On secret sharing protocols

Chi Sing Chum, Benjamin Fine, Anja I. S. Moldenhauer, Gerhard Rosenberger, and Xiaowen Zhang

Abstract. Sharing a secret among \( n \) participants in such a way that any \( t \) of them but not less can access the secret is an extremely important cryptographic protocol. A beautiful solution to the general secret sharing problem was given by Shamir [Sh] and this has become the gold standard for secret sharing protocols yet there are continual improvements. In this paper, partly expository and partly research we examine many different cryptographic protocols and make some basic comparisons. We then introduce three new methods that are part of the Ph.D. thesis of A. Moldenhauer [M]. The first one is a combinatorial method while the second uses combinatorial group theory in particular Nielsen transformations. The last one applies similar techniques using solutions of the Hurwitz equation.

Contents

1. Introduction
2. The Shamir Secret Sharing Scheme
3. Alternatives for Secret Sharing Protocols
4. Comparison of Secret Sharing Protocols
5. Verifying Secret Sharing Protocols (VSS)
7. A Variation of the Secret Sharing Scheme based on Nielsen Transformations
8. A Secret Sharing Protocol based on the Hurwitz Equation
References

1. Introduction

A cryptographic protocol consists of the collection of rules, formulas and methods to handle a cryptographic task. Extremely important along these lines are secret sharing protocols. These consist of methods to distribute a secret among a group of users by giving a share of the secret to each. The secret can be recovered only if a sufficient number of users (but perhaps not all) combine their pieces.

2010 Mathematics Subject Classification. Primary 20F67; Secondary 20F65, 20E06, 20E07.

Key words and phrases. Secret sharing protocol, Shamir scheme, verifiable secret sharing scheme, Nielsen transformations, polynomial interpolation, closest vector theorem.

©2016 American Mathematical Society
Formally we have the following. We have a secret $P$ and a group of $n$ participants. This group is called the access control group. A dealer allocates shares to each participant under given conditions. If a sufficient number of participants combine their shares then the secret can be recovered. If $t \leq n$ then an $(t, n)$-threshold scheme is one with $n$ total participants and in which any $t$ participants can combine their shares and recover the secret but not fewer than $t$. The number $t$ is called the threshold. It is a secure secret sharing scheme if given less than the threshold there is no chance to recover the secret. If a measure is placed on the set of secrets, and on the set of shares, security can be made precise by saying that given less than the threshold all secrets are equally likely but given the threshold there is a unique secret. Secret sharing is an old idea but was formalized mathematically in independent papers in 1979 by Adi Shamir and George Blakley.

In the 1979 paper, Shamir proposed a beautiful $(t, n)$-threshold scheme, based on polynomial interpolation, that has many desirable properties. We describe this in the next section. It is now the standard method for solving the $(t, n)$-secret sharing problem, although there are modifications for different situations (see [CFZ]). Blakely in his original paper proposed a geometric solution that is less space efficient, for computer storage, than Shamir’s. In Blakely’s scheme the distributed shares are larger than the secret, whereas in Shamir’s scheme they are the same size. In this paper, which is part expository and part research, we look at many aspects of the secret sharing problem. We introduce two new secret sharing protocols, one based on combinatorial group theory and in particular on Nielsen transformations and one based on number theory. We consider the expository sections to be an excellent introduction to the whole area.

There are many different motivations for the secret sharing problem. One of the most important is the problem of maintaining sensitive information. There are two crucial issues here: availability and secrecy. If only one person keeps the entire secret, then there is a risk that the person might lose the secret or the person might not be available when the secret is needed. Hence it is often useful to utilize several people in order to access a secret. On the other hand, the more people who can access the secret, the higher the chance the secret will be leaked. By sharing a secret in a threshold scheme the availability and reliability issues can be addressed. The paper by Chum, Fine and Zhang contains a wealth of information on secret sharing in general and managing an access control group.

2. The Shamir Secret Sharing Scheme

Given a secret $K$, a $(t, n)$-secret sharing threshold scheme is a cryptographic primitive in which a secret is split into pieces (shares) and distributed among a collection of $n$ participants $\{p_1, p_2, \ldots, p_n\}$ so that any group of $t$ or more participants, with $(t \leq n)$, can recover the secret. Meanwhile, any group of $t - 1$ or fewer participants cannot recover the secret. By sharing a secret in this way the availability and reliability issues can be solved.

Shamir solved the secret sharing problem in a very simple but beautiful manner using polynomial interpolation. The general idea in a Shamir $(t, n)$-threshold scheme is the following. Let $F$ be any field and $(x_1, y_1), \ldots, (x_n, y_n)$ be $n$ points in $F^2$ with pairwise distinct $x_i$. A polynomial $P(x)$ over $F$ interpolates these points if $P(x_i) = y_i$ for $i = 1, \ldots, n$. The polynomial $P(x)$ is called an interpolating polynomial.
polynomial for the given points. The crucial theoretical result is that for any \( n \) points \((x_i, y_i)\) with distinct \( x_i \) there always exists a unique interpolating polynomial of degree \( \leq n - 1 \).

**Theorem 2.1. (Polynomial Interpolation Theorem)** Let \( F \) be any field and \( x_1, \ldots, x_n \) be \( n \) pairwise distinct elements of \( F \) and \( y_1, \ldots, y_n \) any elements of \( F \). Then there exists a unique polynomial of degree \( \leq n - 1 \) that interpolates the \( n \) points \((x_i, y_i), i = 1, \ldots, n\).

Using this theorem the Shamir \((t, n)\)-threshold scheme works in the following manner. A field \( F \) with more than \( n \) elements is chosen. In general if \( F \) is a finite field we assume that the order of \( F \) is much much larger than \( n \), the number of participants. The secret \( K \) is taken as an element of the field \( F \) and a polynomial \( P(x) \) of degree \( t - 1 \) is chosen with the secret \( K \) as its constant term. Then pairwise distinct elements of \( F \), \( x_1, \ldots, x_n \), are chosen with no \( x_i = 0 \). The points \((x_i, P(x_i))\) are distributed to each of the \( n \) participants. By the polynomial interpolation theorem, given above, any \( t \) participants can determine the interpolating polynomial \( P(x) \) and hence recover the secret \( K \). Given an infinite field and less than \( t \) people there are infinitely many polynomials of degree \( t - 1 \) that can interpolate the given points and hence finding the correct polynomial has probability zero. In a finite field Shamir proved that under random choices for the \( x_i \) each secret in \( F \) is equally likely so guessing the secret is a random choice from \( F \).

In the next section an alternative version to this Shamir scheme will be outlined that uses inner product spaces and the closest vector theorem rather than interpolation.

We now present a more explicit version of the Shamir scheme using the finite field \( F = GF(q) \) where \( q = p^k \) with \( k \geq 1 \) and \( p \) is a large prime. By using a finite field Shamir was able to place a finite measure on the set of plaintexts and ciphertexts and showed that with this scheme if there are less than \( t \) people all secrets are equally likely.

**The Shamir \((t, n)\)-Threshold Secret Sharing Scheme**

**Share distribution:** Let \( K \) be the secret. The dealer generates a polynomial \( P(x) \) of degree at most \( t - 1 \) over \( F = GF(q) \), where \( q \) is much larger than \( n \) as follows:

\[
P(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}
\]

where \( a_0 = K \) is the secret, \( a_1, \ldots, a_{t-1} \in F \) and are generated randomly.

The dealer arbitrarily chooses pairwise distinct \( x_i \in F \setminus \{0\}, i = 1, 2, \ldots, n \). Usually, \( x_i = i \) will be chosen for simplicity. \( x_1, x_2, \ldots, x_n \) are stored in a public area. The dealer calculates \( y_i = P(x_i), i = 1, 2, \ldots, n \), and distributes to the \( n \) participants via a secure channel so that each participant \( p_i \) gets one share \( y_i \). For the rest of the paper, we will not repeat the criteria of the generation of the coefficient \( a_t \) of the polynomial \( P(x) \) and the calculation of the shares \( P(x_i) \).

**Secret Recovery (i):** When any \( t \) participants join together, we have the following system of \( t \) equations. For simplicity, we assume the participants \( p_1, p_2, \ldots, p_t \) join together.

\[
y_1 = P(x_1) = a_0 + a_1 x_1 + \cdots + a_{t-1} x_1^{t-1},
\]

\[
y_2 = P(x_2) = a_0 + a_1 x_2 + \cdots + a_{t-1} x_2^{t-1},
\]
..., $y_t = P(x_t) = a_0 + a_1 x_t + \cdots + a_{t-1} x_t^{t-1}$.

In matrix representation, it will be:

$$
\begin{pmatrix}
1 & x_1 & \cdots & x_1^{t-1} \\
1 & x_2 & \cdots & x_2^{t-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \cdots & \cdots & x_t^{t-1}
\end{pmatrix}
\begin{pmatrix}
a_0 \\
a_1 \\
\vdots \\
a_{t-1}
\end{pmatrix}
= 
\begin{pmatrix}
y_1 \\
y_2 \\
\vdots \\
y_t
\end{pmatrix}
$$

Let $M$ be the above $t \times t$ Vandermonde matrix. Its determinant is

$$
\det(M) = \prod_{1 \leq j < k \leq t} (x_k - x_j).
$$

Since we choose pairwise different points for the participants, that is, pairwise distinct $x_i$’s, $\det(M) \neq 0$, and this guarantees a unique solution. We can solve the system of equations by Gaussian elimination or Cramer’s rule. Hence the secret can be recovered.

