Crucial and Redundant Shares and Compartments in Secret Sharing

Fabian Schillinger\[0000−0001−8771−8290\] and Christian Schindelhauer\[0000−0002−8320−8581\]

Computer Networks and Telematics, Department of Computer Science, University of Freiburg, Germany
{schillfa,schindel}@tf.uni-freiburg.de

Abstract. Secret sharing is the well-known problem of splitting a secret into multiple shares, which are distributed to shareholders. When enough or the correct combination of shareholders work together the secret can be restored. We introduce two new types of shares to the secret sharing scheme of Shamir. Crucial shares are always needed for the reconstruction of the secret, whereas mutual redundant shares only help once in reconstructing the secret. Further, we extend the idea of crucial and redundant shares to a compartmented secret sharing scheme. The scheme, which is based on Shamir’s, allows distributing the secret to different compartments, that hold shareholders themselves. In each compartment, another secret sharing scheme can be applied. Using the modifications the overall complexity of general access structures realized through compartmented secret sharing schemes can be reduced. This improves the computational complexity. Also, the number of shares can be reduced and some complex access structures can be realized with ideal amount and size of shares.

Keywords: Secret Sharing · Compartmented Secret Sharing · Crucial Shares · Redundant Shares · General Access · Ideal Secret Sharing

1 Introduction

A secret sharing scheme allows a dealer to distribute a secret, like an access code to multiple users, often called shareholders. The parts of the secret, often called shares or shadows can be used to reconstruct or reveal the secret when it is lost or destroyed. A simple secret sharing scheme works as follows: First, the dealer converts the secret into a number $S$ from a Galois field modulo $p$. Second, it generates a uniformly distributed random number $r_i$ from $GF(p)$ for each but one shareholder and calculates a $r'$, such that the equation $S = \sum_i r_i + r'$ mod $p$ holds. Third, it distributes each share $r_i$ or $r'$ to the according shareholder. When all shareholders work together they can calculate the sum of their shares to reveal $S$. This allows distributing a secret in a way, such that no shareholder can calculate $S$ solely from their share. The secret cannot be revealed anymore if any shareholder stops helping. Threshold secret sharing schemes overcome this drawback.
Threshold Secret Sharing Schemes

A \((t, n)\)-threshold secret sharing scheme (TSSS) allows a dealer to define some threshold \(t\) and to split a secret \(S\), into \(n\) shares. The shares are distributed to the shareholders. When the threshold is met, i.e. enough shareholders combine their shares, they can reveal \(S\). The following scenario can be solved by a TSSS:

\textit{Example 1.} To open the vault of a company multiple people have to work together. The company owner, three managers, and three shift leaders each have a private access code for the vault. As soon as two of the seven people enter their code the vault can be opened.

Secret sharing schemes were first proposed in 1979 by Shamir \[19\] and Blakley \[5\]. In the scheme of Shamir a random polynomial of degree \(t - 1\) is generated, such that the intersection with the \(x\)-axis defines the secret. The polynomial is used to calculate \(n\) points, which are distributed. When \(t\) points are known the secret can be calculated. The scheme is discussed in detail in Chapter 2. In the scheme of Blakley, the secret is a point of intersection of hyperplanes in a \(t\) dimensional space. Other approaches, like \[7\] or \[11\] use Latin squares or the Chinese Remainder Theorem.

Hierarchical Threshold Secret Sharing Schemes

Hierarchical threshold secret sharing schemes (HSSS), or multilevel threshold schemes allow organizing shareholders in different groups. Each group is a subgroup of a larger group, where the largest group contains all shareholders. This allows replacing shares of a group by shares out of the parent groups. An HSSS can solve the following scenario:

\textit{Example 2.} To open the vault of a company multiple people have to work together. The company owner, three managers, and three shift leaders each have a private access code for the vault. To open the vault all of the shift leaders have to enter their private access codes. Because the owner and managers have higher positions, their access codes can be used as substitutes for the codes of the shift leaders. The vault can be opened for example if two of the managers, together with a shift leader enter their codes, or if the owner, one manager, and one of the shift leaders enter their codes.

Multiple approaches for HSS are presented in \[21,20,23,8,10,24,1,26\].

Compartmented Threshold Secret Sharing Schemes

In compartmented threshold secret sharing schemes (CTSS) the shareholders are grouped in different compartments. Each compartment receives a share through a secret sharing scheme. Each share is used as a new secret and distributed, using another secret sharing scheme to the users in the compartment. This allows to retrieve a secret in a conjunctive CTSS if in every compartment the secret is
retrieved, and then the secrets are combined. In a disjunctive CTSS, only in a specific number of compartments, the shares have to be revealed to calculate the secret. A CTSS can solve the following scenario:

**Example 3.** To open the vault of a company multiple people have to work together. The company owner, three managers, and three shift leaders each have a private access code for the vault. The company owner and the three managers form the higher management, whereas the shift leaders form the lower management. In a conjunctive CTSS two people from the higher management and two people from the lower management have to enter their codes to open the vault, whereas, in a disjunctive CTSS, either two persons from the higher management, or two persons from the lower management suffice to open the vault.

