## 9. Conclusion

In the present chapter we only briefly touched upon a few questions related to number-theoretic algorithms and their complexity estimates. We said nothing about a promising research in expanding sieve algorithms to algebraic number fields (number field sieves) and their applications to integer factorizing or discrete logarithm computing; see [**48**]. These are precisely the algorithms that give the upper estimate

$$\exp(c(\log N)^{1/3}(\log\log N)^{2/3})$$

for the factorization problem. We have not mentioned elliptic curves, that is, sets of the form

$$E_{a,b} = \{(x, y, z) \in (\mathbb{Z}/m\mathbb{Z})^3 \mid y^2z = x^3 + axz^2 + bz^3\}$$

well defined up to an invertible common factor; these sets are endowed with a natural group structure. They can be used to construct rather efficient algorithms for integer factorizing and primality verification. In contrast to the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^*$, the order of the group $E_{a,b}$ depends on $a$ and $b$, and it may be different for the same value of $m$. This property turns out to be very useful, say, when factorizing $m$. Details on the usage of elliptic curves can be found in [**46**].

Chapter 5

# Mathematics of Secret Sharing

## 1. Introduction

Consider the following, now standard, situation. Two people jointly own a piece of jewelry and want to put it into a safe deposit box. The modern safe deposit box has a 16-digit numeric code. Since the owners do not trust each other, they would like to lock the box in a way that would allow them to open it together, but not separately. To reach this goal, they invite a third person (a *dealer*) whom they both trust (say, because he will not have access to the box in the future). The dealer chooses a random sequence of 16 digits as the "key", closes the safe, and then passes the first 8 digits to the first owner and the last 8 digits to the second owner. From the point of view of common sense, this method seems to be optimal. Indeed, each owner receives "half the key". However, each of the owners left alone with the safe can find the half of the key he misses using a simple device searching through keys with frequency 1 MHz. It seems that the only way to improve the situation is to double the length of the key. Fortunately (in this case), mathematics suggests a different approach, which contradicts common sense. Namely, the dealer chooses two random sequences of 16 digits each, one for each of the owners, and calculates the key sequence by adding the respective

digits of these two sequences modulo 10. It is more or less obvious (and we are going to prove this below) that all $10^{16}$ "keys" have the same probability for each of the owners, and the only way to find them is to search through all of them, which would require, in average, about a year and a half if we have a device generating keys with frequency 100 MHz.

The case of two participants is not sufficiently general from theoretical or practical point of view. Informally speaking, a "secret sharing scheme" (SSS) allows one to distribute a secret among $n$ participants in such a way that only some admissible sets of participants would be able to reconstruct the secret, while any other set would not produce any additional information about the secret except for that known from the very beginning. (The tuple of admissible sets is called the access structure.) Such SSS's are called *perfect*, and we consider only perfect SSS's in the present chapter.

The history of SSS's starts in 1979, when this problem was posed and essentially solved by Blakley [**9**] and Shamir [**60**] for the case of so-called threshold $(n,k)$-SSS's (in this case all subsets of at least $k$ elements are admissible). The so-called ideal SSS's are of the main interest; these are the SSS's such that the amount of information received by a participant is not greater than the "size" of the secret (we have already seen that this amount cannot be smaller). It turned out [**14**] that a matroid is associated to any such SSS (see the definition of a matroid in Section 4), and therefore, not each access structure determines an ideal secret sharing. On the other hand, it was shown that there exists a perfect SSS for each tuple of admissible sets, although the ways of constructing such an SSS are rather "inefficient". In the present chapter we discuss some algebro-geometric and combinatorial problems arising in the analysis of secret sharing schemes. Let us start with an example of such a problem.

We say that a family $(L_0,\dots,L_n)$ of subspaces of a finite-dimensional vector space $L$ over a field $K$ satisfies the "everything or nothing" property if for each subset $A\subset\{1,\dots,n\}$ the span of the subspaces $\{L_a, a\in A\}$ either contains the subspace $L_0$, or intersects $L_0$ only at $0\in L_0$. We are going to show in Section 3 that a family with this property determines a "linear" SSS such that a set $A\subset\{1,\dots,n\}$