**Secret Recovery (ii):** Another method is to use Lagrange interpolation. We can construct the polynomial of degree at most $t - 1$ by any $t$ different points $(x_1, y_1), \ldots, (x_t, y_t)$ as

$$
P(x) = \sum_{i=1}^{t} y_i l_i(x),
$$

where

$$
l_i(x) = \prod_{j=1, j \neq i}^{t} \frac{x - x_j}{x_i - x_j} = \frac{(x - x_1) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_t)}{(x_i - x_1) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_t)}.
$$

So, the secret $a_0$ will be

$$
a_0 = P(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{-x_j}{x_i - x_j}.
$$

Shamir in his original paper was able to prove that this secret sharing scheme is **perfect** in the sense that for $t - 1$ participants any secret $K \in F$ is equally likely. If $F$ is an infinite field, then the probability of correctly guessing the secret is zero.

**3. Alternatives for Secret Sharing Protocols**

In this section we describe several alternatives and enhancements to the Shamir Secret Sharing Scheme. The first alternative is a geometric method based on the closest vector theorem and introduced in [CFRZ]. It is similar to the original Blakely scheme but has the advantage that the secret is the same size as the shares. This was not the case in the Blakely protocol. This scheme, like the Shamir scheme, is also perfect in the sense that any $t$ people out of the size $n$ access control group can recover the secret but given less than $t$, then the participants have infinitely many subspaces of dimension $t$ at choice in which the secret could lie in. The probability to choose the right subspace is negligible. Therefore, each possible secret is equally likely. The use of the closest vector theorem is prominent in lattice based cryptography. We refer to [B] for a discussion of this.
The second alternative we discuss is due to Panagopoulos and is based on combinatorial group theory. In particular he uses the solution to the word problem in finitely presented groups.

The third alternative is a new protocol due to A. Moldenhauer and developed in her Ph.D. thesis. The distribution of shares employs a modification of the Panagopoulos technique.

The final alternative is due to C. Chum and X. Zhang and is based on latin squares.

3.1. A Method Based on the Closest Vector Theorem. The geometric alternative scheme depends on the closest vector theorem. Recall the following facts. Let $W$ be a real inner product space and $V$ a subspace of finite dimension $t$. Suppose that $w \in W$ and $e_1, e_2, \ldots, e_t$ is an orthonormal basis of $V$. Then the closest vector theorem is the following (see [A]).

**Theorem 3.1. Closest Vector Theorem.** Let $W$ be a real inner product space and $V$ a subspace of finite dimension $t$. Suppose that $w \in W$, with $w$ not in $V$, and $e_1, e_2, \ldots, e_t$ is an orthonormal basis of $V$. Then the unique vector $w^* \in V$ closest to $w$ is given by

$$w^* = <w, e_1 > e_1 + <w, e_2 > e_2 + \cdots + <w, e_t > e_t$$

where $< , >$ is the inner product on $W$.

Notice that given any basis for the subspace $V$, the Gram-Schmidt orthonormalization procedure (see [A]) can be used to find an orthonormal basis for $V$. Hence given $w \in W$ we can algorithmically always find $w^*$, the unique vector in $V$ closest to $w$. If a basis for $V$ is not known and we only have knowledge or information on proper subspace spans in $V$ of dimension less than $t$ we cannot do this procedure. That is if we do not have complete knowledge of a basis for $V$ we cannot apply the closest vector theorem. Further, since given a subspace of dimension less than $t$ there are infinitely many subspaces of dimension $t$ properly containing it, there is a negligible probability of obtaining the subspace $V$ with only partial knowledge.

**THE SECRET SHARING SCHEME**

We start with an inner product space $W$ of dimension $m$ and an access control group of size $n$. We assume that the dimension $m$ of $W$ is much greater than $n$, that is $m >> n$. Within $W$ there is a hidden subspace $V$ of dimension $t < n$. The secret to be shared is given as an element in this hidden subspace, that is the secret $v \in V$ a vector in $V$.

The dealer distributes to each of the $n$ members of the access control group, $i = 1, \ldots, n$, two vectors, $v_i, w$, where $v_i \in V$, and $w$ is a vector in the big space $W$. The common vector $w$ has the property that $w \notin V$ and $v$ is the vector in $V$ closest to $w$. In general the vector $w$ can be given publically. The set $\{v_1, v_2, \ldots, v_n\}$ has the property that any subset of size $t$ is independent. Hence any subset of size $t$ determines a basis for $V$.

Suppose $t$ valid users get together. They can determine a basis for $V$ and hence using the Gram-Schmidt procedure (see [A]) determine an orthonormal basis. Since $w$ is given, they can determine $v$ by the closest vector theorem and recover the secret.
Given a subset of size less than $t$ the given vectors generate a subspace of $V$ of dimension less than $t$ and hence in $W$ there are infinitely many extensions to subspaces of dimension $t$. This implies that determining $V$ with less than $t$ elements of a basis has negligible probability.

As suggested by Shamir the secret should be altered periodically. In this method it is extremely easy to change the secret $v$ without altering much of the scheme; simply send each user a new $w$.

This is a general method like the Shamir protocol. In [FMR], Fine, Moldenhauer and Rosenberger, compared several different secret sharing plans including the classic Shamir plan and the CFRZ plan.

### 3.2. A Method Based on Combinatorial Group Theory

The protocol in this section and the later new protocol using Nielsen transformations rely on group theory. For this material we refer to the book [Ro] for general group theoretic information and to the book [MKS] for material on combinatorial group theory.

Recall that a finitely presented group is a group with a presentation (see [MKS]) with finitely many generators and only finitely many relators. The word problem for group presentations is: Given a group presentation $G = \langle X; R \rangle$ and a word $W$ in the generators of $G$ to determine algorithmically if $W$ represents the identity or not. It is known that the word problem is insolvable in general, that is, there exist group presentations where the word problem cannot be solved.

D. Panagopoulos [P] devised a secret sharing scheme based on the word problem in finitely presented groups. It is an $(t, n)$-threshold scheme and its main advantage over many other secret sharing schemes is that it does not require the secret message to be determined before each individual person receives his share of the secret. For this scheme it is assumed that the secret is in the form of a binary sequence. The scheme is as follows.

**Step 1.** A group $G$ with finite presentation $G = \langle x_1, x_2, \ldots, x_k; r_1 = \cdots = r_m = 1 \rangle$ is chosen. It is assumed that the word problem is solvable for this presentation and that $m = \binom{n}{t-1}$.

**Step 2.** Let $A_1, \ldots, A_m$ be an enumeration of the subsets of $\{1, \ldots, n\}$ with $t - 1$ elements. Define $n$ subsets of $\{r_1, \ldots, r_m\}$, $R_1, \ldots, R_n$ with $r_j \in R_i$ if and only if $i \notin A_j$, $j = 1, \ldots, m$, $i = 1, \ldots, n$. Then for every $j = 1, \ldots, m$, $r_j$ is not contained in exactly $t - 1$ of the subsets $R_1, \ldots, R_n$. It follows that $r_j$ is contained in any union of $t$ of them whereas if we take any $t - 1$ of the $R_1, \ldots, R_n$ there exists a $j$ such that $r_j$ is not contained in their union.

**Step 3.** Distribute to each of the $n$ persons one of the $R_1, \ldots, R_n$. The set $\{x_1, \ldots, x_k\}$ is known to all of them.

**Step 4.** If the binary sequence to be distributed is $a_1, \ldots, a_k$ construct and distribute a sequence of elements $w_1, \ldots, w_k$ of $G$ such that $w_i = 1$ in $G$ if and only if $a_i = 1$, $i = 1, \ldots, k$. The word $w_i$ must involve most of the relations $r_1, \ldots, r_m$ if $w_i = 1$. Furthermore, all of the relations must be used at some point in the construction of some element.

Any $t$ of the $n$ persons can obtain the sequence $a_1, \ldots, a_k$ by taking the union of the subsets of the relations of $G$ that they possess and thus obtaining the presentation $G = \langle x_1, x_2, \ldots, x_k; r_1 = \cdots = r_m = 1 \rangle$ and solving the word problem $w_i = 1$ in $G$ for $i = 1, \ldots, k$. 

---

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.
A collection of fewer than \( t \) persons cannot decode correctly the message since the union of fewer than \( t \) of the sets \( R_1, \ldots, R_n \) contains some but not all of the relations \( r_1, \ldots, r_m \). Thus such a collection could obtain a group presentation \( G_1 = \langle x_1, x_2, \ldots, x_k; r_1 = \cdots = r_p = 1 \rangle \) with \( p < m \) and \( G \neq G_1 \), where \( w_i = 1 \) in \( G \) is not equivalent to \( w_i = 1 \) in \( G_1 \) in general.

Notice that the secret sequence to be shared is not needed until the final step. It is possible for someone to distribute the sets \( R_1, \ldots, R_n \) and decide at a later time what the sequence would be. In that way the scheme can also be used so that \( t \) of the \( n \) persons can verify the authenticity of the message. In particular the binary sequence in step 4 could contain a predetermined subsequence (signature) along with the normal message. Then \( t \) persons may check whether this predetermined sequence is contained in the encoded message thus validating it.

In the paper by D. Panagopoulos, he also describes some methods for attacking this scheme and also makes some suggestions for possible group presentation types to use. We refer to [P] for these.

### 3.3. A Combinatorial Secret Sharing Scheme.

In her Ph.D. thesis A. Moldenhauer [M] developed a combinatorial \((t,n)\)-secret sharing scheme, where the secret is the sum of multiplicative inverses of elements in the natural numbers.

The method used by the dealer, to develop and distribute the shares, is patterned on the method of Panagopoulos as described in the last section.

Given \( n \), the number of participants and \( t \) the threshold, the dealer does the following:

1. The dealer first calculates the number \( m = \binom{n}{t-1} \).
2. He chooses \( m \) elements \( a_1, a_2, \ldots, a_m \in \mathbb{N} \). From these elements he constructs the sets \( R_1, R_2, \ldots, R_n \) analogously as in the Panagopoulos method. The secret \( S \) is the sum
   \[ S := \sum_{i=1}^{m} \frac{1}{a_i} \in \mathbb{Q}. \]
3. Each participant \( P_i \) gets one share \( R_i, 1 \leq i \leq n \).