It is possible to construct far more complex access structures, by using a CTSS. In [3] it is shown, that every CTSS may be used for general access structures. Shareholders might receive more than one share in those schemes. The approach discussed in [16] can be used to generate both, HSSS and CTSS. Other approaches are presented in [9][13][21].

**Weighted Threshold Secret Sharing Schemes**

In a weighted threshold secret sharing schemes (WTSS) each shareholder has a specific weight. If the sum of weights of the combined shares is larger than the threshold value, the secret can be revealed. Single shares of shareholders with a higher weight, therefore, can replace multiple shares of shareholders with lower weights. A WTSS can solve the following scenario:

**Example 4.** To open the vault of a company multiple people have to work together. The company owner, three managers, and three shift leaders each have a private access code for the vault. The personal access code of the company owner has a weight of 5, the codes of the managers each have a weight of 3, the access codes of the shift leaders each have a weight of 1. To open the vault, access codes with a combined weight of 5 or more are needed. The company owner can open the vault alone. At least two of the managers can open it together. Two shift leaders need an additional manager to open the vault.

Some WTSS are presented in [17][18][14].

**General Access Secret Sharing Schemes**

The previous schemes were able to map specific access structures efficiently. In [15], the multiple assignment scheme is proposed, where multiple shares are assigned to each shareholder. With this approach, general access structures can be realized, with the downside, that in the worst case a total of $O(n \cdot 2^n)$ shares have to be distributed to $n$ shareholders. A general access secret sharing scheme allows mapping every possible subgroup of shareholders into the access structure. Multiple schemes, like those presented in [3][4][22][26] improve the efficiency by reducing the number of shares or the size of each share.
Our contribution

Various scenarios can be mapped by using the displayed methods. Still, there are some scenarios where either, the amount of distributed shares, the computational complexity or the complexity of the secret sharing scheme can be drastically reduced: In Chapter 3.4 two specific use-cases are shown. Our contribution consists of modifications to the well-known secret sharing scheme of Shamir, and the compartmented secret sharing scheme proposed by Simmons [21], which is based on Shamir’s scheme. The modifications allow constructing general access schemes while reducing the complexity of the scheme which improves the computational complexity. Further, the number of shares can be reduced and many of the good properties of Shamir’s scheme, like, easy implementation, high understandability, and ideality can be retained.

Organization of the paper

The paper is structured as follows: Chapter 2 describes the backgrounds of secret sharing schemes and explains the used schemes. In Chapter 3 our contributions are described, Chapter 3.1 states the modifications to the threshold secret sharing scheme of Shamir, whereas in Chapter 3.2 the modifications to compartmented threshold secret sharing schemes are discussed. Further, the implications for realizing general access structures are shown and two specific use-cases are displayed. Finally, Chapter 4 concludes the work.

2 Secret Sharing Backgrounds

Definition 1 ((t, n)-Secret Sharing Scheme). A (t, n)-secret sharing scheme allows a dealer to distribute n shares \( S = \{S_1, \ldots, S_n\} \) of a secret \( S \), to the users \( U = \{U_1, \ldots, U_n\} \). Any set \( A \) of shares, with \( |A| \geq t \) can compute \( S \).

Definition 2 (Access Structure). A family \( \{A' \subseteq A : A' \text{ can reconstruct } S\} \) in a secret sharing scheme with secret \( S \) and shares \( A \) is called access structure.

The schemes proposed by Shamir and Blakley are called threshold secret sharing schemes because any subset of shares that reaches the threshold value can reveal the secret. A general access secret sharing scheme allows constructing all access structures.

Definition 3 (Perfect Secret Sharing Scheme). A secret sharing scheme is called perfect, if no set \( A' \) of shares allows learning anything about the secret, if \( A' \) is not in the access structure.

This means that correctly guessing the secret \( S \) with less than \( t \) shares in a \((t, n)\)-secret sharing scheme or any set of shares which is not part of the access structure has the same probability as guessing \( S \) without a single share.

Definition 4 (Ideal Secret Sharing Scheme). A secret sharing scheme is called ideal if it is perfect and the size of each shareholder’s share is in the same domain as the secret.
Algorithm 1 Generation of shares in the Shamir \((t, n)\)-secret sharing scheme. \(t\) defines the threshold value, \(n\) defines the amount of shares, \(S\) defines the secret, and \(U\) defines the set of shareholders.