is admissible if and only if the span of the subspaces $\{L_a, a\in A\}$ contains $L_0$. A number of questions arises in connection with this notion. Suppose, for example, that the field $K$ is finite, $|K|=q$, and all subspaces $\{L_0,\dots,L_n\}$ are one-dimensional; then what is the maximum number $n$ of participants for linear threshold $(n,k)$-SSS's for a given $k>1$? In other words, what is the maximum number of vectors $\{h_0,\dots,h_n\}$ such that any $k$ vectors whose span contains $h_0$ are linearly independent, while any $k+1$ vectors with the same property are linearly dependent? It happens that this property is equivalent to the following one, which looks stronger, at least at first glance: any $k$ vectors are linearly independent, while any $k+1$ vectors are linearly dependent. Such systems of vectors were studied under the name of $N$-sets ($N=n+1$) in finite projective geometry $PG(k-1,q)$, under the name of orthogonal tables of strength $k$ and index $\lambda=1$ in combinatorics, and under the name of verification matrices for the MDR-code in the coding theory (see details in [**49**]). In Section 3 we present a well-known construction of such sets with $N=q+1$, and a rather old conjecture states that this value of $N$ is exactly the maximum one except for two cases: the case of $q<k$, where $N=k+1$, and the case of $q=2^m$ and $k=3$ or $k=q-1$, where $N=q+2$.

## 2. Secret sharing for arbitrary access structures

Let us start with a formal mathematical model. Suppose we have $n+1$ sets $\mathcal{S}_0,\mathcal{S}_1,\dots,\mathcal{S}_n$ and a (joint) probability distribution $P$ on the direct product $\mathcal{S}=\mathcal{S}_0\times\cdots\times\mathcal{S}_n$. Denote the corresponding random values by $S_i$. A set $\Gamma$ of subsets of $\{1,\dots,n\}$, called the access structure, is also given.

**Definition 1.** A pair $(P,\mathcal{S})$ is called a *perfect probabilistic SSS* realizing the access structure $\Gamma$ if

(1) $$P(S_0=c_0 \mid S_i=c_i, i\in A)\in\{0,1\} \text{ for } A\in\Gamma,$$

(2) $$P(S_0=c_0 \mid S_i=c_i, i\in A)=P(S_0=c_0) \text{ for } A\notin\Gamma.$$

This definition can be interpreted as follows. There is a set $\mathcal{S}_0$ of all possible secrets; a secret $s_0\in\mathcal{S}_0$ is chosen with probability $p(s_0)$; and there is an SSS that "distributes" the secret $s_0$ among

$n$ participants by sending "projections" $s_1, \ldots, s_n$ of the secret with probability $P_{s_0}(s_1, \ldots, s_n)$. Note that the $i$th participant gets the projection $s_i \in \mathcal{S}_i$, but receives no information about the values of other projections, although he knows all sets $\mathcal{S}_i$ as well as both probability distributions $p(s_0)$ and $P_{s_0}(s_1, \ldots, s_n)$. These two distributions can be replaced with the single distribution $P(s_0, s_1, \ldots, s_n) = p(s_0)P_{s_0}(s_1, \ldots, s_n)$, see above. As was pointed out in the Introduction, the goals of SSS's are:

a) to allow the participants forming an admissible set $A$ (that is, a set $A \in \Gamma$) together reconstruct the value of the secret (property (1));

b) to prevent participants forming a nonadmissible set $A$ ($A \notin \Gamma$) from obtaining additional information about $s_0$; this means that the probability of reconstructing the secret value $S_0 = c_0$ must be independent of the "projections" $S_i$ for $i \in A$ (property (2)).

*A terminology remark.* The "parts" of information sent to a participant of an SSS are called "shares" by Shamir and "shadows" by Blakley. The first name became the most popular one. The following example justifies the term "projection".

**Example 1.** Suppose the set $\mathcal{S}_0$ of all possible secrets is the set $\{0, 1, 2\}$ and the elements of this set are represented by a ball, a cube with edges parallel to the coordinate axes, and a cylinder with axis parallel to the $z$-axis. We assume that the diameter of the ball, the diameter of the cross section and the height of the cylinder, and the edge length of the cube, are all identical. The "part" of the first participant is the projection of the secret to the plane $XY$, while the "part" of the second is the projection to the plane $XZ$. Of course, the participants can reconstruct the secret together, but they are unable to do this separately. However, this SSS is not perfect since each of the participants gets some information about the secret: only two bodies from the given three can produce a given projection (say, if the projection is a square, then the projected body cannot be the ball).

