Laboratoire d'Informatique Fondamentale, de Recherche Opérationnelle, de Combinatoire et d'Économétrie

Availaible on line at http://www.liforce.usthb.dz
bulletin-liforce@usthb.dz
Bulletin du Laboratoire 01 (2020) 01 - 14

An ideal hierarchical secret sharing scheme

GHANEM Meriem[1], **BOUROUBI Sadek**[2,*]

[1,2] USTHB, Faculty of Mathematics,
P.B. 32 El-Alia, 16111, Bab Ezzouar, Algiers, Algeria.

ghanem.meriem@gmail.com,
sbouroubi@usthb.dz or bouroubis@gmail.com

Résumé : One of the methods used in order to protect a secret K is a *secret sharing scheme*. In this scheme the secret K is distributed among a finite set of participants P by a special participant called the *dealer*, in such a way that only predefined subsets of participants can recover the secret after collaborating with their secret shares. The construction of secret sharing schemes has received a considerable attention of many searchers whose main goal was to improve the information rate. In this paper, we propose a novel construction of a secret sharing scheme which is based on the hierarchical concept of companies illustrated through its organization chart and represented by a tree. We proof that the proposed scheme is *ideal* by showing that the information rate equals 1. In order to show the efficiency of the proposed scheme, we discuss all possible kinds of attacks and proof that the security in ensured. Finally, we include a detailed didactic example for a small company organization chart.

Mots clés : Hierarchical secret sharing scheme; Qualified subsets; Access structure; Interpolation; Information rate.

2020 AMS Subject Classifications: 11T71; 94A60; 94A62

[*] Corresponding author.

1 Introduction

The fast development of computer networks and data communication systems make the protection of secret data extremely imperative. In order to protect a secret, several methods have been applied before, one of theme is to encrypt data, but this will change the problem instead of solving it, since another method is required to protect the encrypted data. It's also possible to keep the secret in one well-guarded location, but this method is very unreliable since the secret can be destroyed or become inaccessible. Another method consists in sharing the data, either by storing multiple copies of the data in different locations, which would increase security vulnerabilities, or by splitting the data into several parts and sharing them between different members of the system. This last method is called secret sharing scheme and would be very efficient in case where the reconstruction of the initial data does not require the presence of all the system members, otherwise the veto given to each member would paralyze the system [1]. Secret sharing schemes have many applications in different areas, such as access control, launching a missile, and opening a bank vault. For more details see for instance [16, 15].

The secret sharing scheme is therefore a method of distributing a secret K among a finite set of participants P, in such a way that only predefined subsets of participants can collaborate with their secret shares to recover the secret K. These subsets are called *qualified subsets* and the set of all qualified subsets is called the *access structure* denoted Γ [7]. Each subset of participants $Y \in \Gamma$ is called *a minimal qualified subset* if ($Y' \subset Y$ and $Y' \in \Gamma$) implies $Y' = Y$. The family of all minimal qualified subsets is noted Γ_0. In a secret sharing scheme, the secret K is chosen by a special participant, called the dealer, who is responsible for computing and distributing the shares among the set of participants P. The share of any participant refers specifically to the information that the dealer sends in private. It is required to keep the size of shares as small as possible since the security of a system degrades as the amount of information that must be kept secret increases.

Many approaches have been proposed for the construction of a secret sharing scheme [17]. The first one called (t,n)-*threshold scheme* was introduced independently by Shamir and Blakley [1, 5] in 1979. In a (t,n)-threshold scheme, all groups of at least t participants of n-participants are qualified and can reconstruct the secret, while those with less than t participants are unqualified and can't have any information about the secret. The scheme proposed by Shamir is based on polynomials over a finite field $GF(q)$ since a random polynomial f is chosen by the dealer for computing and distributing the shares among the set of participants P in such a way that, each participant p_i is given an ordered pair $(x_i, f(x_i))$ as a share. This scheme still reliable and secure even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces. This scheme is *perfect*, since all qualified subsets can reconstruct the secret and unqualified subsets cannot determine any information about the secret. The scheme is called *ideal*, if x_i is publicly revealed so that the share of participant p_i becomes just $f(x_i)$ and then the size of each share equals the size of the secret. The scheme proposed by Blakley is based on geometries over finite fields, it's perfect and can be modified slightly to become ideal, as explained by Ernest [7].