1: procedure \text{Shamir}(t, n, S, U)  
2: \(S \leftarrow \emptyset\)  
3: for \(i \leftarrow 1, (t - 1)\) do  
4: \(a_i \leftarrow \) uniformly distributed random number from \(GF(p)\)  
5: end for  
6: \(f(x) \leftarrow S + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{t-1} \cdot x^{t-1} \mod p\)  
7: for \(i \leftarrow 1, n\) do  
8: \(S_i \leftarrow f(x_i)\)  
9: \(S \leftarrow S \cup S_i\)  
10: end for  
11: for all \(U_i \in U\) do  
12: Distribute corresponding \(S_i\)  
13: end for  
14: end procedure

Any scheme where a shareholder receives more than one share cannot be ideal. In the following, we modify the secret sharing scheme of Shamir. This scheme is well-known, easy to understand and to implement. The idea is to generate a polynomial \(f(x) = S + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{t-1} \cdot x^{t-1} \mod p\), where \(S\) is the secret and the coefficients \(a_1, a_2, \ldots, a_{t-1}\) are uniformly distributed random variables, each from \(GF(p)\), the Galois field of order \(p\). Each shareholder then receives a point \(S_i = f(x_i)\). The generation of shares is displayed in Algorithm 1.

\[
\begin{align*}
S + a_1 \cdot x_1 + a_2 \cdot x_1^2 + \cdots + a_{t-1} \cdot x_1^{t-1} &= S_1 \pmod{p} \\
S + a_1 \cdot x_2 + a_2 \cdot x_2^2 + \cdots + a_{t-1} \cdot x_2^{t-1} &= S_2 \pmod{p} \\
& \quad \vdots \\
S + a_1 \cdot x_n + a_2 \cdot x_n^2 + \cdots + a_{t-1} \cdot x_n^{t-1} &= S_n \pmod{p}
\end{align*}
\]  

(1)

Any set of \(t\) shareholders can obtain \(S\). The secret sharing scheme of Shamir is ideal \([6]\). For reconstruction, Equation System (1) can be used, but there are faster reconstruction procedures. Using the Lagrange polynomial interpolation \([25]\), the secret can be computed if the shareholders \(U_i\) calculate the following sum:

\[
S = \sum_i \left( S_i \cdot \prod_{i \neq j} \frac{-x_j}{x_i - x_j} \pmod{p} \right)
\]

(2)

Lemma 1. Calculating shares in Shamir’s scheme is in \(O(t \cdot n)\).

Proof. For generating shares \(t - 1\) random variables have to be chosen and the polynomial \(f(x)\), of degree \(t - 1\), has to be evaluated. Using Horner’s method \([12]\),
\(t - 1\) multiplications are needed for a single share. Therefore, for computing \(n\) shares \(t - 1 + n \cdot (t - 1) < t + t \cdot n\) calculations are needed. \(\Box\)

**Lemma 2.** Revealing \(S\) in Shamir’s secret sharing scheme is in \(O(t^2)\).

**Proof.** A shareholder \(i\) has to calculate the product of the share \(S_i\) and \((t - 1)\) times the given fraction. Therefore, \(t\) shareholders have to calculate \(t \cdot (t - 1) < t^2\) products. \(\Box\)

**Definition 5 (Compartmented Threshold Secret Sharing Scheme).** In a compartmented threshold secret sharing scheme with threshold \(t\) the users \(U\) are partitioned into compartments \(C = \{C_1, \ldots, C_m\}\), such that \(U = \bigcup_{i=1}^{m} C_i\). The Secret \(S\) can be computed, if a set \(A\) of compartments, with \(|A| \geq t\) combine their shares. Each compartment \(C_i\), can distribute the share \(S_i\) in a \((t_i, |C_i|)\)-secret sharing scheme to the \(|C_i|\) users.

In the following, the CTSS based on Shamir’s scheme, as proposed by Simmons is used. In the scheme a secret \(S\) is divided into shares \(S_i\) by generating a polynomial \(f(x)\) and then calculating a point \(f(x_i)\) for each compartment \(C_i\). In each compartment, then, another \((t, n)\)-secret sharing scheme is applied. I.e., each share \(S_i\) is a new secret inside the compartment, which is distributed to the users hold by the compartment. Generation of shares is displayed in Algorithm 2. To calculate the secret, in \(t\) compartments the users have to combine their shares using the Lagrange polynomial interpolation shown in Equation 2. With the \(t\) shares another polynomial interpolation has to be calculated to find \(S\).