**One more remark.** An element $x \in \{1, \ldots, n\}$ (a participant) is called *inessential* (with respect to the given $\Gamma$) if for an arbitrary nonadmissible set $A$ the set $A \cup \{x\}$ is nonadmissible either. Obviously, there is no need to send any information to inessential participants. Therefore, without loss of generality, we consider only access



structures $\Gamma$ such that all elements are essential for them. Besides, it is natural to assume that $\Gamma$ is a monotonic structure, that is, the assumptions $A \subset B$ and $A \in \Gamma$ imply that $B \in \Gamma$.

**Example 2.** Consider the simplest access structure, the $(n, n)$-threshold scheme; this means that all $n$ participants together can reconstruct the secret, while an arbitrary proper subset of participants cannot obtain additional information about the secret. Let us try to construct an ideal SSS by choosing a secret and its projections from the set $\mathbb{Z}_q$ of residues modulo $q$, i.e., we set $\mathcal{S}_0 = \mathcal{S}_1 = \cdots = \mathcal{S}_n = \mathbb{Z}_q$. The dealer generates $n$ independent random values $x_i$ uniformly distributed over $\mathbb{Z}_q$ and sends to the $i$th participant ($i = 1, \ldots, n-1$) its "projection" $s_i = x_i$, while to the $n$th participant he sends the value $s_n = s_0 - (s_1 + \cdots + s_{n-1})$. The illusory "discrimination" of the $n$th participant disappears if we look at the distribution value $P_{s_0}(s_1, \ldots, s_n)$, which obviously is $1/q^{n-1}$ if $s_0 = s_1 + \cdots + s_n$, and is 0 otherwise. Now it is easy to verify property (2), which means, in this case, that the random value $S_0$ is independent of the random values $\{S_i : i \in A\}$ for an arbitrary proper subset $A$.

The definition of SSS given above uses the term "probability distribution". Below we give an almost equivalent combinatorial definition, which seems to be easier to understand. An arbitrary $M \times (n+1)$-matrix $V$ with rows of the form $\mathbf{v} = (v_0, v_1, \ldots, v_n)$, $v_n \in \mathcal{S}_i$, is called the matrix of a combinatorial SSS, and its rows are called the "rules" for secret sharing. For a given value $s_0$ of the secret, the SSS dealer chooses randomly a row $\mathbf{v}$ with equal probability from the set of rows of $V$ with the first element $s_0$.

**Definition 2.** A matrix $V$ determines a *perfect combinatorial SSS* which realizes an access structure $\Gamma$ if, first, for each set $A \in \Gamma$ the zero coordinate of each row of the matrix $V$ is uniquely determined by the values of the coordinates in this row with indices in $A$ and, second, for each set $A \notin \Gamma$ and arbitrary given values of coordinates with indices in $A$ the number of rows of $V$ with prescribed value $\alpha$ of the zero coordinate is independent of $\alpha$.

To a perfect probabilistic SSS given by a pair $(P, \mathcal{S})$ we associate the matrix $V$ whose rows $s \in \mathcal{S}$ are such that $P(s) > 0$. Note that

if we set all nonzero values of $P$ in Definition 1 equal to each other and reformulate conditions (1) and (2) in the combinatorial language, then we obtain Definition 2. This combinatorial definition can be generalized slightly if we allow identical rows in the matrix $V$. The generalized definition is equivalent to Definition 1 with rational values of the probabilities $P(s)$.

**Example 2 (continued).** Let us reformulate the construction of an $(n, n)$-threshold SSS above in the combinatorial language. The rows of the matrix $V$ are all vectors $\mathbf{s}$ such that $-s_0 + s_1 + \cdots + s_n = 0$. Obviously, the matrix $V$ determines a perfect combinatorial SSS for $\Gamma = \{1, \ldots, n\}$ since for any proper subset $A \subset \{1, \ldots, n\}$ and arbitrary given values of coordinates in the set $A$ the number of rows of $V$ with a given value of the zero coordinate is $q^{n-1-|A|}$.