If \( t \) of the \( n \) participants come together they can reconstruct the secret. They first combine their \( t \) private sets \( R_i \) and get by construction the set \( \tilde{R} = \{a_1, a_2, \ldots, a_m\} \). The secret is the sum of the inverse elements in the set \( \tilde{R} \), that is
   \[ S = \sum_{i=1}^{m} \frac{1}{a_i}. \]

If the dealer needs a special secret \( \tilde{S} \in \mathbb{Q} \) he gives every participant one more element \( x \in \mathbb{Q} \) in each \( R_i \), with
   \[ x := \frac{\tilde{S}}{S}. \]

The participants get \( \tilde{S} \) by multiplying the reconstructed secret \( S \) with \( x \).

The secret could also just be the sum of the elements, i.e., \( S := \sum_{i=1}^{m} a_i \).

The security of this method is a consequence of the following. Each element \( a_j \) is exactly contained in \( n - (t-1) \) subsets. Hence for each \( j = 1, 2, \ldots, m \) the element \( a_j \) is not contained in \( t - 1 \) subsets from \( \{R_1, R_2, \ldots, R_n\} \). As a consequence, \( a_j \) is in each union of \( t \) subsets. On the other hand, if just \( t - 1 \) arbitrary sets from
\{R_1, R_2, \ldots, R_n\} are combined, there exist a \(j\) so that the element \(a_j\) is not included in the union of this sets.

If just one element \(a_j\) is absent, the participants do not get the correct sum \(S\), and hence cannot compute the correct secret.

**Example 3.2.** To illustrate the method we perform the steps for a \((3, 4)\)-secret sharing protocol.

The dealer follows the steps:

1. He first calculates \(m = \binom{n}{t-1} = \binom{4}{2} = 6\).
2. The dealer chooses the numbers \(a_1 := 2, a_2 := 1, a_3 := 2, a_4 := 8, a_5 := 4\) and \(a_6 := 2\). The secret is
   \[ S := \sum_{i=1}^{m} \frac{1}{a_i} = \frac{23}{8}. \]

(a) The six subsets with size 2 of the set \(\{1, 2, 3, 4\}\) are
   \[ A_1 = \{1, 2\}, \quad A_2 = \{1, 3\}, \quad A_3 = \{1, 4\}, \]
   \[ A_4 = \{2, 3\}, \quad A_5 = \{2, 4\}, \quad A_6 = \{3, 4\}. \]

With help of the \(A_i\) the dealer gets the sets \(R_1, R_2, R_3\) and \(R_4\), which contain elements from \(\{a_1, \ldots, a_6\}\). He puts the element \(a_j\) for which \(i\) is not contained in the set \(A_j\) for \(i = 1, \ldots, 4\) and \(j = 1, \ldots, 6\), into the set \(R_i\):

\[ 1 \notin A_4, A_5, A_6 \implies R_1 = \{a_4, a_5, a_6\}, \]
\[ 2 \notin A_2, A_3, A_6 \implies R_2 = \{a_2, a_3, a_6\}, \]
\[ 3 \notin A_1, A_3, A_5 \implies R_3 = \{a_1, a_3, a_5\}, \]
\[ 4 \notin A_1, A_2, A_4 \implies R_4 = \{a_1, a_2, a_4\}. \]

3. The dealer distributes the set \(R_i\) to the participant \(P_i\), for \(i = 1, \ldots, 4\).

If three of the four participants come together, they can calculate the secret \(S\). For example the participants \(P_1, P_2\) and \(P_3\) have the set \(\check{R} := R_1 \cup R_2 \cup R_3\)

\[ = \{a_4, a_5, a_6\} \cup \{a_2, a_3, a_6\} \cup \{a_1, a_3, a_5\} \]
\[ = \{a_1, a_2, a_3, a_4, a_5, a_6\}, \]

and hence get the secret

\[ S = \sum_{i=1}^{6} \frac{1}{a_i} = \frac{23}{8} \quad \text{with} \ a_i \in \check{R}. \]

**Remark 3.3.** It is important in terms of practicability, that the dealer calculates and distributes the shares for the participants long before the secret is needed by the participants. Hence the dealer has enough time to execute the share distribution and his computational cost should be of no consequence for the protocol. If \(t\) participants reconstruct the secret, they add up only \(m\) elements, which is feasible in linear time.
3.4. An Alternative Using Latin Squares. A second alternative is algebraic and relies on the use of Latin squares. A Latin square of order \( n \) is a 2-dimensional array that consists of \( n \) rows and \( n \) columns such that for any row and any column only one out of the \( n \) given symbols is filled in exactly once. For simplicity, we usually use \( 0, \ldots, n - 1 \) to represent the symbols so that each entry in a Latin square can be represented as a triple \((i, j, k)\), where \( 0 \leq i, j, k \leq n - 1 \), and \( i, j, k \) are the row, the column and the symbol, respectively. In this subsection we introduce two kinds of Latin square based secret sharing schemes.

3.4.1. Using an element of a union of critical sets as a share. A critical set of a Latin square is a partial Latin square that leads to an unique full Latin square, which represents the secret. A critical set will become a partial Latin square if any element is removed. Cooper, Donovan and Seberry (CDS) proposed to use an element of a set \( S \) as a share for a participant in a secret sharing scheme. \( S \) is a union set of several critical sets, i.e., consisted of elements of several critical sets for a Latin square. Any subset of participants is an authorized subset if their shares form one of the critical sets in \( S \).

Example: A (2,3)-threshold scheme is shown in Table 1.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

\[
C_1 \quad C_2 \quad C_3 \quad L
\]

Table 1. A (2,3)-threshold secret sharing scheme.

We can see that all the partial Latin squares \( C_1, C_2, C_3 \) are critical sets. They can be extended uniquely to the full Latin square \( L \). Let \( S \) be the union of the three critical sets \( C_1, C_2, C_3 \). Then

\[
S = \{(0,0,0),(1,1,2),(2,2,1)\}.
\]

We distribute a triple to a participant as a share. Any two participants can recover the full Latin square. So we have a (2,3)-threshold scheme.

However there are serious limitations of using elements of critical sets as shares for a secret sharing scheme. For example, it is difficult to recover the full Latin square from a critical set, it is very hard to find or verify critical sets for a given Latin square. For detailed discussions on the limitations, please see (CZ).

3.4.2. Applying hash function. This was developed by Chum and Zhang (CZ1). Suppose we use the hash of a Latin square to represent a secret and its order, \( n \), is made public. From the literature, we know that if the order \( n \) is increased by 1, the number of Latin squares will grow exponentially. For a large \( n \), say \( n \geq 10 \), there are sufficient numbers of Latin squares of that order.

The idea of using Latin squares for a secret sharing scheme is to store the Latin square in a hash \( h \). For simplicity, we assume that the size of the hash that represents the secret is the same as that of the Latin square (means the order \( n \) of the Latin square).

1) Scheme setup

(1) The dealer generates a random share (a random string) for each participant. Share \( s_i \) will be given to participant \( P_i, i = 1, \ldots, n \).
The dealer decides the authorized subsets $A_1, \ldots, A_w$. Each participant holds a share and concatenation of the shares from any authorized subset leads to a private message $M_{\text{priv}}$. For example, if an authorized subset consists of $P_1, P_3$ and $P_4$, then the corresponding private message is $M_{\text{priv}} = s_1 || s_3 || s_4$, here $||$ symbolizes the concatenation between the shares.

(3) The dealer calculates the hashes for all $w$ private messages

$$H(M_{\text{priv}_i}) = h_i, \ i = 1, \ldots, w.$$  

Let $h$ be the secret with the same size as $h_i$. Then the dealer generates a control $c_i$ as public information for each authorized subset as follows (here $\oplus$ is bit-wise exclusive OR):

$$c_i = h_i \oplus h, \ i = 1, \ldots, w.$$  

2) Secret recovering

Suppose authorized subset $A_i$ consists of participants $P_1, \ldots, P_b$. Pooling their shares together they can recover the secret as follows, see Figure 1.

- Get the public information $c_i$.
- $H(s_1 || s_2 || \ldots || s_b) = h_i$, and $h_i \oplus c_i = h$.

This hash function based Latin square secret sharing scheme has the following features:

- **Perfect**: a participant in a minimal authorized subset is missing, the randomness property of a hash function makes it impossible to recover his/her share directly;
- **Ideal**: the hash of the private message has the same size as the hash of the secret;
- **Fast**: the scheme setup and secret recovery can be done very quickly;
- **Flexible**: no limit to the number of participants;
- **Control area**: used to make sure only authorized subsets can recover the secret.

For an example of the hash function method see [CZ1].

Remark 3.4. The secret is a hash $h$ (a binary sequence). Hence this secret sharing scheme also works without a Latin square. The Dealer needs as a secret just a hash $h$, which is a binary sequence. There is no need that it must be a hash of a Latin square. For each participant the dealer generates a random share $s_j$ such that the hash $h_i$ of the corresponding private messages to the authorized subsets has the same size than the hash $h$ of the secret. Now the secret can be reconstructed with the public controls $c_i$, that correspond to the hashes $h_i$, as explained above.
3.5. Asymmetric and Ranked Secret Sharing. In many instances more involved secret sharing tasks must be handled. As an example consider the following situation. We are in a company that has directors and vice-directors. The directors and vice-directors are in the access control group but they do not have equal weight. Suppose that a secret can be recovered only if one of the following conditions is satisfied:

(a) two directors of the company cooperate;
(b) four vice-directors of the company cooperate;
(c) one director and two vice-directors of the company cooperate.