Ito et al. have generalized the concept of threshold scheme and showed that, given any *monotone access structure* Γ, i.e., for $Y \in \Gamma$, if $Y \subset Y'$ then $Y' \in \Gamma$, there exist a perfect secret sharing scheme to realize the structure [10, 9]. Benaloh and Leichter proposed a different algorithm that has a lower *information rate* than Ito's et al. construction [11]. In both constructions, the information rate decreases exponentially as a function of the number of participants $n = |P|$. The information rate, noted ρ, is considered as a measure of the efficiency of a secret sharing scheme. It is defined as the ratio between the secret size and the maximum size of the shares S, that is, $\rho = \frac{\log_2(|K|)}{\log_2(|S|)}$ [7]. Other measures can also be considered such as *the average information rate*, which is defined as the ratio between the length of the secret and the arithmetic mean of the length of all shares and expressed as follow $\widetilde{\rho} = \frac{n \log_2(|K|)}{\sum_{i=1}^{n} \log_2(|S_i|)}$ [12].

Another approach based on the *multilevel access structures* was presented by Simmons in 1988. In this approach each participant is assigned a level which is a positive integer and the access structure consists of those subsets which contain at least r participants all of level at most r. That means for instance if $r = 3$, then 3 participants of level 3 can determine the secret, and also 1 participant of level 1 and one other participant of level 2 and one participant of level 3 can determine the secret, for more details see for instance [8]. In [7] Brickell shown that given any multilevel access structure, there exists q_0 such that for any q a prime power with $q > q_0$, there is an ideal secret sharing scheme realizing this access structure over $GF(q)$.

There are also another approaches based on *graph access structure* that have received a considerable attention. In the most of these approaches, many researchers have proposed different constructions of a perfect secret sharing scheme based on uniform access structures which contains qualified subsets all of the same cardinality m. In these constructions, participants are represented by the vertices of a graph G, the uniform access structure Γ is based on the concept of adjacent vertices and represented by the edges, for more details see for instance [4, 18, 3, 14, 6, 13]. In [2] a novel approach to design a graph access structure, which is based on the concept of non-adjacent vertices, was proposed. In this approach, an independent dominating set of vertices in a graph G was introduced and applied as a novel idea to construct a perfect secret sharing scheme such that the vertices of the graph represent the participants and the dominating set of vertices in G represents the minimal qualified set.

2 The proposed construction algorithm

Shamir [1] had specified that one of the useful properties of the proposed threshold scheme is that by using tuples of polynomial values as parts, it is possible to get a hierarchical scheme in which the number of parts needed to determine the secret depends on the importance of the participants. He also brought a brief explanation based on an example of a company's check signature. The motivation of this paper is to propose a novel construction algorithm of an ideal secret sharing scheme which is based on the hierarchical concept of companies and in which the access structure is not uniform.The proposed construction algorithm include two phases which are achieved by the dealer who can, for instance, be represented by the board of directors (BOD) at a company.

2.1 The initialization phase

The hierarchical concept of any company is illustrated through its organization chart which is represented by a tree $T = (V, E)$ such that:

- The height of T corresponds to the number of hierarchical levels at the company, denoted h, and each hierarchical level is denoted N_j, for $j = 1, \ldots, h$.
- The set of vertices V corresponding to the company's employees represents the set of participants P. As each participant i belong to a specified level j, we denote by P_{ij} such participant.
- The set of edges E corresponds to the hierarchical relations between participants (employees).

Figure 1 given bellow, illustrates an organization chart of a company with 9 employees and 3 hierarchical levels.