Although this seems strange, but using the simple scheme of Example 2 as the main block, we can construct a perfect SSS for arbitrary access structure. Namely, we can realize the threshold $(|A|, |A|)$-SSS described above independently for all admissible sets, that is, for $A \in \Gamma$, and send to the $i$th participant the projections $s_i^A$ for each set $A$ he belongs to. It is easy to translate this informal description into the combinatorial language of properties of $V$ and verify that this SSS is perfect. As it often happens, the word "perfect" does not mean "efficient", and the size of the "projection" in this SSS is usually much greater than the size of the secret. This scheme can be made much more efficient since it suffices to realize the threshold $(|A|, |A|)$-SSS's only for the minimal admissible sets $A$, i.e., for $A \in \Gamma_{\min}$, where $\Gamma_{\min}$ is the set of all minimal (with respect to inclusion) sets from $\Gamma$. Nevertheless, the size (say, in bits) of the "projection" for a threshold $(n, n/2)$-SSS is $\binom{n}{n/2} \sim 2^n/\sqrt{2\pi n}$ times larger than the size of the secret (this is the worst case for the above construction). On the other hand, as we are going to verify later, any threshold access structure admits an ideal realization, i.e., it can be realized as an SSS with the same sizes of the secret and the "projections". Thus, the problem arises, what is the maximum possible ratio of the size of the "projection" and the size of the secret for the worst access structure with the best implementation? Formally, we set $R(n) = \max R(\Gamma)$, where the maximum is taken over all access structures with $n$ participants, and



$R(\Gamma) = \min \max \frac{\log |S_i|}{\log |S_0|}$, where the minimum is taken over all SSS's realizing the given access structure $\Gamma$, and the maximum is taken over all $i = 1, \ldots, n$. The above construction shows that $R(n) \le \binom{n}{n/2}$. On the other hand, it was proved recently in [**23**] that $R(n) \ge n/\log n$. Such a huge gap between the upper and lower estimates gives further research full scope (we conjecture that $R(n)$ grows exponentially in $n$).

## 3. Linear secret sharing

We start with the elegant secret sharing scheme for threshold access structures suggested by Shamir [**60**]. Let $K = \mathbb{F}_q$ be the finite field of $q$ elements (for example, we can assume that $q = p$ is a prime number, and $K = \mathbb{Z}_p$) and take $n < q$. We assign to each of the $n$ participants nonzero elements $\{a_1, \ldots, a_n\}$ of the field, and set $a_0 = 0$. When sharing a secret, the dealer of the SSS generates $k-1$ independent random values $f_j$ $(j = 1, \ldots, k-1)$ uniformly distributed over $\mathbb{F}_q$ and sends the value $s_i = f(a_i)$ to the $i$th participant; here $f$ is the polynomial $f(x) = f_0 + f_1 x + \cdots + f_{k-1}x^{k-1}$, where $f_0 = s_0$. Since an arbitrary polynomial of degree $k-1$ can be uniquely reconstructed from its values at arbitrary $k$ points (say, by the Lagrange interpolation formula), any $k$ participants together can reconstruct the polynomial $f$ and find the secret as the value $s_0 = f(0)$. For the same reason, for arbitrary $k-1$ participants, arbitrary values $s_i$ of the projections they receive, and an arbitrary secret $s_0$, there is exactly one polynomial $f$ such that $s_i = f(a_i)$ for all $i$. Hence, this scheme is perfect, by Definition 2. The "linearity" of this scheme becomes obvious if we write the secret sharing in the matrix form:

$$\mathbf{s} = \mathbf{f}H, \tag{3}$$

where $\mathbf{s} = (s_0, \ldots, s_n)$, $\mathbf{f} = (f_0, \ldots, f_{k-1})$, the $k \times (n+1)$-matrix $H$ has the form $H = (h_{ij}) = (a_i^{j-1})$ and $h_{00} = 1$. Note that any $k$ columns of this matrix are linearly independent, and the maximum possible number of columns of $H$ is $q$; in order to reach the value $q+1$ promised in Section 1 we must add the column corresponding to the point at infinity.

**Exercise.** Figure out how this can be done.

Let us take, for $H$ in (3), an arbitrary $r \times (n+1)$-matrix with elements from $K$. We call the resulting SSS a *linear one-dimensional SSS*. It is a perfect combinatorial SSS with the access structure $\Gamma$ consisting of sets $A$ such that the vector $\mathbf{h}_0$ can be expressed as a linear combination of the vectors $\{\mathbf{h}_j : j \in A\}$, where $\mathbf{h}_j$ is the $j$th column of the matrix $H$. We see from (3) that the rows of the matrix $V$ corresponding to this SSS are linear combinations of the rows of $H$. Let us rewrite (3) in the form