Thus here the threshold for the access control group differs depending on the status of the members. This is called an asymmetric secret sharing scheme or ranked secret sharing scheme.

In general, every \((t, n)\)-secret sharing scheme can be converted into an asymmetric secret sharing protocol. In a standard \((t, n)\)-secret sharing scheme every share is equivalent. To obtain an asymmetric secret sharing protocol every participant gets a different number of shares depending on the importance of the participant.

For example we can change a \((4, 8)\)-secret sharing scheme into an asymmetric secret sharing protocol. The secret can be reconstructed if two presidents \((D_1\) and \(D_2)\) or four vice-presidents \((V_1, V_2, V_3, V_4)\) or one president and two vice-presidents get together (e.g. \(D_1, V_2\) and \(V_4\)). The dealer distributes the shares as follow:

\[
D_1 = (v_5, v_6), D_2 = (v_7, v_8);
V_1 = (v_1), V_2 = (v_2), V_3 = (v_3), V_4 = (v_4).
\]

Here the \(v_i\), \(i = 1, 2, 3, 4, 5, 6, 7, 8\) are the shares.

Two of the presidents get together, so they have four different shares and with the protocol they can reconstruct the secret.

Every vice-president has only one share, hence four of them have to cooperate to determine the secret. It is sufficient though if one president and two vice-presidents get together to calculate the secret.

Less participants using this structure cannot determine the secret.

4. Comparison of Secret Sharing Protocols

In [FMR] a comparison was done between the Shamir scheme, the Panagopoulos scheme and the Closest Vector scheme. Here we present a brief recap of these results and add the combinatorial secret sharing scheme to the comparison.

Shamir in his paper [Sh] presents some useful properties for a secure \((t, n)\)-secret sharing scheme:

1. The size of each piece does not exceed the size of the secret.
2. When \(t\) is kept fixed, pieces can be dynamically added or deleted. That is, when executives join or leave the company without affecting the other pieces. (A piece is deleted only when a leaving executive makes it completely inaccessible, even to himself.)
3. It is easy to change the pieces without changing the original data (i.e. the secret). A frequent change of this type can greatly enhance security since the pieces exposed by security breaches cannot be accumulated.
4. By using tuples of polynomial values as pieces, we can get a hierarchical scheme in which the number of pieces needed to determine the secret
depends on their importance. For example, if we give the company’s president three values of \(P(x)\), each vice-president two values of \(P(x)\), and each executive one value of \(P(x)\), then a \((3, n)\)-threshold scheme enables checks to be signed either by any three executives, or by any two executives one of whom is a vice-president, or by the president alone.

All of these properties are satisfied by the standard Shamir interpolation scheme. An additional important property would be:

5) It is easy to generate a new secret without changing the shares from the participants.

This last property is not true for Shamir’s secret sharing scheme since the supporting points fixed the polynomial and the constant term (the secret) cannot be changed without redistributing the shares. In \([\text{FMR}]\) the scheme of Panagopoulos and the closest vector scheme were analyzed relative to these criteria.

For the **Panagopoulos scheme**:

1) The secret is a binary sequence and the shares are sets of relations. The length from the relations is not defined. In every set \(R_j\) are \(\binom{n-1}{t-1}\) relations of the group. Therefore, the size of each share can exceed the size of the secret.

2) The dealer creates the shares according to instructions. Hence he cannot add or delete shares, because the way he creates them depends on the number \(m\) of relations and the number \(n\) of participants.

3) The dealer can change the shares if he changes the group \(G\). He had to pay attention that the sent word in the new group is equivalent to 1 if and only if it is also in the previous group. Thus the secret is not changed.

4) Every \((t, n)\)-secret sharing scheme can be converted into an asymmetric secret sharing protocol.

5) The secret, which is a binary sequence, can be changed at every time by sending new words to the participants.

For the **closest vector scheme**:

1) The secret is a vector in the subspace \(V\) of the inner product space \(W\). A share is a basis vector for the subspace \(V\). The size of each share does not exceed the size of the secret.

2) If we fix the number \(t\) of shares (we need at least to reconstruct the secret) we can arbitrarily add or delete many shares. The dealer has to pay attention to the construction, that every possible combination of \(t\) shares form a basis for the subspace \(V\).

3) We can change the shares without changing the secret. We need only another subspace, \(V_0\), which contains the secret \(v\). For this new subspace \(V_0\) with dimension \(t\) we can calculate new shares, which are a set of vectors where every arbitrary \(t\) of them form a basis for \(V_0\). A new vector \(w\) can be constructed (see \([\text{FMR}]\)).

4) An asymmetric system is possible.

5) We can change the secret easily. Every vector in the subspace can be used as a new secret \(v_{\text{new}}\) (excluding the shares from the participants) and hence we can calculate the associated vector \(w_{\text{new}}\) as described in \([\text{FMR}]\).
Thus the closest vector scheme satisfies all five of the important necessary properties. In the Shamir scheme it is not as easy to change the secret.

We add the comparison for the **combinatorial secret sharing scheme**:

1. The secret is the sum over \( m \) elements: \( \sum_{j=1}^{m} \frac{1}{a_j} \in \mathbb{Q}^+ \). The shares are subsets \( R_j \) of \( \{a_1, a_2, \ldots, a_m\} \), \( a_i \in \mathbb{N} \), with \( |R_j| = \binom{n-1}{t-1} \). Therefore, the size of each piece exceed the size of the secret.

2. We use the method of D. Panagopoulos, hence this property is not valid due to the same reasons as for his secret sharing scheme.

3. The shares are subsets of the set \( \{a_1, a_2, \ldots, a_m\} \). If we choose a new set \( \{a'_1, a'_2, \ldots, a'_m\} \) with the property \( \sum_{j=1}^{m} \frac{1}{a_i} = \sum_{j=1}^{m} \frac{1}{a'_i} \), and give every participant subsets of this new set as a share, then the shares can be changed without changing the secret.

4. An asymmetric system is possible.

5. The secret cannot be changed easily, because it is the sum over all elements in the set \( \{a_1, a_2, \ldots, a_m\} \) and hence depends on this set.

In **[FMR]** the time complexity for the participants of the three schemes was also compared. We summarize this below and add the combinatorial secret sharing scheme:

1. **Shamir’s scheme**: The polynomial interpolation has an quadratic running time, i.e. if we have \( t \) supporting points we have a complexity of \( O(t^2) \).

2. **Panagopoulos’ scheme**: The word problem in e.g. a Coxeter group is solvable in quadratic time. Because Coxeter groups are automatic and automatic groups have a solvable word problem with a quadratic running time.

3. **The Closest Vector Scheme**: To orthonormalize \( t \) linear independent vectors in a real inner product space with dimension \( m \) we have a total running time of \( O(t^2m) \). In the closest vector scheme the variable \( m \) depends on the number \( t \), because \( m > t \) is postulated. The total running time for this scheme is longer than for Shamir’s.

4. **Combinatorial secret sharing scheme**: For the reconstruction of the shares the participants only add up \( m \) elements. Therefore, for the participants it is just \( O(m) \), where \( m = \binom{n}{t-1} \) is already previously calculated by the dealer, and hence \( m \) is fixed for the participants.

**Remark 4.1.** In the special case of a \( (t, t+1) \)-secret sharing scheme the running time depends also only on \( t \) like in Sharmir’s scheme:

\[
m = \binom{n}{t-1} = \frac{(t+1)!}{t!} = \frac{(t+1)t}{2} < \frac{2t^2}{2} = t^2.
\]
Hence the running time is also in $O(t^2)$, but as shown above the participants only sum up $m$ elements, which is a very easy operation to reconstruct the secret.

5. Verifying Secret Sharing Protocols (VSS)

In a standard secret sharing protocol it is assumed that the dealer and the participants are honest. To ensure the proper behavior of the dealer and the participants we enhance the standard secret sharing scheme. A verifiable secret sharing protocol, denoted VSS, is one such enhancement. The aim of a VSS protocol is to be certain that the dealer and the participants behave correctly. A verifiable secret sharing protocol ensures that even if the dealer is dishonest there is a well-defined secret that the participants can recover. Verifiable secret sharing is important in secure multiparty computation.

There are many different verifiable secret sharing protocols (see [CFZ]). We first consider the case of a $(2,2)$-VSS and then give a generalization. We must construct a protocol where we can be certain that the dealer and the participants behave correctly. This first VSS protocol uses finite group theory. For a formal definition of homomorphism and isomorphism see [Ro].

(1) Let $G$ and $H$ be two groups and $\phi : G \rightarrow H$ be a group homomorphism so that

$$\phi(g_1g_2) = \phi(g_1)\phi(g_2)$$

which is also a hash function.

(2) Let $s \in G$ be the secret. The dealer chooses $g_1, g_2 \in G$ with $g_1g_2 = s$ and publishes $\phi(g_1), \phi(g_2)$. Nobody can efficiently calculate $s$ from the published data since $\phi$ is a hash function. However, everyone can verify that $\phi(s) = \phi(g_1)\phi(g_2)$.

(3) The dealer tells $g_1$ to the participant $A_1$ and $g_2$ to the participant $A_2$. Each $A_i$ can calculate $\phi(g_i)$ from his secret $g_i$ and can check if the correct partial secret was received.

(4) When the participants reconstruct the secret $s$ each $A_i$ can prove if the other participant has exposed his correct partial secret by calculating $\phi(g_i)$ and comparing with the published values.

We now consider a more general $(t,n)$-VSS protocol. This example requires some elementary number theory. The required material can be found in the book [FR]. Recall that if $p$ is a prime then an integer $g$ is a primitive element modulo $p$ if the order of $g$ is $p - 1$ in the multiplicative group $\mathbb{Z}_p^*$. For an integer $g$ we let $\overline{g}$ denote its residue class modulo $p$.