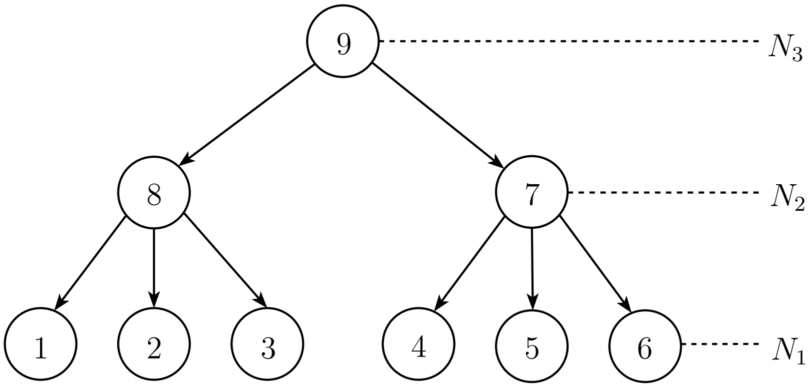

Figure 1: Company organization chart T with 9 employees.

In the initialization phase, the dealer proceed to the construction of the access structure Γ containing all the qualified subsets. A subset X of P is considered as qualified if and only if:

1. X contains more than one participant. No participant will have the veto right for reconstructing the secret alone, especially the first manager. This condition is formulated by:

$$\sum_{P_{ij}\in X} j \geq h+1.$$

2. The elements of X cannot all be at the same hierarchical level, in order to reduce the risk of corruption. This condition is expressed by:

$$|X \cap N_j| \leq \left\lceil \frac{h+1}{j} \right\rceil - 1, \text{ for } j = 1, \ldots, h.$$

The access structure Γ is then:

$$\Gamma = \left\{ X \subset P \ : \ \sum_{P_{ij}\in X} j \geq h+1 \text{ and } |X \cap N_j| \leq \left\lceil \frac{h+1}{j} \right\rceil - 1, \text{ for } j = 1, \ldots, h \right\}.$$

The minimum access structure Γ_0 is then

$$\Gamma_0 = \left\{ X \in \Gamma : \forall X' (X' \subsetneq X \Rightarrow X' \notin \Gamma) \right\}.$$

2.2 The decomposition phase

In this phase, the dealer:

- Choose a prime power number q;
- Select the secret to share $K = (k_1, \ldots, k_h)$ that he encodes in the finite field $GF(q)$;
- Generate randomly one value a_0 in $GF(q)$;
- Construct the polynomial $f(x)$ of degree h:

$$f(x) = a_0 + k_1 x + \cdots + k_h x^h;$$

- Calculate and distribute the shares to all participants. The share given to each participant P_{ij}, denoted S_{ij}, consists on two parts. The first one is publicly revealed and correspond to there login i and hierarchical level j. The second part is sent in private and consists on j values of ordered pairs $(x_{i1}, f(x_{i1})), \ldots, (x_{ij}, f(x_{ij}))$, so that the number of participants who can pool their shares to reconstruct the secret depends on their importance.

The following algorithm resumes the proposed construction of secret sharing scheme.

Algorithm 1 Construction of secret sharing scheme

Require:

1. The set of company's participants $P = \{P_{ij},\ i = 1, \ldots, n;\ j = 1, \ldots, h\}$;
2. A prime power q;
3. The polynomial $f(x) = a_0 + k_1 x + \cdots + k_h x^h$.

Ensure: The set of shares assigned to participants $S = \{S_{ij},\ i = 1, \ldots, n;\ j = 1, \ldots, h\}$.

```
For each participant $P_{ij}$, calculate $x_{im} = 1 + mih,\ m = 1, \ldots, j$;
Calculate $S_{ij} = (i, j, (x_{i1}, f(x_{i1})), (x_{i2}, f(x_{i2})), \ldots, (x_{ij}, f(x_{ij}))),\ i = 1, \ldots, n;\ j = 1, \ldots, h$;
Return: $S = \{S_{ij},\ i = 1, \ldots, n;\ j = 1, \ldots, h\}$.
```

According to Horner's method, Algorithm 1 can be achieved, in the worst case, in $O(nH)$ time complexity.

