of generality). Then the MSP with the matrix M defined by $M^T = H'$ computes the access structure Γ if and only if the set of vectors C is suitable for Γ .

There is a tight connection between an access structure and its dual. It turns out that the codes generated by the corresponding sets of suitable vectors are dual.

Theorem 3.5 [10] Let $\Gamma^- = \{X_1, \dots, X_r\}$ be an access structure and $(\Gamma^\perp)^- = \{Z_1, \dots, Z_t\}$ be its dual. Then there exists a suitable set $C = \{\mathbf{c}^i : 1 \leq i \leq r\}$ for Γ if and only if there exists a suitable set $C^\perp = \{\mathbf{h}^j : 1 \leq j \leq t\}$ for Γ^\perp .

Suppose there exists a suitable set C for Γ and a suitable set C^\perp for Γ^\perp . Let \mathcal{C}^* be the code defined by the linear span of vectors $\{(1, \mathbf{c}^i) : 1 \leq i \leq r\}$ and let \mathcal{C}^\perp be the code defined by the linear span of vectors of $\{(1, \mathbf{h}^j) : 1 \leq j \leq t\}$. Then the codes \mathcal{C}^* and \mathcal{C}^\perp are orthogonal to each other.

Actually this result can be improved.

Corollary 3.6 [22] Let \mathcal{M} be an MSP program computing Γ , and \mathcal{M}^\perp be an MSP computing the dual access structure Γ^\perp . Let code \mathcal{C}^\perp have the parity check matrix $H^\perp = (\varepsilon \mid (M^\perp)^T)$ and let code \mathcal{C} have the parity check matrix $H = (\varepsilon \mid M^T)$. Then for any MSP \mathcal{M} there exists an MSP \mathcal{M}^\perp such that \mathcal{C} and \mathcal{C}^\perp are dual.

Now it is easy to observe that the approaches of building SSS based on matroids and error-correcting codes can be considered as particular cases of the monotone span program approach.

3.2. Error-Set Correcting Codes

As usual any non-empty subset \mathcal{C} of $\mathbb{F}^{p_0} \times \dots \times \mathbb{F}^{p_n} = \mathbb{F}^N$ is called a code. For a code \mathcal{C} the set of possible (allowed) distances is defined by

$$\Gamma(\mathcal{C}) = \{A : \text{there exist } \mathbf{a}, \mathbf{b} \text{ in } \mathcal{C}, \mathbf{a} \neq \mathbf{b} \text{ such that } \delta_{\mathcal{P}}(\mathbf{a}, \mathbf{b}) \subseteq A\}$$

and the *set of forbidden distances* is defined by $\Delta(\mathcal{C}) = \Gamma(\mathcal{C})^c$ [23]. It is easy to see that $\Delta(\mathcal{C})$ is monotone decreasing and that $\Gamma(\mathcal{C})$ is monotone increasing.

Thus, the linear $[n, k, d]$ -code over \mathbb{F} can be generalized to the linear $[N, T, \Delta(\mathcal{C})]$ -code over \mathbb{F} . The $[N, T, \Delta(\mathcal{C})]$ -code is called an error-set code [23] because of the property that all vectors for which the support belongs to $\Delta(\mathcal{C})$ are no codewords. It also implies that if x is a codeword then $\text{supp}_{\mathcal{P}}(x) \notin \Delta(\mathcal{C})$. It is clear that for $\Delta(\mathcal{C}) = \{A : |A| \leq d - 1\}$, the $[n + 1, k, \Delta(\mathcal{C})]$ -code coincides with the usual definition of $[n + 1, k, d]$ -code.

The set of *minimal* codewords is defined as $\Gamma(\mathcal{C})^- = \{A : \text{there exist } \mathbf{a}, \mathbf{b} \text{ in } \mathcal{C}, \mathbf{a} \neq \mathbf{b} \text{ such that } \delta_{\mathcal{P}}(\mathbf{a}, \mathbf{b}) = A \text{ but, there is no } \mathbf{c}, \mathbf{d} \in \mathcal{C}, \mathbf{c} \neq \mathbf{d}, \delta_{\mathcal{P}}(\mathbf{c}, \mathbf{d}) \subsetneq A\}$. It was proven that the error-set correcting codes have similar error-correcting capabilities as classical codes have.