In the situation from the $(2,2)$-VSS protocol above we choose for the group $G$ the additive group modulo $(p - 1)$, that is $\mathbb{Z}_{p-1}$. For $H$ we choose the multiplicative group $(\mathbb{Z}_p^*, \cdot)$ where $p$ is a sufficiently large prime.

Let $g$ be a primitive element modulo $p$. As a hash function we choose

$$\phi : \mathbb{Z}_{p-1} \rightarrow \mathbb{Z}_p^*$$

by

$$a \mapsto \overline{g}^a \text{ for } a \in \{0, 1, \ldots, p - 1\}.$$  

The dealer chooses randomly a polynomial

$$f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1}$$
where \( a_0, a_1, \ldots, a_{t-1} \in \mathbb{Z}_{p-1} \setminus \{0, 1, \frac{p-1}{2}, p-1\} \) and \( a_0 = s \) is the secret.

The dealer then publishes \( \overline{y}^{s_i} \) for \( i = 0, 1, \ldots, t-1 \). Recall that \( \overline{y}^{s_0} = \overline{y}^s \).

The dealer chooses randomly pairwise distinct elements \( x_1, \ldots, x_n \in \mathbb{Z}_{p-1} \). He calculates \( s_i = f(x_i) \) for \( i = 1, \ldots, n \). He then publishes the values \( x_i \) and \( \overline{y}^{s_i} \) for \( i = 1, \ldots, n \).

Then:

(a) Each participant \( A_i \) can prove if they received \( s_i \) correctly by calculating \( \overline{y}^{s_i} \) and comparing with the published values.

(b) Each participant can prove if

\[
\prod_{j=0}^{t-1} (\overline{y}^{s_j})^{x_i^j} = \overline{y}^{f(x_i)} = \overline{y}^{s_i}.
\]

Practically the dealer cannot cheat. All distributions from the dealer can be proved by the participants.

Finally we present another protocol similar to the one above, due to ElGamal, where the participants cannot cheat but discrepancies from the dealer are hard to discover. This is known as the ElGamal \((t, n)\)-threshold signature protocol.

1. The participants reach an agreement on two large primes \( p, q \) with \( q \mid (p-1) \)
   and a hash function \( h : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p \). We assume that \( M = \mathbb{Z}_p \) is the set of plain text units.

2. There exists a unique cyclic subgroup \( G_q \) of \( \mathbb{Z}_p^* \) with \( q \) elements (see the ElGamal signature method). The participants reach an agreement on a generator \( g \in G_q \).

3. The dealer chooses randomly \( a_0, \ldots, a_{t-1} \in \mathbb{Z}_q \) and defines the polynomial

\[
f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \in \mathbb{Z}_q[x]\]

4. Let \( s = f(0) = a_0 \) be the secret where \( s \in \mathbb{Z}_p \setminus \{0, 1, \frac{p-1}{2}, p-1\} \) and let \( y \equiv g^s \pmod{p} \) be made public.

5. The dealer chooses randomly pairwise distinct elements \( \mu_i, x_i \in \mathbb{Z}_q^* \) for \( i = 1, \ldots, n \) and calculates the partial secrets \( s_i = \mu_i + f(x_i) \) for the participants \( A_i \). The values \( x_i \) are published.

6. The dealer calculates for each participant \( A_i \) the values \( y_i \equiv g^{s_i} \pmod{p} \) and \( z_i \equiv g^{\mu_i} \pmod{p} \) and makes these public.

7. To sign the protocol, each participant \( A_i \) chooses randomly \( k_i \in \mathbb{Z}_q^* \) and calculates \( r_i \equiv g^{k_i} \pmod{p} \). The value \( r_i \) will be sent to the other participants.

8. Suppose that \( t \) participants have sent their values, say, \( A_1, \ldots, A_t \) have sent their values \( r_1, \ldots, r_t \). Then participant \( A_i \) with \( 1 \leq i \leq t \) calculates the value

\[
R = r_1 \cdots r_t \equiv g^{k_1 + \cdots + k_t} \pmod{p}
\]

and the value

\[
E \equiv h(m, R) \pmod{p}, m \in M.
\]

Then \( A_i \) has his partial signature

\[
c_i \equiv s_i \prod_{j \neq i} \frac{x_j}{x_i - x_j} + k_i E \pmod{q}.
\]
(9) The dealer verifies the partial signatures by checking if
\[ \prod_{i \neq j} \frac{x_j}{x_i - x_j} r_i E \equiv g^{c_i} \pmod{p}. \]
(Recall that \( r_i \equiv g^{k_i} \pmod{p} \) and \( y_i \equiv g^{s_i} \pmod{p} \).)
In this case the dealer then calculates \( \sigma \equiv (c_1 + \cdots + c_t) \pmod{q} \).
The signature of \( m \in M \) is then \( (\{A_1, \ldots, A_t\}, R, \sigma) \).

(10) The verification of the signature is to calculate
\[ T \equiv \prod_{i=1}^t \frac{x_j}{x_i - x_j} \quad (\text{mod } p) \]
and check if \( g^\sigma \equiv yTR^E \pmod{p} \).

Notice that the set \( \{A_1, \ldots, A_t\} \) has to be given. However, given such a set the participants practically cannot cheat and the dealer can realize this. The signature is correct. Further, in this protocol, which verifies that the participants cannot cheat, it is difficult to discover any violations to the protocol by the dealer.


In her thesis \([M]\) A. Moldenhauer suggested several ways to use combinatorial group theory to develop further cryptographic protocols. We describe one such new method that relies on Nielsen transformations. Nielsen transformations are the basis of a linear technique to study free groups and general infinite groups. For a complete discussion of these we refer to \([MKS]\) and to the paper \([FRS]\). Below we review some basic definitions concerning regular Nielsen transformations and Nielsen reduced sets. (See \([CgrRR]\), \([LS]\), \([FRS]\) or \([MKS]\).)

Let \( F \) be a free group on the free generating set \( X := \{x_1, x_2, \ldots\} \) and let \( U := \{u_1, u_2, \ldots\} \subset F \).

**Definition 6.1.** An **elementary Nielsen transformation** on \( U = \{u_1, u_2, \ldots\} \) is one of the following transformations

- (T1) replace some \( u_i \) by \( u_i^{-1} \);
- (T2) replace some \( u_i \) by \( u_i u_j \) where \( j \neq i \);
- (T3) delete some \( u_i \) where \( u_i = 1 \).

In all three cases the \( u_k \) for \( i \neq k \) are not changed. A (finite) product of elementary Nielsen transformations is called a **Nielsen transformation**. A Nielsen transformation is called **regular** if it is a finite product of the transformations (T1) and (T2), otherwise it is called **singular**. The set \( U \) is called **Nielsen-equivalent** to the set \( V \), if there is a regular Nielsen transformation from \( U \) to \( V \).

**Definition 6.2.** Consider elements \( v_1, v_2, v_3 \) of the form \( u_i^{\pm 1} \), call \( U \) **Nielsen reduced** if for all such triples the following conditions hold:

- (N0) \( v_1 \neq 1 \);
- (N1) \( v_1 v_2 \neq 1 \) implies \( |v_1 v_2| \geq |v_1|, |v_2| \);
- (N2) \( v_1 v_2 \neq 1 \) and \( v_2 v_3 \neq 1 \) implies \( |v_1 v_2 v_3| > |v_1| - |v_2| + |v_3| \).

Here \( |\cdot| \) denotes the free length in \( F \).
Proposition 6.3. If \( U = \{u_1, u_2, \ldots, u_n\} \) is finite, then \( U \) can be carried by a Nielsen transformation into some \( V \) such that \( V \) is Nielsen reduced.

For the secret sharing scheme based on Nielsen transformations we will only use regular Nielsen transformations.

We write \((T1)_i\) if we replace \( u_i \) by \( u_i^{-1} \) and we write \((T2)_{ij}\) if we replace \( u_i \) by \( u_i u_j \). If we want to apply \( t \)-times one after the other the same Nielsen transformation \((T2)\) we write \( [\underbrace{(T2)}_{ij}]^t \) and hence replace \( u_i \) by \( u_i u_j^t \). In all cases the \( u_k \) for \( i \neq k \) are not changed.

We now describe a \((t,n)\)-secret sharing scheme using Nielsen transformations. We consider free groups as abstract groups but also as subgroups of the special linear group of all \( 2 \times 2 \) matrices over \( \mathbb{Q} \), that is,

\[
SL(2, \mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; a, b, c, d \in \mathbb{Q} \text{ and } ad - bc = 1 \right\}
\]

We use the special linear group over the rational numbers because these numbers can be stored and computed more efficiently on a computer than irrational numbers.

Let \( F \) be a free group in \( SL(2, \mathbb{Q}) \) of rank \( m := \binom{n}{t-1} \). The dealer wants to distribute the shares for the participants as in the Panagopoulos scheme. The shares will be subsets of a free generating set of the group \( F \).

**Steps for the Dealer:** The numbers \( n \) and \( t \) are given, whereby \( n \) is the number of participants and \( t \) is the threshold. We have \( m := \binom{n}{t-1} \).

1. The dealer chooses an abstract free generating set \( X \) for the free group \( F \) of rank \( m \), it is

\[
F = \langle X; \rangle \quad \text{with } X := \{x_1, x_2, \ldots, x_m\}.
\]

He also needs an explicit free generating set \( M \), so it is

\[
F = \langle M; \rangle \quad \text{with } M := \{M_1, M_2, \ldots, M_m\}
\]

and \( M_i \in SL(2, \mathbb{Q}) \).

2. With the known matrices in the set \( M \) he computes the secret

\[
S := \sum_{j=1}^{m} \frac{1}{|a_j|} \in \mathbb{Q}^+ \quad \text{with } a_j := \text{tr}(M_j) \in \mathbb{Q},
\]

\( \text{tr}(M_j) \) is the trace for the matrix \( M_j := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Q}) \), that is, \( \text{tr}(M_j) := a + d \). If the dealer needs a special secret he can act as described in Section 3.3.