**Algorithm 2** Generation of shares in the \((t, n)\)-compartment secret sharing scheme based on Shamir’s scheme. \(t\) defines the threshold value, \(n\) defines the amount of shares, \(S\) defines the secret, and \(C\) defines the set of compartments.

\begin{verbatim}
1: procedure COMPARTMENTEDSHAMIR\((t, n, S, C)\)
2:    \(S \leftarrow \emptyset\)
3:    for \(i \leftarrow 1, (t - 1)\) do
4:        \(a_i \leftarrow\) uniformly distributed random number from \(GF(p)\)
5:    end for
6:    \(f(x) \leftarrow S + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{t-1} \cdot x^{t-1} \mod p\)
7:    for \(i \leftarrow 1, n\) do
8:        \(S_i \leftarrow f(x_i)\)
9:        \(S \leftarrow S \cup S_i\)
10: end for
11: for all \(S_i\) in \(S\) do
12:    SHAMIR\((t, |C_i|, S_i, C_i)\)
13: end for
14: end procedure
\end{verbatim}
3 Our Approach

In the following, some modifications to Shamir’s scheme are introduced. Later, the respective modifications to the CTSS proposed by Simmons are discussed.

3.1 Secret Sharing

In Shamir’s secret sharing scheme each share has the same impact. Therefore, in a \((2, 4)\)-secret sharing scheme with the shares \(S_1, S_2, S_3,\) and \(S_4\) all sets \(\{S_i, S_j\}\), with \(i \neq j\) can retrieve the secret. The following modification allows to restrict the access group:

**Definition 6 (Crucial Share).** A share \(R\) is called crucial, if there exists no set \(A'\) of shares, with \(R \notin A'\), such that \(S\) can be computed.

By defining \(S_1\) as a crucial share the access group can be restricted to the following: \(\{\{S_1, S_2\}, \{S_1, S_3\}, \{S_1, S_4\}\}\).

**Lemma 3.** Any number of crucial shares can be introduced to the secret sharing scheme of Shamir, when \(S\) in the polynomial is replaced by a \(S'\), with \(S' = S + \sum_{i=1}^{r} R_i \mod p\), where each \(R_i\) is drawn uniformly random from \(GF(p)\).

**Proof.** The value \(S'\) of the modified polynomial can be found by using \(t\) linearly independent combinations of \(x_i\) and \(S_i\) to solve the following equation system:

\[
S' + a_1 \cdot x_1 + a_2 \cdot x_1^2 + \cdots + a_{t-1} \cdot x_1^{t-1} = S_1 \pmod p \\
S' + a_1 \cdot x_2 + a_2 \cdot x_2^2 + \cdots + a_{t-1} \cdot x_2^{t-1} = S_2 \pmod p \\
\vdots \\
S' + a_1 \cdot x_n + a_2 \cdot x_n^2 + \cdots + a_{t-1} \cdot x_n^{t-1} = S_n \pmod p
\]

Then, \(S\) then can be computed by subtracting all crucial shares from \(S'\):

\[
S = S' - \sum_{i=1}^{r} R_i \mod p.
\]

**Lemma 4.** The modified secret sharing scheme with crucial shares remains perfect.

**Proof.** Calculating the secret \(S\) in the modified secret sharing scheme is the combination of two problems. The first problem is finding the value \(S'\) for the polynomial \(f'(x) = S' + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{t-1} \cdot x^{t-1} \mod p\). Here, every set of combinations of \(x_i\) and \(S_i\), which is smaller than \(t\), leads to infinitely many possible polynomials. The next problem is finding \(S\) from \(S'\), which is moving the correct polynomial vertically. Having more than \(t\) linearly independent combinations of \(x_i\) and \(S_i\), does not help in computing \(S\), because the crucial shares \(R_i\) are independent of the points of the polynomial. Having less than \(r\) crucial shares leaves the shareholders with some \(S'' \neq S\). Finding \(S\) by using \(S''\) in a meaningful way is not possible because all crucial shares are independent. Therefore guessing \(S\) from this point is as effective, as guessing it without any knowledge.
Lemma 5. The modified secret sharing scheme with crucial shares remains ideal.

Proof. The modified scheme is perfect. Further, each value $R_i$ is a uniformly chosen random number out of $GF(p)$. The resulting points, when evaluating the polynomial remain in $GF(p)$. Therefore all shares and the secret are from the same domain. \hfill \Box

Another way of restricting the access group is by making shares less important than others. In a $(2,4)$-scheme with shares $S_1, S_2, S_3$, and $S_4$ the access group can be reduced to $\{\{S_1, S_3\}, \{S_1, S_4\}, \{S_2, S_3\}, \{S_2, S_4\}\}$ by not allowing to appear $S_1$ and $S_2$, or $S_3$ and $S_4$ in the same set. This can be achieved by redundant shares:

Definition 7 (Redundant Share). Two shares $R$ and $Q$, in a $(t,n)$-secret sharing scheme, are called redundant, if there exists no set $A'$ of shares, with $R, Q \in A'$ and $|A'| = t$, which can compute $S$.