Theorem 3.7 [23] *A code \mathcal{C} with set of forbidden distances $\Delta(\mathcal{C})$ can correct all errors in Δ if and only if $\Delta \uplus \Delta \subseteq \Delta(\mathcal{C})$.*

Consider the special case with threshold access structure, so $\Delta = \{A : |A| \leq e\}$. Now $\Delta \uplus \Delta = \{A : |A| \leq 2e\} = \Delta(\mathcal{C})$ and so $\Gamma(\mathcal{C}) = \{A : |A| \geq 2e + 1\}$. Hence the minimum distance of \mathcal{C} is $d_{\min} = 2e + 1$. In this case, Theorem 3.7 is equivalent to the classical error-correcting theorem. A connection between MSP and error-set codes is further established in [23].

Theorem 3.8 *Let $\mathcal{M} = (\mathbb{F}, M, \varepsilon, \psi)$ be an MSP computing an access structure Γ . Let $\tilde{\mathcal{C}}$ be an $[N, T, \Delta(\mathcal{C})]$ -code with generator matrix \tilde{G} of the form $\tilde{G} = (\varepsilon \mid M^T)$. Then the minimal codewords (i.e. those in $\Gamma(\mathcal{C})^-$) are suitable vectors for Γ^\perp (i.e. these are vectors of the form $(1, c)$ and $\text{supp}_{\mathcal{P}}(c) \in \Gamma^\perp$).*

Definition 3.9 [22] *An MSP is called Δ -non-redundant (denoted by Δ -rMSP) when $v \in \ker(M^T) \iff v \neq 0$ and $\text{supp}_{\mathcal{P}}(v) \in \Gamma$ ($\Gamma = \Delta^c$).*

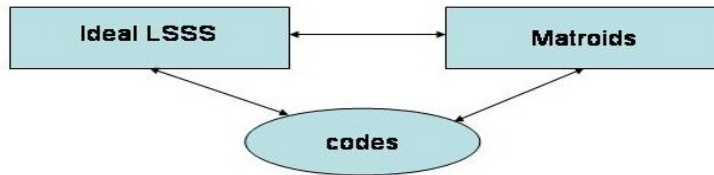
Corollary 3.10 [23] *Let \mathcal{M}^\perp be a Δ^\perp -rMSP computing Γ^\perp and let M be the matrix of the dual MSP \mathcal{M} computing Γ . Let $\tilde{\mathcal{C}}$ be an error-set correcting code with a generator matrix \tilde{G} of the form $\tilde{G} = (\varepsilon \mid M^T)$. Then the set of forbidden distances $\Delta(\tilde{\mathcal{C}})$ is equal to $\Delta^\perp \uplus \{\emptyset, P_0\}$.*

Corollary 3.11 [23] *An error-set correcting code $\tilde{\mathcal{C}}$ corrects $\Delta_{\mathcal{A}}$ (k_a in the threshold case) errors and one erasure (e.g. $\{P_0\}$) if and only if $\Delta_{\mathcal{A}} \uplus \Delta_{\mathcal{A}} \subseteq \Delta^\perp$ (analogously $2k_a < n - k$).*

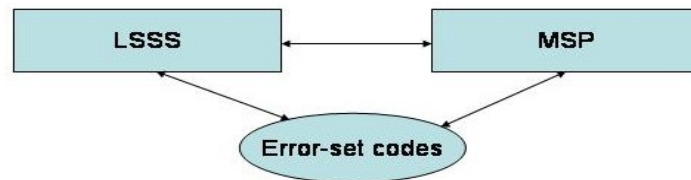
Note that no relation between Δ and $\Delta_{\mathcal{A}}$ (or for k and k_a) is required. Thus the main difference between error-set correcting codes and SSS is that the SSS provides additionally *privacy*, meaning that $\Delta \supseteq \Delta_{\mathcal{A}}$ (or $k \geq k_a$).

4. Conclusions

In this paper we give an overview of some of the approaches for building secret sharing schemes. First we present two approaches based on well studied objects, namely, error correcting codes - to build threshold SSS and matroids - to build ideal linear SSS. These approaches are efficient but not general. The first known techniques for building general SSS lead to exponential number of shares. Moreover these approaches are not suitable for building more complex protocols like verifiable SSS or multi party computation on the top of SSS.



In 1993 MSP have been introduced as an algebraic model of computation. Later it has been proven that for any general access structure can be build linear SSS based on MSPs. Moreover the number of shares in the worst case is super-polynomial. On the other hand MSPs can be considered as a generalization of matroids. Recently we have introduced error-set codes as a generalization of the notion of codes. By means of error-set codes and MSPs one can build general SSS. Moreover this approach is general and can easily be applied to more complex protocols, which use SSS as a building block.



Finally we have shown that the relations that are valid between ideal linear SSS, matroids and error-correcting codes are also valid between their generalizations - LSSS, MSP and error-set codes, respectively (see the figures).