3. The dealer constructs the shares for the participants in the following way:
   a) He first applies regular Nielsen transformations simultaneously for both sets \( X \) and \( M \) to get Nielsen equivalent sets \( U \) and \( N \) to \( X \) and \( M \), respectively (see Figure 2).
\[ X := \{x_1, x_2, \ldots, x_m\} \quad M := \{M_1, M_2, \ldots, M_m\} \]

Figure 2. Simultaneously regular Nielsen transformations

The elements \(u_i\) are words in \(X\) and the elements \(N_i\) are words in \(M\). Hence we have \(N_i \in \text{SL}(2, \mathbb{Q})\).

(b) The dealer now uses the method of Panagopoulos to split \(U\) and \(N\) and to get the share \((R_i, S_j)\) for the participant \(P_k\) with \(R_i \subset U\) and \(S_j \subset N\).

(4) The dealer distributes the shares.

If \(t\) of the \(n\) participants combine their parts then they obtain the sets \(U\) and \(N\). The secret can be recovered as follows:

(1) The participants apply regular Nielsen transformations in a Nielsen reduction manner for \(U\) and step by step simultaneously for \(N\). By Proposition 6.3 they get Nielsen reduced sets \(X^\pm = \{x^\pm_1, x^\pm_2, \ldots, x^\pm_m\}\) and \(M^\pm = \{M^\delta_1, M^\delta_2, \ldots, M^\delta_m\}\) with \(\epsilon_i, \delta_i \in \{+1, -1\}\), see Figure 3.

\[ U := \{u_1, u_2, \ldots, u_m\} \quad N := \{N_1, N_2, \ldots, N_m\} \]

Figure 3. Simultaneously regular Nielsen transformations

(2) With the knowledge of the set \(M^\pm\) it is easy to reconstruct the secret

\[ S = \sum_{j=1}^{m} \frac{1}{|a_j|} \in \mathbb{Q}^+ \quad \text{with } tr(M_j) = a_j \in \mathbb{Q}. \]

Recall that \(tr(M^\delta_i) = tr(M_i)\) for \(i = 1, \ldots, m\).

Less than \(t\) participants can neither get the whole set \(U\), which is Nielsen-equivalent to \(X^\pm\), nor the set \(N\), which is Nielsen-equivalent to \(M^\pm\).

For the calculation of the secret, the participants need the set \(M^\pm\), because the secret depends on the traces of the matrices \(M_i \in M^\pm\). The participants need both sets \(U\) and \(N\). If they just have one set \(U\) or \(N\) they cannot get information about the set \(M^\pm\).

If the set \(U\) is known, it is only known which Nielsen transformation should be done to get the Nielsen equivalent set \(X^\pm\), but it is unknown on which matrices they should be simultaneously done.
If only the set $N$ is known, then the matrices in $\text{SL}(2, \mathbb{Q})$ are known, but nobody knows which Nielsen transformations should be done on $N$ to get the set $M^\pm$. It is also unknown how many Nielsen transformations were used.

**Remark 6.4.** Analogously to the combinatorial secret sharing scheme, this scheme fulfills the same properties ((3) and (4)) of Section 4, because both schemes are based on the share distribution method of D. Panagopoulos. There is an idea to fulfill the property (5) by publishing the set $N$. If the Dealer changes the set $N$ he changes the secret. But there is not enough security analysis about this idea, yet.

In [Ste] an algorithm, using elementary Nielsen transformations, is presented which, given a finite set $S$ of $m$ words of some free group, returns a set $S'$ of Nielsen reduced words such that $\langle S \rangle = \langle S' \rangle$; the algorithm runs in $O(\ell^2 m^2)$, where $\ell$ is the maximum length of a word in $S$.

In this protocol, the dealer fixes the number $m$, hence the running time depends only on the maximum length $\ell$ of the words in the Nielsen-equivalent set $U$ to the set $X$. Thus the participants have a running time of $O(\ell^2)$ to get the set $X^\pm$.

If the participants perform the associated elementary Nielsen transformations on the set $N$ of matrices at the same time, then they perform either matrix multiplication or they calculate an inverse matrix. In order to multiply two $2 \times 2$ matrices in $\text{SL}(2, \mathbb{Q})$ they need 8 multiplications and 4 additions of rational numbers, hence 12 operations. The inverse matrix of

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Q})$$

is

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$  

The participants need 4 operations to get $\frac{1}{ad - bc}$; for the entries in the matrix $A^{-1}$ they do not need any operations, they just swap two entries and write a minus in front of the other two entries.

All together the participants have a running time of $O(\ell^2)$, where $\ell$ is the maximum length of the elements in $U$.

In the book of J. Lehner [Leh] on page 247 a method is given to explicitly obtain a free generating set $M$ for a free group $F$ on the abstract generating set $X := \{x_1, x_2, \ldots, x_m\}$:

**Example 6.5.** Let $F$ be a free group with countably many free generators $x_1, x_2, \ldots$. Corresponding to $x_j$ define the matrix

$$M_j = \begin{pmatrix} -r_j & -1 + r_j^2 \\ 1 & -r_j \end{pmatrix}$$

with $r_j \in \mathbb{Q}$ such that the following inequalities hold:

(2) \hspace{1cm} r_{j+1} - r_j \geq 3 \quad \text{and} \quad r_1 \geq 2.

The group $G$ generated by $\{M_1, M_2, \ldots\}$ is isomorphic to $F$ (see [Leh]).

We now present an example for this secret sharing scheme.
EXAMPLE 6.6. We perform the steps for an \((2, 3)\)-secret sharing scheme with the help of the computer program Maple 16. It is \(n = 3\), \(t = 2\) and hence \(m = \binom{3}{1} = 3\). First the Dealer generates the shares for the participants.

1. The dealer chooses an abstract presentation for the free group \(F\) of rank 3

\[
F = \langle X; \rangle \quad \text{with} \quad X := \{x_1, x_2, x_3\}.
\]

He takes an explicit presentation

\[
F = \langle M; \rangle \quad \text{with} \quad M := \{M_1, M_2, M_3\},
\]

\(M_i \in \text{SL}(2, \mathbb{Q})\) as above. We first mention that the inequalities \((2)\) hold for

\[
\begin{align*}
    r_1 &= \frac{7}{2}, & r_2 &= \frac{15}{2}, & r_3 &= 11
\end{align*}
\]

and hence the set of the matrices

\[
\begin{align*}
    M_1 &= \begin{pmatrix} -\frac{7}{2} & 1 \\ -\frac{7}{2} & -1 + \left(\frac{7}{2}\right)^2 \end{pmatrix} = \begin{pmatrix} -\frac{7}{2} & \frac{45}{4} \\ 1 & -\frac{7}{2} \end{pmatrix}, \\
    M_2 &= \begin{pmatrix} -\frac{15}{2} & 1 \\ -\frac{15}{2} & -1 + \left(\frac{15}{2}\right)^2 \end{pmatrix} = \begin{pmatrix} -\frac{15}{2} & \frac{221}{4} \\ 1 & -\frac{15}{2} \end{pmatrix}, \\
    M_3 &= \begin{pmatrix} -11 & 1 \\ 1 & -11 \end{pmatrix} = \begin{pmatrix} -11 & 120 \\ 1 & -11 \end{pmatrix}
\end{align*}
\]

is a free generating set for a free group of rank 3.

2. We have

\[
\begin{align*}
    a_1 := tr(M_1) &= -7, & a_2 := tr(M_2) &= -15, & a_3 := tr(M_3) &= -22,
\end{align*}
\]

and hence the secret is

\[
S := \sum_{j=1}^{3} \frac{1}{|a_j|} = \frac{589}{2310}.
\]

3. Construction of the shares for the participants:

   (a) First the dealer applies regular Nielsen transformations (NTs) simultaneously for both sets \(X\) and \(M\) to get Nielsen equivalent sets \(U\) and \(N\) to \(X\) or \(M\), respectively. These transformations are shown in the Tables 2 and 3.
### Table 2. Nielsen transformations (NTs) of the dealer I