Lemma 6. Redundant shares can be introduced to the scheme of Shamir by distributing the same share multiple times to different shareholders.

Proof. For finding $S$ in Shamir’s scheme least $t$ linearly independent combinations of $x_i$ and $S_i$ are needed. Any set of $s = t$ shares with at least two shares $j, k$ with $x_j = x_k, S_j = S_k$, and $j \neq k$ has at most $t - 1$ linearly independent shares. \hfill \Box

This allows introducing two or more redundant shares having the same value. Multiple redundant shares with different values can be used in the modified secret sharing scheme. We call any number of redundant shares corresponding to the same value mutual.

Lemma 7. The modified secret sharing scheme with redundant shares remains perfect.

Proof. Redundant shares are copies of normal shares. Knowing multiple mutual redundant shares results in the same amount of linearly independent pairs $x_i, S_i$ as having a single redundant share. \hfill \Box

Lemma 8. The modified secret sharing scheme with redundant shares remains ideal.

Proof. Redundant shares are copies of normal shares out of $GF(p)$. \hfill \Box

Generating and distributing shares in the modified $(t,n)$-secret sharing scheme, allowing both crucial and redundant schemes is displayed in Algorithm 3. To calculate the secret from the shares Equation 3 has to be evaluated.

\[
S = \sum_i \left( S_i \cdot \prod_{i \neq j} \frac{-x_j}{x_i - x_j} \mod p \right) - \sum_{k=1}^r R_k \mod p \tag{3}
\]
Lemma 9. Calculating shares in the modified scheme is in $O(t \cdot n)$.

Proof. $r$ crucial shares and $t - r - 1$ coefficients $a_i$ have to be drawn because each crucial share reduces the degree of the polynomial $f'(x)$ by one. A normal share $S_i$ is calculated by evaluating $f'(x)$, which needs $(t - r - 1)$ multiplications according to Horner’s method. Therefore, calculating $(n - r - d)$ normal shares and $r$ crucial shares needs $r + (t - r - 1) + (n - r - d) \cdot (t - r - 1) < t + t \cdot n$ calculations. Redundant shares need no additional calculations. \hfill \Box

Lemma 10. Reconstruction of $S$ in the modified scheme is in $O(t^2)$.

Proof. Each shareholder $U_i$ contributing a normal share or a unique redundant share has to calculate the product of the share $S_i$ and $(t - r - 1)$ times the given fraction. Afterwards, the sum of crucial shares $\sum_{k=1}^{r} R_k \mod p$ is subtracted. Therefore, the $(t - r)$ shareholders with a normal share have to calculate in total $(t - r) \cdot (t - r - 1) < t^2$ products, this equation holds because $t \geq r \geq 0$. \hfill \Box

Algorithm 3 Generation of shares in the modified Shamir $(t, n)$-secret sharing scheme with crucial and redundant shares. $t$ defines the threshold value, $n$ defines the amount of shares, $S$ defines the secret, $U$ defines the set of users, $r$ defines the number of crucial shares, and $d$ defines the number of additional redundant shares.

1: procedure ModifiedShamir($t, n, S, U, r, d$)
2: $S \leftarrow \emptyset$
3: for $i \leftarrow 1, (t - r - 1)$ do
4: \hspace{1cm} $a_i \leftarrow$ uniformly distributed random number from $GF(p)$
5: end for
6: for $i \leftarrow 1, r$ do
7: \hspace{1cm} $R_i \leftarrow$ uniformly distributed random number from $GF(p)$
8: end for
9: $S' \leftarrow \sum_{i=1}^{r} R_i \mod p$
10: $f'(x) \leftarrow S' + a_1 x + a_2 x^2 + \cdots + a_{t-r-1} x^{t-r-1} \mod p$
11: for $i \leftarrow 1, (n - r - d)$ do
12: \hspace{1cm} $S_i \leftarrow f(x_i)$
13: $S \leftarrow S \cup S_i$
14: end for
15: for all $U \in U$ do
16: \hspace{1cm} if $U$ gets crucial share then
17: \hspace{2cm} Distribute corresponding $R_U$
18: \hspace{1cm} else
19: \hspace{2cm} Distribute corresponding $S_U$
20: \hspace{1cm} end if
21: end for
22: end procedure

The modified scheme allows using multiple crucial and redundant shares at the same time. Therefore, the access structure can be more flexible. Crucial
shares in some way are a contradiction to the initial ideas behind secret sharing. Secret sharing can be used to retrieve a secret which was lost or forgotten. The possibility to lose the secret increases again, when crucial shares are used, because they can be lost, or shareholders might become malicious and stop helping in revealing the secret.