$$s_j = (\mathbf{f}, \mathbf{h}_j) \text{ for } j = 0, 1, \ldots, n,$$

where $(\mathbf{f}, \mathbf{h}_j)$ is the inner product of the vectors $\mathbf{f}$ and $\mathbf{h}_j$. If $A \in \Gamma$, i.e., $\mathbf{h}_0 = \sum \lambda_j \mathbf{h}_j$, then

$$s_0 = (\mathbf{f}, \mathbf{h}_0) = (\mathbf{f}, \sum \lambda_j \mathbf{h}_j) = \sum \lambda_j (\mathbf{f}, \mathbf{h}_j) = \sum \lambda_j s_j,$$

whence the value of the secret can be uniquely reconstructed from its "projections". Now suppose the vector $\mathbf{h}_0$ cannot be presented as a linear combination of the vectors $\{\mathbf{h}_j : j \in A\}$. We want to show that in this case for arbitrary given values of the coordinates from the set $A$, the number of rows of the matrix $V$ with a prescribed value of the zero coordinate is independent of this value. This can be easily verified if we treat equation (3) as a system of linear equations with respect to the variables $f_i$ and use the fact that the system is compatible if and only if the rank of the matrix of coefficients is equal to the rank of the extended matrix of coefficients and all compatible systems have the same number of solutions, which coincides with the number of solutions of a homogeneous system.

*Hint.* Consider two systems: one without the "zero equation" (that is, without the free term), and the other with it. Since the vector $\mathbf{h}_0$ cannot be represented as a linear combination of the vectors $\{\mathbf{h}_j : j \in A\}$, the rank of the coefficient matrix of the second system exceeds the rank of the coefficient matrix of the first system by one. This fact implies immediately that if the first system is compatible, then the same is true for the second system for an arbitrary $s_0$ as well.

This construction suggests the following definition of a general linear SSS. Suppose the secret and its "projections" are represented as



finite-dimensional vectors $\mathbf{s}_i = (s_i^1, \ldots, s_i^{m_i})$ produced by the formulas $\mathbf{s}_i = \mathbf{f}H_i$, where $H_i$ are some $r \times m_i$-matrices. Associate to each matrix $H_i$ the vector space $L_i$ spanned by its columns (i.e., the space of linear combinations of the column vectors of $H_i$). An easy argument similar to that for the one-dimensional case above (all $m_i = 1$) shows that this construction leads to a perfect SSS if and only if the family of vector subspaces $\{L_0, \ldots, L_n\}$ of the finite-dimensional vector space $K^r$ possesses the "everything or nothing" property mentioned in the Introduction. Then the set $A$ is admissible ($A \in \Gamma$) if and only if the span of the spaces $\{L_a : a \in A\}$ contains the entire space $L_0$. On the other hand, the set $A$ is nonadmissible ($A \notin \Gamma$) if and only if the span of the subspaces $\{L_a : a \in A\}$ intersects $L_0$ merely in the origin. Note that were the intersection of $L_0$ with the span of $\{L_a : a \in A\}$ nontrivial for some $A$, the participants of $A$ would be able to obtain some additional information about $A$, which nevertheless would not allow them to reconstruct the secret; this means, of course, that the scheme would not be perfect.

**Example 3.** Consider the access structure $\Gamma_{\min} = \{\{1,2\}, \{2,3\}, \{3,4\}\}$ for four participants. This was the first example of an access structure without an ideal realization. Moreover, it was proved that $R(\Gamma) \geq 3/2$ for an arbitrary perfect realization of this structure. On the other hand, it can be verified directly that the matrices $H_0, H_1, \ldots, H_4$ in Table 1 determine a perfect linear SSS with $R = 3/2$, which realizes this structure. Therefore, this SSS is optimal (most efficient).

## 4. Ideal secret sharing and matroids

We start with the definition of an ideal SSS. Let us return to the definition of a perfect SSS. The following definition of a perfect SSS from [**14**] is even more general than the probabilistic Definition 1 since the property (2) is replaced there with a weaker one.

For an arbitrary set $B \subseteq \{0, 1, \ldots, n\}$, we denote by $V_B$ the $M \times |B|$-matrix obtained from $V$ by selecting the columns with indices belonging to $B$. Denote the number of pairwise distinct rows in a matrix $W$ by $\|W\|$.