<table>
<thead>
<tr>
<th>NTs</th>
<th>theoretical set X</th>
<th>explicit set M</th>
</tr>
</thead>
<tbody>
<tr>
<td>({x_1, x_2, x_3})</td>
<td>(\left{ \left( \begin{array}{c} -\frac{7}{2} \ 1 \end{array} \right), \left( \begin{array}{c} 45 \ -\frac{7}{2} \end{array} \right), \left( \begin{array}{c} -11 \ 1 \end{array} \right), \left( \begin{array}{c} 120 \ 1 \end{array} \right) \right})</td>
<td></td>
</tr>
<tr>
<td>((T1)_{2})</td>
<td>({x_1, x_2^{-1}, x_3})</td>
<td>(\left{ \left( \begin{array}{c} -\frac{7}{2} \ 1 \end{array} \right), \left( \begin{array}{c} 45 \ -\frac{7}{2} \end{array} \right), \left( \begin{array}{c} -11 \ 1 \end{array} \right), \left( \begin{array}{c} 120 \ 1 \end{array} \right) \right})</td>
</tr>
<tr>
<td>((T2)_{12})</td>
<td>({x_1x_2^{-1}, x_2^{-1}, x_3})</td>
<td>(\left{ \left( \begin{array}{c} 15 \ -4 \ -29 \end{array} \right), \left( \begin{array}{c} -15 \ -1 \ -\frac{221}{15} \end{array} \right), \left( \begin{array}{c} -11 \ 1 \end{array} \right), \left( \begin{array}{c} -110 \right) \right})</td>
</tr>
<tr>
<td>([(T2)<em>{32}]</em>{3})</td>
<td>({x_1x_2^{-1}, x_2^{-1}, x_3x_2^{-3}})</td>
<td>(\left{ \left( \begin{array}{c} 15 \ -4 \ -29 \end{array} \right), \left( \begin{array}{c} -15 \ -1 \ -\frac{221}{15} \end{array} \right), \left( \begin{array}{c} -8565 \ 799 \end{array} \right), \left( \begin{array}{c} -63664 \ 5939 \end{array} \right) \right})</td>
</tr>
<tr>
<td>((T2)_{23})</td>
<td>({x_1x_2^{-1}, x_2^{-1}x_3x_2^{-3}, x_3x_2^{-3}})</td>
<td>(\left{ \left( \begin{array}{c} 15 \ -4 \ -29 \end{array} \right), \left( \begin{array}{c} 5145 \ 38243 \end{array} \right), \left( \begin{array}{c} 507401 \ 3292 \end{array} \right), \left( \begin{array}{c} -8565 \ 799 \end{array} \right), \left( \begin{array}{c} -63664 \ 5939 \end{array} \right) \right})</td>
</tr>
<tr>
<td>((T1)_{1})</td>
<td>({x_2x_1^{-1}, x_2^{-1}x_3x_2^{-3}, x_3x_2^{-3}})</td>
<td>(\left{ \left( \begin{array}{c} -29 \ 4 \ 15 \end{array} \right), \left( \begin{array}{c} 80371 \ 5145 \end{array} \right), \left( \begin{array}{c} 507401 \ 38243 \end{array} \right), \left( \begin{array}{c} -8565 \ 799 \end{array} \right), \left( \begin{array}{c} -63664 \right) \right})</td>
</tr>
<tr>
<td>((T2)_{12})</td>
<td>({x_2^{-1}x_3x_2^{-3}, x_3x_2^{-3}})</td>
<td>(\left{ \left( \begin{array}{c} -2452369 \ 237317 \end{array} \right), \left( \begin{array}{c} 256666640 \end{array} \right), \left( \begin{array}{c} 1768447 \end{array} \right) \right})</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3. Nielsen transformations (NTs) of the dealer II

<table>
<thead>
<tr>
<th>NTs</th>
<th>theoretical set</th>
<th>explicit set</th>
</tr>
</thead>
<tbody>
<tr>
<td>(T1)3</td>
<td>( { x_2 x_1^{-1} x_2^{-1} x_3 x_2^{-3}, x_2^{-1} x_3 x_2^{-3}, x_2^{3} x_3^{-1} } )</td>
<td>( \left{ \left( \begin{array}{cc} -3452369 &amp; -25661603 \ 237917 &amp; 1768447 \end{array} \right), \left( \begin{array}{cc} 80371 &amp; 597401 \ 5145 &amp; 38243 \end{array} \right), \left( \begin{array}{cc} 1132425929 &amp; 8417369243 \ 152350279 &amp; -1132425989 \end{array} \right) \right} )</td>
</tr>
</tbody>
</table>

The Dealer gets the sets

\[ U = \{ u_1, u_2, u_3 \} := \{ x_2 x_1^{-1} x_2^{-1} x_3 x_2^{-3}, x_2^{-1} x_3 x_2^{-3}, x_2^{3} x_3^{-1} x_2^{-1} x_3 x_2^{-3} \} \]

and

\[ N = \{ N_1, N_2, N_3 \} := \left\{ \left( \begin{array}{cc} -3452369 & -25661603 \\ 237917 & 1768447 \end{array} \right), \left( \begin{array}{cc} 80371 & 597401 \\ 5145 & 38243 \end{array} \right), \left( \begin{array}{cc} 1132425929 & 8417369243 \\ 152350279 & -1132425989 \end{array} \right) \right\} \]

(b) He gets the share \((R_i, S_j)\) for the participant \(P_k\) with \(R_i \subset U\) and \(S_j \subset N\) as follow:

(i) It is \(m = \binom{n}{3} = \binom{3}{3} = 3\).

(ii) The dealer chooses the elements \(\tilde{a}_1, \tilde{a}_2, \tilde{a}_3\) and gets the three sets

\( A_1 = \{ 1 \}, \quad A_2 = \{ 2 \}, \quad A_3 = \{ 3 \}. \)

With the help of the \(A_i\) the dealer gets the sets \(R'_1, R'_2, R'_3\) which contain elements from the set \(\{\tilde{a}_1, \tilde{a}_2, \tilde{a}_3\}\). He puts the element \(\tilde{a}_j\) by which \(i\) is not contained in the set \(A_j\) for \(i = 1, 2, 3\) and \(j = 1, 2, 3\), into the set \(R'_i\).

\( 1 \not\in A_2, A_3 \Rightarrow R'_1 = \{ \tilde{a}_2, \tilde{a}_3 \}, \)

\( 2 \not\in A_1, A_3 \Rightarrow R'_2 = \{ \tilde{a}_1, \tilde{a}_3 \}, \)

\( 3 \not\in A_1, A_2 \Rightarrow R'_3 = \{ \tilde{a}_1, \tilde{a}_2 \}. \)

Now we apply this to \(U\) and \(N\) to create the share-sets for the participants, respectively:

\( R_1 = \{ u_2, u_3 \}, \quad S_1 = \{ N_2, N_3 \}, \)

\( R_2 = \{ u_1, u_3 \}, \quad S_2 = \{ N_1, N_3 \}, \)

\( R_3 = \{ u_1, u_2 \}, \quad S_3 = \{ N_1, N_2 \}. \)
(4) The Dealer gives every participant $P_k$ a tuple $(R_i, S_j)$. Participant $P_1$ gets $(R_1, S_1)$, $P_2$ gets $(R_2, S_2)$ and $P_3$ gets $(R_3, S_3)$.

Assume the participants $P_1$ and $P_2$ come together to reconstruct the secret. They generate the sets $U = \{u_1, u_2, u_3\}$ and $N = \{N_1, N_2, N_3\}$. The secret can be recovered as follow.

The participants apply regular Nielsen transformations step by step simultaneously for both sets $U$ and $N$ to get $X^\pm$ and $M^\pm$. The steps are shown in the Tables 4 and 5.

### Table 4. Nielsen transformations (NTs) from the participants I

<table>
<thead>
<tr>
<th>NTs</th>
<th>theoretical set $U$</th>
<th>explicit set $N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(T1)_2$</td>
<td>${x_2^{-1}x_1^{-1}x_2x_3^{-3},$ \</td>
<td>$\left{ \begin{array}{c} -\frac{3452369}{237017} - \frac{25661603}{1768447} \ \frac{80371}{5145} - \frac{507401}{80371} \end{array} \right}$, $\left{ \begin{array}{c} -\frac{152250279}{4} - \frac{1132492843}{4} \ -\frac{152250279}{4} - \frac{1132492843}{4} \end{array} \right}$</td>
</tr>
<tr>
<td>$(T2)_{32}$</td>
<td>${x_2^{-1}x_1^{-1}x_2x_3^{-3},$ \</td>
<td>$\left{ \begin{array}{c} -\frac{3452369}{237017} - \frac{25661603}{1768447} \ \frac{80371}{5145} - \frac{507401}{80371} \end{array} \right}$, $\left{ \begin{array}{c} -\frac{152250279}{4} - \frac{1132492843}{4} \ -\frac{152250279}{4} - \frac{1132492843}{4} \end{array} \right}$</td>
</tr>
<tr>
<td>$(T1)_2$</td>
<td>${x_2^{-1}x_1^{-1}x_2x_3^{-3},$ \</td>
<td>$\left{ \begin{array}{c} -\frac{3452369}{237017} - \frac{25661603}{1768447} \ \frac{80371}{5145} - \frac{507401}{80371} \end{array} \right}$, $\left{ \begin{array}{c} -\frac{152250279}{4} - \frac{1132492843}{4} \ -\frac{152250279}{4} - \frac{1132492843}{4} \end{array} \right}$</td>
</tr>
<tr>
<td>$(T2)_{23}$</td>
<td>${x_2^{-1}x_1^{-1}x_2x_3^{-3},$ \</td>
<td>$\left{ \begin{array}{c} -\frac{3452369}{237017} - \frac{25661603}{1768447} \ \frac{80371}{5145} - \frac{507401}{80371} \end{array} \right}$, $\left{ \begin{array}{c} -\frac{152250279}{4} - \frac{1132492843}{4} \ -\frac{152250279}{4} - \frac{1132492843}{4} \end{array} \right}$</td>
</tr>
</tbody>
</table>
Table 5. Nielsen transformations (NTs) from the participants II

<table>
<thead>
<tr>
<th>NTs</th>
<th>theoretical set</th>
<th>explicit set</th>
</tr>
</thead>
<tbody>
<tr>
<td>(T2)_{13}</td>
<td>{x_2x_1^{-1}x_2^{-1}, x_2^{-1}, x_2^3x_3^{-1}}</td>
<td>{(653/7, 9679, -45 - 457/2), (-15/1 - 221/2, 5939, 63664), (-799, -8565)}</td>
</tr>
<tr>
<td>(T1)_{2}</td>
<td>{x_2x_1^{-1}x_2^{-1}, x_2, x_2^3x_3^{-1}}</td>
<td>{(653/7, 9679, -45 - 457/2), (-15/1 - 221/2, 5939, 63664), (-799, -8565)}</td>
</tr>
<tr>
<td>(T2)_{12}</td>
<td>{x_2x_1^{-1}, x_2, x_2^3x_3^{-1}}</td>
<td>{(-29, -109, 15, -15, 221, 5939, 63664), (-799, -8565)}</td>
</tr>
<tr>
<td>(T1)_{1}</td>
<td>{x_2x_1^{-1}, x_2, x_2^3x_3^{-1}}</td>
<td>{(-29, -109, 15, -15, 221, 5939, 63664), (-799, -8565)}</td>
</tr>
<tr>
<td>(T2)_{12}</td>
<td>{x_1, x_2, x_2^3x_3^{-1}}</td>
<td>{(-7, 45, 1, -2), (-15, 221, 5939, 63664), (-799, -8565)}</td>
</tr>
<tr>
<td>(T1)_{3}</td>
<td>{x_1, x_2, x_3x_2^{-3}}</td>
<td>{(-7, 45, 1, -2), (-15, 221, 5939, 63664), (-799, -8565)}</td>
</tr>
<tr>
<td>[(T2)<em>{32}]</em>{3}</td>
<td>{x_1, x_2, x_3}</td>
<td>{(-7, 45, 1, -2), (-15, 221, 5939, 63664), (-799, -8565)}</td>
</tr>
</tbody>
</table>