3.2 Compartmented Secret Sharing

With modifications to compartmented threshold secret sharing schemes the downside of using crucial shares can be offset, because similar to the previous chapter crucial compartments can be introduced, where a compartment is on the one hand needed for the reconstruction of the secret, but on the other hand multiple users help in reconstructing the share held by the compartment. Therefore, the following definitions are similar to the ones of secret sharing.

**Definition 8 (Crucial Compartment).** A compartment $R$ is called crucial, if there exists no set $A'$ of shares of compartments, with $R \notin A'$, such that $S$ can be computed.

Crucial compartments can be introduced to the scheme similar to the method shown in Lemma [3] by replacing $S$ with a $S' = S + \sum_{i=1}^{r} R_i \mod p$, where $R_i$ are the secrets of the crucial compartments. The secret sharing scheme inside a crucial compartment is independent of the one used in the outer scheme. Therefore, it can be another CTSS or a modified Shamir scheme.

**Definition 9 (Redundant Compartment).** Two compartments $R$ and $Q$ are called redundant, if there exists no set $A'$ of shares of compartments, with $R, Q \in A'$ and $|A'| = t$, which can compute $S$.

Additionally, redundant compartments can be introduced. Similar to Lemma [6] every redundant compartment receives the same secret, which leads to the case that only one of the mutual redundant compartments can help in revealing the secret. Again, the scheme inside the compartment is independent. Therefore, every redundant compartment can use another secret sharing scheme, a different number of shareholders, or different threshold values.

The computational complexity for the distribution of shares in the modified scheme and for reconstructing the secret is again in the same bounds, as the initial CTSS. Because as shown in Lemmas [9] and [10] sharing and reconstruction in the non-compartmented scheme remain in the same bounds.

3.3 Feasible Access Structures and Ideality

Following the remarks of [3] it is possible to construct the compartments for a CTSS to realize any access structure: Any formula in conjunctive normal form (CNF) can be mapped. Consider two shareholders $U_1, U_2$ in a $(2, 2)$-secret sharing scheme. Neither $U_1$, nor $U_2$ are sufficient to retrieve the secret on their own. Therefore, the specific secret sharing scheme realizes the AND operator. Whereas,
two shareholders $U_1$, $U_2$ in a $(1, 2)$-secret sharing scheme realize the or operator, because both can retrieve the secret on their own. Because both, the and and the or operator are possible to map, any formula in CNF can be mapped. Of course, the operators are not limited to be binary, but they can be $n$-ary.

Consider the following scenario: There are four users $U_1$, $U_2$, $U_3$, and $U_4$, which can retrieve the secret if $U_1$ with either $U_2$ or $U_3$ and one of $U_2$, $U_4$ work together. The formula in CNF is $(U_1 \land (U_2 \lor U_3) \land (U_2 \lor U_4))$. The CTSS has three compartments $C_1 = \{U_1\}$, $C_2 = \{U_2, U_3\}$, and $C_3 = \{U_2, U_4\}$, where $C_1$ holds only a single shareholder. The threshold is $t = 3$ in the outer scheme, and $t = 1$ in the inner schemes. In the given example the shareholder $U_2$ has to receive two independent and possibly unequal shares.

Previously, each level in the CTSS either could work as an and or an or operator. Now, by introducing the modifications to Shamir’s scheme and or operators can be used on the same level: Any crucial share $R$ is needed to retrieve a secret, therefore it is introducing another and operator. Two mutual redundant shares $S$ and $S'$ do not help in revealing the secret. Therefore, redundant shares introduce another kind of or operator. This or operator can be especially useful whenever a structure in the form $(A \land (B \lor C))$ appears, where $(B \land C)$ should not be allowed. The previous example can be mapped as a modified $(3, 4)$-secret sharing scheme with $U_1$ receiving a crucial share, $U_2$ receiving a normal share, and both $U_3$ and $U_4$ receiving the same redundant share. The secret can be retrieved, if $U_1$, $U_2$, and one of $U_3$ or $U_4$ work together. In this scheme every shareholder gets one single share, therefore it is ideal. Furthermore, no CTSS is needed. This reduces both the computational complexity and the total amount of shares.