3 The proposed reconstruction algorithm

Let $K = (k_1, \ldots, k_h)$ be the secret shared over the finite set of participants P by application of Algorithm 1. According to the polynomial chosen by the dealer for calculating and distributing the shares, a group of participants X who want to collaborate with their shares in order to recover the secret K, should in first reconstruct the polynomial f, which can be done by interpolation, for that X should own at least $h+1$ values of ordered pairs, $(x_1, f(x_1)), \ldots, (x_{h+1}, f(x_{h+1}))$. The secret K can be recover by applying the logical XOR operator on the k_i's deduced from f:

$$K = k_1 \oplus k_2 \oplus \cdots \oplus k_h.$$

The proposed reconstruction is summarized in Algorithm 2.

Theorem 1 *The constructed secret sharing scheme is perfect.*

Preuve. Let X be a qualified subset of participants, then the conditions (i) and (ii), in the initialization phase 2.1 above, are satisfied. According to the decomposition phase 2.2, each P_{ij} belonging to X owns as much values of $(x, f(x))$ as his level j, $(x_{i1}, f(x_{i1})), \ldots, (x_{ij}, f(x_{ij}))$. Thus, X owns at least $h+1$ values of $(x, f(x))$ and can recover $f(x)$, by using interpolation, and then the secret K by applying the logical XOR operator on the k_i's deduced from f. Therefore, any qualified subset can reconstruct the secret.

Now, let X be an unqualified subset of participants, then one of the conditions (i) and (ii), in the initialization phase 2.1, is not satisfied. If the condition (i) is not, X owns less than $h+1$ values of $(x, f(x))$, which don't allow the reconstruction of $f(x)$. In the other hand, as the elements of X cannot all be at the same hierarchical level, if the condition (ii) is not satisfied, the system denies access. Therefore, any unqualified subset has no information about the secret. ■

Algorithm 2 Reconstruction of a secret K

Require:

1. A subset of participants $X \subset P$;
2. The set of hierarchical levels, $N_1, \ldots, N_h$;
3. The shares of participants belonging to X.

Ensure:

1. The secret $K = k_1 \oplus k_2 \oplus \cdots \oplus k_h$ or
2. The system denies access.

```
If $X \in \Gamma$ Then Apply interpolation to reconstruct $f(x)$ and then the secret $K$
                Else The system denies access and displays "The subset is not qualified".
```

4 The efficiency of the proposed secret sharing scheme

To measure the efficiency of the proposed secret sharing scheme, we consider the information rate $\rho = \dfrac{\log_2(|K|)}{\log_2(|S|)}$, where S is the maximum share.

Theorem 2 *The constructed secret sharing scheme is ideal.*

Preuve. The secret $K = (k_1, \ldots, k_h)$ is an h-dimensional vector such that each k_i, $i = 1 \ldots, h$, is in $GF(q)$. The k_i's length is then equal to $\log_2(q)$. According to the decomposition phase 2.2, each share S_{ij} is represented by a vector of $j+2$ components, in which j components are private. The maximum share S is the one corresponding to the first manager of the company which is at the high level h, its length is then equal to $h \log_2(q)$. Hence, $\rho = 1$. ■

5 Security analysis

The two main security requirements in a secret sharing scheme are confidentiality and authentication. Confidentiality is about ensuring that the information is only available to the qualified subsets, while the authentication is intended to ensure that each participant trying to collaborate in order to reconstruct the secret, is the one he claims to be.

In this paper, confidentiality has been demonstrated in Theorem 1 by proving that the proposed secret sharing scheme is perfect, while authentication is ensured by denying the access of all types of attacks. In fact, in such protocols, two types of attacks can arise: the insider and outsider attacks.