With the knowledge of the set \( M^\pm = \left\{ \left( \frac{-7}{1}, \frac{45}{1}, -\frac{2}{2} \right), \left( \frac{-15}{1}, \frac{221}{1}, -\frac{11}{2} \right), \left( \frac{-11}{1}, \frac{120}{1}, -\frac{11}{1} \right) \right\} \) the participants can reconstruct the secret easily. It is

\[ a_1 := tr(M_1) = -7, \quad a_2 := tr(M_2) = -15, \quad a_3 := tr(M_3) = -22, \]

and hence it is

\[ S := \sum_{j=1}^{3} \frac{1}{|a_j|} = \frac{1}{7} + \frac{1}{15} + \frac{1}{22} = \frac{589}{2310}. \]

In general we can use any free matrix group \( F \) of rank \( m := (t, n) \) for a \( (t, n) \)-secret sharing scheme as it is described in this section. The shares can be generated by the method of D. Panagopoulos and are tuples \((R_i, S_j)\) with \( R_i \subset U \) and \( S_j \subset N \).
Some other ideas for the secret $S$ are

\[ S := \prod_{i=1}^{m} |\text{tr}(M_i)| \] or \[ S := \sum_{i=1}^{m} |\text{tr}(M_i)| \]

\[ S := \prod_{i=1}^{m} (\text{tr}(M_i))^2 \] or \[ S := \sum_{i=1}^{m} (\text{tr}(M_i))^2 \]

\[ S := \prod_{i=1}^{m} \text{tr}([M_{2i-1}, M_{2i}]) \] if $m$ is even or \[ S := \sum_{i=1}^{m} \text{tr}(M_i^2). \]

7. A Variation of the Secret Sharing Scheme based on Nielsen Transformations

We now present a variation of the secret sharing protocol given in the last section. Let $F$ be a finitely generated free group with the abstract free generating set $X := \{x_1, x_2, \ldots, x_q\}$, $q \in \mathbb{N}$, that is,

\[ F = \langle X; \rangle. \]

In this variation we just work with respect to the given basis elements of a finitely generated free group. For a $(t, n)$-secret sharing scheme the dealer chooses a Nielsen reduced set $U \subset F$ with $U = \{u_1, u_2, \ldots, u_m\}$. The $u_i$ are given as words in $X$. The secret is the sum

\[ S := \sum_{i=1}^{m} \frac{1}{|u_i|}, \]

with $|u_i|$ the free length of the word $u_i$.

The dealer does a regular Nielsen transformation on the set $U$ to get the Nielsen-equivalent set $V$ as shown in Figure 4.

\[ U := \{u_1, u_2, \ldots, u_m\} \]

\[ V := \{v_1, v_2, \ldots, v_m\} \]

Figure 4. Regular Nielsen transformation

Each participant $P_i$, $1 \leq i \leq n$, gets one set $R_i \subset V$, which was generated with the method of D. Panagopoulos.

If $t$ of the $n$ participants come together to reconstruct the secret, they combine their shares and get the set $V = \{v_1, v_2, \ldots, v_m\}$. They have to find a Nielsen-reduced set $U' := \{u_1', u_2', \ldots, u_m'\}$ to $V$. They apply Nielsen transformations in
a Nielsen reducing manner as described in [CgrRR] and [LS] and get from \(V\) a Nielsen-reduced set \(U'\). The secret is the sum
\[
S = \sum_{i=1}^{m} \frac{1}{|u'_i|},
\]
because for each \(i\) we have \(|u'_i| = |u_j|\) for some \(j\) (see the proof of Corollary 3.1 in [MKS]). From \(U'\) we get \(U\) by permutations and length preserving Nielsen transformations.

**Remark 7.1.** Analogously to the combinatorial secret sharing scheme, this scheme fulfills the same properties ((3) and (4)) of Section 4, because both schemes are based on the share distribution method of D. Panagopoulos.

In [Ste] an algorithm, using elementary Nielsen transformations, is presented which, given a finite set \(S\) of \(m\) words of some free group, returns a set \(S'\) of Nielsen reduced words such that \(\langle S \rangle = \langle S' \rangle\); the algorithm runs in \(O(\ell^2m^2)\), where \(\ell\) is the maximum length of a word in \(S\).

In this protocol, the dealer fixes the number \(m\), hence the running time depends only on the maximum length \(\ell\) of the words in the Nielsen-equivalent set \(V\) to the set \(U\). Thus the participants have a running time of \(O(\ell^2)\) to get the set \(U'\). The secret is then the above sum, which is computable in linear time.

As an example we may take the respective Example 6.6 but now the participants do not need the single elementary Nielsen transformations, they just have to Nielsen reduce the set \(V\) (see [Ste]).

8. A Secret Sharing Protocol based on the Hurwitz Equation

A generalized Hurwitz equation is given by
\[
a_1 x_1^2 + \cdots + a_m x_m^2 = dx_1 \cdots x_m - k
\]
where \(m \geq 3\), \(k \in \mathbb{N} \cup \{0\}\), \(a_1, \ldots, a_m, d \in \mathbb{N}\) with \(a_i|d\) for \(i = 1, \ldots, m\) and the \(a_i\) are pairwise coprime. Hurwitz [H] considered the special case \(a_1 = \cdots = a_m = 1\). For \(m = 3\) the equation is often called the Markov-Rosenberger equation and is quite well understood. Such an equation occurs in connection with many different mathematical theories and problems (see [FKMR] and the references there).

Related to the general Hurwitz-equation is the Baragar and Umeda diophantine equation
\[
a x^2 + b y^2 + c z^2 = d x y z + e
\]
with \(a, b, c, d, e \in \mathbb{N}\) such that \(a|d, b|d, c|d\) and \(\gcd(a, b, c) = 1\). Further we assume that \(\gcd(a, b, c) = 1\) because if \(\gcd(a, b, c) = t\) then \(t|e\). In [FKMR] we considered various aspects of the integer solutions to these equations and certain variations of them. As a by-product, we observed that the equations could be used as the basis of a \((t, n)\)-secret sharing protocol.

The secret sharing protocol works as follows:
Consider the basic Hurwitz equation
\[
x_1^2 + x_2^2 + \cdots + x_m^2 = x_1 \cdots x_m - k.
\]
We now consider this equation over a field \(K\), for example \(K = \mathbb{Q}\) or \(K = F\) where \(F\) is a big finite field, with \(k \neq 0\).

The secret in this protocol is the element
\[
S = x_1^2 + x_2^2 + \cdots + x_m^2 - x_1 \cdots x_m
\]
The shares for the participants are subsets from \( \{ x_1, \ldots, x_m \} \). To generate these shares the method from D. Panagopoulos is again used:

1. \( m = \binom{n}{t-1} \) is the number of elements the participants need to know to reconstruct the secret, that is, they have to know the set \( \{ x_1, \ldots, x_m \} \).
2. Let \( A_1, A_2, \ldots, A_m \) be an enumeration of the subsets of \( \{ 1, 2, \ldots, n \} \) with \( t-1 \) elements. Define \( n \) subsets \( \{ R_1, R_2, \ldots, R_n \} \) of \( \{ x_1, x_2, \ldots, x_m \} \) with the property

\[
x_j \in R_i \iff i \notin A_j
\]

for \( j = 1, \ldots, m \) and \( i = 1, \ldots, n \).
3. Each of the \( n \) participants gets one of the sets \( \{ R_1, R_2, \ldots, R_n \} \).

Each element \( x_j \) is exactly contained in \( n - (t-1) \) subsets. Hence for each \( j = 1, \ldots, m \) the element \( x_j \) is not contained in \( t-1 \) subsets from \( R_1, \ldots, R_n \). As a consequence, \( x_j \) is in each union of \( t \) subsets. On the other hand if just \( t-1 \) arbitrary sets from \( \{ R_1, \ldots, R_n \} \) are combined, there exist a \( j \) so that the element \( x_j \) is not included in the union of this sets. If just one element \( x_j \) is absent, the participants cannot get the element \( S \) and hence cannot compute the secret. If \( t \) of \( n \) participants come together they get by construction the set

\[
\{ x_1, x_2, \ldots, x_m \}
\]

and hence they can calculate the secret

\[
S = x_1^2 + x_2^2 + \cdots + x_m^2 - x_1 \cdots x_m.
\]

**Remark 8.1.** Analogously to the combinatorial secret sharing scheme, this scheme fulfills the same properties ((3) and (4)) of Section 4, because both schemes are based on the share distribution method of D. Panagopoulos.

The time complexity for the participants is as in the combinatorial secret sharing scheme. Therefore the running time is linear in \( m \). As an example we can take the respective variation of Example 3.2. With the numbers in Example 3.2 the secret here is

\[
S = 2^2 + 1^2 + 2^2 + 8^2 + 4^2 + 2^2 - 2 \cdot 1 \cdot 2 \cdot 8 \cdot 4 \cdot 2 = -163.
\]

**References**