Using crucial and redundant shares is not useful in every case. For example, every secret sharing scheme, where only two shareholders participate can be constructed without crucial and redundant shares: A scheme consisting solely of two redundant shares can be realized by a $(1, 2)$-secret sharing scheme. A scheme consisting solely of two crucial shares can be realized by a $(2, 2)$-secret sharing scheme, or by the much simpler method displayed in Chapter 1. A scheme consisting of a crucial and a normal share can be mapped by a $(2, 2)$-secret sharing scheme. In contrast, as soon as there are three shareholders the modifications can be useful. Consider a scheme consisting of a crucial share $R_1$, and two normal shares $S_1$ and $S_2$. The access structure is $(R_1 \land (S_1 \lor S_2))$. This scheme, previously, could only be mapped by using a CTSS. Another example would be a scheme consisting of a normal share $S_1$ and two redundant shares $S_2$ and $S'_2$. This scheme previously needed a compartmented scheme like in the example before, because the access structure is $(S_1 \land (S_2 \lor S'_2))$.

The modifications allow realizing general access structures with the advantage that in some cases no CTSS is needed, which reduces the computational complexity. In other cases, the number of shares can be reduced to only one share per participant, i.e. ideality can be achieved. Furthermore, in many of the cases, both advantages can be realized. In most other cases at least the complexity of the secret sharing scheme can be improved by reducing clauses.
3.4 Exemplary Use-cases

The introduced modifications allow creating complex access structures, like the following examples show:

**Example 5.** To open the vault of a company multiple people have to work together. The company owner, the head of security, three managers, and three shift leaders each have a private access code for the vault. Any combination of at least four codes can open the vault, but in any case, the codes of the owner and the head of security have to be two of them, and the remaining two codes cannot be both from shift leaders.

Example 5 can be mapped with the modified secret sharing as follows: Each manager receives a normal share from the dealer, the shift leaders each receive a mutual redundant share, and both the owner and the head of security receive crucial shares. The threshold is \( t = 2 \), the number of different shares is \( n = 4 \). This allows opening the vault if at most one share of a shift leader, together with one or two shares of the managers, and both shares from the owner and the head of security are used. The mapping is displayed in Figure 1.

**Example 6.** To open the vault of a company multiple people have to work together. There are three managers and their deputies for three departments. The staff in the departments can open the vault if there is a majority of staff in two departments. Additionally, two department leaders, either manager or deputy manager, of two different departments have to support them.

Example 6 can be mapped with the modified CTSS as follows: The three managers and their deputies form a crucial compartment, where the secret is shared in a \((2,3)\)-secret sharing. Each manager receives a normal share and the respective deputy each receives a redundant share. Therefore, the secret in the crucial compartment can be calculated if two managers, one manager, and another department’s deputy or two deputies combine their shares. The staff of each department \( i \) forms a compartment \( C_i \), where each secret is the share of a \((2,3)\)-secret sharing. The secret of a compartment \( C_i \) is distributed through

---

**Figure 1.** A solution to Example 5. The corresponding polynomial is \( f(x) = S' + a_1 \cdot x + a_2 \cdot x^2 \mod p \), with \( S' = S + R_1 + R_2 \mod p \). The secret can be computed when the shares \( R_1, R_2 \), and two unique shares of \( \{S_1, \ldots, S_4\} \) are combined.

---
a \((\lfloor \frac{n_i}{2} \rfloor + 1, n_i)\)-secret sharing. This allows computing a compartments secret if a majority of staff provides their shares. If two of the compartments provide their shares, together with the crucial share the secret can be computed. The proposed mapping is displayed in Figure 2.

![Diagram showing secret sharing compartments and crucial shares](image)

Fig. 2. A solution to Example 6. The corresponding polynomial for the compartmented secret sharing is \(f(x) = S' + a_1 \cdot x + a_2 \cdot x^2 \mod p\), with \(S' = S + R_1 \mod p\). The secret \(S\) can be computed, when two of the shares \(\{S_1, S_2, S_3\}\) and the share \(R_1\) are combined. \(R_1\) can be computed when two of the shares \(\{S_{R_1,1}, S_{R_1,2}, S_{R_1,3}\}\) are combined. Calculating a \(S_i\) needs \(\lfloor \frac{n_i}{2} \rfloor + 1\) of the shares in the compartment.

## 4 Conclusions

In this paper, we present simple modifications to the secret sharing scheme of Shamir. The modifications allow defining redundant shares which give no additional advance in computing the secret if more than one mutual redundant shares are used. Further, crucial shares can be defined which are essential for retrieving the secret. We showed, that these modifications are easy to understand and implement, that the resulting schemes still are ideal, and that the computational complexity is not worse than in the original scheme. Further, the modifications are introduced to the CTSS, as proposed by Simmons. The modifications can help in constructing complex access structures, like for the scenarios described in Chapter 3.4, by reducing the complexity of the access structure. Further, general access structures can be realized, where in some cases an optimal amount of distributed shares of one per shareholder can be achieved, i.e. the resulting scheme is ideal. In other cases, the computational complexity can be reduced compared to the naive approach.