**Table 1**

$$H_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad H_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad H_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

$$H_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad H_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

**Definition 3.** A matrix $V$ determines a BD-perfect[1] SSS realizing an access structure $\Gamma$ if

$$\|V_{A\cup\{0\}}\| = \|V_A\| \cdot \|V_0\|^{\delta_\Gamma(A)}, \tag{4}$$

where $\delta_\Gamma(A) = 0$ if $A \in \Gamma$, and $\delta_\Gamma(A) = 1$ otherwise.

The assumption on nonadmissible sets $A$ in this definition is much weaker than that in Definitions 1 and 2; namely, we require that if the set of rows of $V$ with given values of coordinates belonging to $A$ is nonempty, then the zero coordinate of these rows must take all possible values of the secret (without requiring "with the same multiplicity" as in the combinatorial Definition 2, or "with the same a probability" as in the probabilistic Definition 1). It is easy to show that the matrix of an arbitrary perfect probabilistic SSS determines a BD-perfect SSS, but the converse is false.

For an arbitrary combinatorial SSS given by a matrix $V$, let us consider on sets $A \subseteq \{0, 1, \ldots, n\}$ the function $h(A) = \log_q \|V_A\|$, where $q = |\mathcal{S}_0|$. It can be easily verified that $\max\{h(A), h(B)\} \le h(A \cup B) \le h(A) + h(B)$ for any two sets $A$ and $B$, and condition (4)

[1]The letters BD here stand for Brickell and Davenport who suggested this notion. (*Added in translation.*)



can be rewritten in the form

$$h_q(V_{A\cup\{0\}}) = h_q(V_A) + \delta_\Gamma(A) h_q(V_0).$$

**Lemma.** *For any BD-perfect SSS, the following holds: if $A \notin \Gamma$ and $\{A \cup i\} \in \Gamma$, then*

$$h(i) \ge h(0).$$

**Proof.** By the assumptions of the lemma, $h(A \cup \{0\}) = h(A) + h(0)$, and $h(A \cup \{i\} \cup \{0\}) = h(A \cup \{i\})$. Therefore,

$$\begin{aligned} h(A) + h(i) &\ge h(A \cup \{i\}) = h(A \cup \{i\} \cup \{0\}) \\ &\ge h(A \cup \{0\}) = h(A) + h(0). \end{aligned}$$

□

Since we assumed that all elements $i \in \{1, \ldots, n\}$ are essential, i.e., for any $i$ there is a subset $A$ such that $A \notin \Gamma$ and $\{A \cup \{i\}\} \in \Gamma$, the lemma immediately implies the following

**Corollary.** *For an arbitrary BD-perfect SSS we have $|\mathcal{S}_i| \ge |\mathcal{S}_0|$ for all $i = 1, \ldots, n$.*

This corollary means that, as we already mentioned at the beginning of the chapter, the "size" of a projection for perfect SSS's cannot be less than the "size" of the secret. That is why a BD-perfect SSS is called ideal if $|\mathcal{S}_i| = |\mathcal{S}_0|$ for all $I = 1, \ldots, n$.

**Remark.** The inequality $|\mathcal{S}_i| \ge |\mathcal{S}_0|$ is valid for perfect probabilistic SSS's as well since their matrices determine BD-perfect SSS's.

Now we have the following natural question: what are the access structures $\Gamma$ such that there exist ideal (either probabilistic or combinatorial) SSS's realizing them? As was already mentioned in the introduction, the best currently known answer uses the notion of a matroid. Recall the definition of a matroid and some properties of these objects.

A *matroid* is a finite set $X$ together with a family $I$ of its subsets which are called independent (all other subsets are dependent),

satisfying the following conditions:

$(5_1)$ $\quad \emptyset \in I;$

$(5_2)$ $\quad$ if $A \in I$ and $B \subset A$, then $B \in I;$

$(5_3)$ $\quad$ if $A, B \in I$ and $|A| = |B| + 1$, then there exists $a \in A \setminus B$ such that $a \cup B \in I$.

**Example 4.** The set $X$ is a set of vectors in a vector space, while an independent subsets are the subsets of linearly independent vectors.

The theory of matroids started, in fact, with this example as an attempt to formalize "intrinsic" properties of linear dependence. Fortunately, this attempt failed since there are matroids that cannot be realized in this way (i.e., as systems of vectors), and the theory of matroids spread far beyond linear algebra; see [**64**].