References

- [1] G. Blakley. Safeguarding cryptographic keys, *AFIPS* 48, 1979, pp. 313-317.
- [2] A. Braeken, V. Nikov, S. Nikova, Error-Set Codes and Related Objects, COCOON 2005, LNCS 3595, 2005, pp. 577-585.
- [3] E. Brickell. Some ideal secret sharing schemes, *J. of Comb. Math. and Comb. Computing* 9, 1989, pp. 105-113.
- [4] E. Brickell, D. Davenport, On the classification of ideal secret sharing schemes, *J. of Cryptology*, 4, 1991, pp. 123-134.
- [5] A. Beimel, A. Gal, M. Paterson. Lower Bounds for Monotone Span Programs. *FOCS'95*, 1995.
- [6] M. Ben-Or, S. Goldwasser, A. Wigderson. Completeness theorems for Non-Cryptographic Fault-Tolerant Distributed Computation, *STOC'88*, 1988, pp. 1-10.

- [7] G. Blakley, G. Kabatianskii. Linear Algebra Approach to Secret Sharing Schemes, LNCS 829, 1994, pp. 33-40.
- [8] R. Cramer. Introduction to Secure Computation, *Lectures on Data Security – Modern Cryptology in Theory and Practice*, LNCS 1561, 1999, pp. 16-62.
- [9] D. Chaum, C. Crepeau, I. Damgard. Multi-Party Unconditionally Secure Protokols, *STOC'88*, 1988, pp. 11-19.
- [10] M. van Dijk. Secret Key Sharing and Secret Key Generation, *Ph.D. Thesis*, TU Eindhoven, 1997.
- [11] M. van Dijk, W.-A. Jackson, K. Martin, A note on duality in linear secret sharing scheme, *Bull. of the Inst. of Comb. and its Appl.*, 19, 1997, pp. 93-101.
- [12] S. Fehr, U. Maurer. Linear VSS and Distributed Commitments Based on Secret Sharing and Pairwise Checks, *CRYPTO'02*, LNCS 2442, 2002, pp. 565-580.
- [13] W. -A. Jackson, K. Martin. Geometric Secret Sharing Schemes and Their Duals, *Desings Codes and Cryptography*, 4, 1994, pp. 83-95.
- [14] W. -A. Jackson, K. Martin, C. O'Keefe. Geometrical contributions to secret sharing theory, *Journal of Geometry*, 79, 1-2, 2004, pp. 102-133.
- [15] M. Karchmer, A. Wigderson. On Span Programs, *Proc. of 8th Annual Structure in Complexity Theory Conference*, 1993, pp. 102-111.
- [16] J. Massey. Minimal codewords and secret sharing, *Proc. 6th Joint Swedish-Russian Int. Workshop on Inform. Theory*, 1993, pp. 276-279.
- [17] U. Maurer. Secure Multi-Party Computation Made Simple, *SCN'02*, LNCS 2576, 2003, pp. 14-28.
- [18] R. McEliece, D. Sarwate. On sharing secrets and Reed-Solomon codes, *Commun. ACM* 24, 1981, pp. 583-584.
- [19] F. MacWilliams, N. Sloane. The Theory of Error-Correcting Codes, *Elsevier Science, Amsterdam*, 1988.
- [20] V. Nikov. Verifiable Secret Sharing and Applications, *Ph.D. Thesis*, TU Eindhoven, 2005.
- [21] V. Nikov, S. Nikova, B. Preneel, J. Vandewalle. Applying General Access Structure to Proactive Secret Sharing Schemes, *Proc. of the 23rd Symposium on Information Theory in the Benelux*, 2002, pp. 197-206, *Cryptology ePrint Archive*: Report 2002/141.
- [22] V. Nikov, S. Nikova, B. Preneel. On the Size of Monotone Span Programs, *SCN'04*, LNCS 3352, 2004, pp. 252-265.
- [23] V. Nikov, S. Nikova. On a Relation between Verifiable Secret Sharing Schemes and a class of Error-Correcting Codes, *WCC'05*, Bergen, Norway, 2005, pp. 372-382, *Cryptology ePrint Archive*: Report 2003/210,.

- [24] A. Shamir. How to share a secret, *Commun. ACM* 22, 1979, pp. 612-613.
- [25] H. Whitney. On the Abstract Properties of Linear Dependence, *American J. of Math.*, 57, 1935, pp. 509-533.
- [26] D. Welsh, *Matroid Theory*, Academic Press, London, 1976.