## Acknowledgments

The authors acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the framework of SoNaTe (project number 16SV7405).
References

1. Ballico, E., Boato, G., Fontanari, C., Granelli, F.: Hierarchical secret sharing in ad hoc networks through birkhoff interpolation. In: Advances in Computer, Information, and Systems Sciences, and Engineering, pp. 157–164. Springer (2007)
2. Beimel, A., Weinreb, E.: Monotone circuits for monotone weighted threshold functions. Information Processing Letters 97(1), 12–18 (2006)
3. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Proceedings on Advances in cryptology. pp. 27–35. Springer-Verlag (1990)
4. Bertilsson, M., Ingemarsson, I.: A construction of practical secret sharing schemes using linear block codes. In: International Workshop on the Theory and Application of Cryptographic Techniques. pp. 67–79. Springer (1992)
5. Blakley, G.R., et al.: Safeguarding cryptographic keys. In: Proceedings of the national computer conference. vol. 48 (1979)
6. Brickell, E.F.: Some ideal secret sharing schemes. In: Workshop on the Theory and Application of of Cryptographic Techniques, pp. 468–475. Springer (1989)
7. Cooper, J., Donovan, D., Seberry, J.: Secret sharing schemes arising from latin squares (1994)
8. Farras, O., Padró, C.: Ideal hierarchical secret sharing schemes. IEEE transactions on information theory 58(5), 3273–3286 (2012)
9. Ghodosi, H., Pieprzyk, J., Safavi-Naini, R.: Secret sharing in multilevel and compartmented groups. In: Australasian Conference on Information Security and Privacy. pp. 367–378. Springer (1998)
10. Harn, L., Fuyou, M.: Multilevel threshold secret sharing based on the chinese remainder theorem. Information processing letters 114(9), 504–509 (2014)
11. Harn, L., Fuyou, M., Chang, C.C.: Verifiable secret sharing based on the chinese remainder theorem. Security and Communication Networks 7(6), 950–957 (2014)
12. Horner, W.: A new method of solving numerical equations of all orders, by continuous approximation. In: Abstracts of the Papers Printed in the Philosophical Transactions of the Royal Society of London. pp. 117–117. No. 2, The Royal Society London (1833)
13. Iftene, S.: Compartmented secret sharing based on the chinese remainder theorem. IACR Cryptology ePrint Archive 2005, 408 (2005)
14. Iftene, S., Boureanu, I.C.: Weighted threshold secret sharing based on the chinese remainder theorem. Scientific Annals of Cuza University 15(ARTICLE), 161–172 (2005)
15. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing general access structure. Electronics and Communications in Japan (Part III: Fundamental Electronic Science) 72(9), 56–64 (1989)
16. Lin, C., Harn, L., Ye, D.: Ideal perfect multilevel threshold secret sharing scheme. In: 2009 Fifth International Conference on Information Assurance and Security. vol. 2, pp. 118–121. IEEE (2009)
17. Morillo, P., Padró, C., Sáez, G., Villar, J.L.: Weighted threshold secret sharing schemes. Information Processing Letters 70(5), 211–216 (1999)
18. Padró, C., Sáez, G.: Secret sharing schemes with bipartite access structure. IEEE Transactions on Information Theory 46(7), 2596–2604 (2000)
19. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
20. Shima, K., Doi, H.: A hierarchical secret sharing scheme over finite fields of characteristic 2. Journal of Information Processing 25, 875–883 (2017)
21. Simmons, G.J.: How to (really) share a secret. In: Conference on the Theory and Application of Cryptography. pp. 390–448. Springer (1988)
22. Tan, K., Zhu, H.: General secret sharing scheme. Computer Communications 22(8), 755–757 (1999)
23. Tassa, T.: Hierarchical threshold secret sharing. In: Theory of Cryptography Conference. pp. 473–490. Springer (2004)
24. Tentu, A.N., Paul, P., Venkaiah, V.C.: Ideal and perfect hierarchical secret sharing schemes based on mds codes. IACR Cryptology ePrint Archive 2013, 189 (2013)
25. Waring, E.: Vii. problems concerning interpolations. Philosophical transactions of the royal society of London (69), 59–67 (1779)
26. Zhang, Y., Liu, Z., Huang, G.: Sure interpolation and its application to hierarchical threshold secret sharing scheme. In: 2008 International Symposium on Computer Science and Computational Technology. vol. 1, pp. 447–450. IEEE (2008)