**Example 5** (Vamos matroid)**.** Consider the set $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and put $a = \{1, 2\}$, $b = \{3, 4\}$, $c = \{5, 6\}$, and $d = \{7, 8\}$. In the Vamos matroid, all sets $a \cup c$, $a \cup d$, $b \cup c$, $b \cup d$, $c \cup d$, as well as all sets containing 5 or more elements, are dependent, while all other subsets of $X$ are independent. It is known that this matroid is not linear.

Matroids can also be defined using the so-called rank functions. The rank function of a matroid is the function $r$ on the subsets of $X$ whose value on a set $A \subset X$ is equal to the maximal cardinality of an independent subset $B \subseteq A$. Obviously, $r(A) = |A|$ exactly on independent subsets. The rank function has the following properties:

$(6_1)$ $\quad r(A) \in \mathbb{Z}, \quad r(\emptyset) = 0;$

$(6_2)$ $\quad r(A) \le r(A \cup \{b\}) \le r(A) + 1;$

$(6_3)$ $\quad$ if $r(A \cup \{b\}) = r(A \cup \{C\}) = r(A)$, then $r(A \cup \{b\} \cup \{c\}) = r(A)$.

Conversely, suppose a function $r$ possesses properties $(6_1)$–$(6_3)$. We declare the subsets $A$ such that $r(A) = |A|$ independent. Then these subsets determine a matroid, and $r$ is the rank function for this matroid. It is also possible to define a matroid in terms of minimal dependent subsets, called *cycles*. A matroid is called *connected* if



for any pair of its elements there is a cycle containing both these elements.

Now we can formulate the main result.

**Theorem** (see [**14**])**.** *For a BD-perfect SSS realizing an access structure $\Gamma$ the independent sets defined by the condition $\log_{|S_0|} \|V_A\| = |A|$ determine a connected matroid on the set $\{0, 1, \dots, n\}$. All cycles of this matroid containing the element 0 have the form $\{0\} \cup A$, where $A \in \Gamma_{\min}$.*

The main step in the proof of this theorem is the "verification" of the fact that the function $h(\cdot)$ takes integer values. Indeed, the other properties $(6_1)$–$(6_3)$ are obvious for $h$, whence it determines a matroid provided it takes integer values. The proof of the theorem and of some more general statements can be found in [**10**].

Note that the second part of the theorem implies that distinct ideal SSS's realizing the same access structure are always associated to the same matroid since the matroid is uniquely determined by all cycles passing through a given element (see [**64**]). Hence, a matroid is associated to each access structure admitting an ideal realization, and this matroid is unique.

A number of natural questions arise in connection with this theorem. First of all, do the ideal SSS's generate all matroids? The answer is negative; indeed, the Vamos matroid cannot be obtained as the matroid of an ideal SSS [**59**]. On the other hand, linear matroids are precisely the ideal one-dimensional linear SSS's studied in Section 3. Now we can ask whether there is an access structure $\Gamma$ that cannot be realized by an ideal one-dimensional SSS, but admits an ideal multidimensional linear SSS realization. Such an example was constructed recently in [**6**], whence the class of multidimensional linear matroids is more general than that of one-dimensional linear matroids.

Thus, the class of ideal SSS's contains the class of linear matroids, but there are matroids that cannot be realized by ideal SSS's. To analyze the differences between these classes seems to be a complicated task. In particular, does there exist an access structure $\Gamma$ that

admits an ideal realization but cannot be realized by an ideal linear multidimensional SSS?

Chapter 6

# Cryptography Olympiads for High School Students

## 1. Introduction

Suppose you want to send a message to a receiver in such a way that its contents remains secret to anybody else. There are at least two possible ways to do this. First, you may try to use methods related to *steganography* (invisible ink, microphotographs, etc.), i.e., to conceal the very existence of a secret message. The other possibility is to disguise the meaning of the message so that an unauthorized person who just occasionally or deliberately reads your message cannot understand it. In this case you can use the methods of cryptography. The word *cryptography* stems from the two Greek roots: "$\kappa\rho\upsilon\pi\tau o\varsigma$", secret, and "$\gamma\rho\alpha\varphi\omega$", to write. Thus *cryptography* is the art of disguising the substance of a message. The message that you want to transmit to the receiver is called the *plaintext*. For example, in Problem 2.5 (in the Problems section) one of the plaintexts is THEREARETWOQUESTIONSLEFT. To keep the message a secret it is transformed, by using a method of cryptography, before transmission. The transformed message is called a *ciphertext* or a *cryptogram*.