For the outsider attacks, where the attackers are not belonging to the system, the attacker aims to recover the secret by trying all possible combinations. As the secret K is an h-dimensional vector in which each component is in $GF(q)$, the number of possible combinations increases according to the number of hierarchical levels h. Thus, the brute force attack becomes a combinatorial explosion.

For the insider attacks, where the attackers are belonging to the system but consist on an unqualified subset of participants, as all parameters are public in the proposed scheme except the secret K, three types of insider attacks can arise:

- The first case consists on participant in level N_i who may pretend to be a participant of another lower level $N_j,\ j < i$, and use only a part of his share, in order to escape the condition (ii) described in the initialization phase 2.1. The following conditions (iii) and (iv) are then included in the proposed scheme and checked before proceeding to the reconstruction algorithm 2. In the case where these conditions are not satisfied, the system generates an authentication error and display an attack attempt message without executing the reconstruction algorithm 2.

  For each given share

  $$S_{ij} = \left(i, j, \left(x_{i1}, f(x_{i1})\right), \left(x_{i2}, f(x_{i2})\right), \ldots, \left(x_{ij}, f(x_{ij})\right)\right),\ i = 1, \ldots, n;\ j = 1, \ldots, h,$$

  3. The login i corresponds to a participant of the level j. This condition is formulated by:

     $$\forall S_{ij},\ i = 1, \ldots, n \text{ and } j = 1, \ldots, h;\ P_{ij} \in N_j.$$

  4. Each ordered pairs $(x_{im}, f(x_{im})),\ m = 1, \ldots, j$, corresponds to the one sent by the dealer to the participant i belonging to the level j. This condition is expressed by:

     $$\forall S_{ij},\ i = 1, \ldots, n \text{ and } j = 1, \ldots, h;\ \forall x_{im},\ m = 1, \ldots, j;\ x_{im} = 1 \ (\bmod\ ih) \text{ and } \left\lfloor \frac{x_{im}}{ih} \right\rfloor \leq j,$$

     where $\lfloor . \rfloor$ denotes the floor function.

- The second case of insider attacks consists on participants in the same level N_i, who are not allow to collaborate with their shares, according to condition (ii), in Section

2.1, trying to merge their shares to have only one and pretend to be a participant of another higher level $N_j,\ j > i$. This case is treated as the first case described above.

- The last case of insider attacks consists on participant in level N_i, who may pretend to be a participant of another higher level $N_j,\ j > i$, and try to calculate another value of $f(x)$. This case is similar to the outsider attacks described above.

6 Didactic example

Let consider the case of a company whose organization chart is represented by the tree T given in Figure 1 above. According to the initialization phase 2.1:

- The number of hierarchical levels $h = 3$.
- The set of participants $P = \{P_{11}, P_{21}, P_{31}, P_{41}, P_{51}, P_{61}, P_{72}, P_{82}, P_{93}\}$.
- According to their hierarchical levels, participants are assigned as follow:

  $N_1 = \{P_{11}, P_{21}, P_{31}, P_{41}, P_{51}, P_{61}\}$;

  $N_2 = \{P_{72}, P_{82}\}$;

  $N_3 = \{P_{93}\}$.
- The access structure Γ_0 containing all the minimal qualified subsets is given as follow:

$$\begin{aligned}\Gamma_0 =\{&\{P_{93}, P_{11}\},\ \{P_{93}, P_{21}\},\ \{P_{93}, P_{31}\},\ \{P_{93}, P_{41}\},\ \{P_{93}, P_{51}\},\ \{P_{93}, P_{61}\},\ \{P_{93}, P_{72}\},\\ &\{P_{93}, P_{82}\}, \{P_{82}, P_{11}, P_{21}\}, \{P_{82}, P_{11}, P_{31}\}, \{P_{82}, P_{11}, P_{41}\}, \{P_{82}, P_{11}, P_{51}\}, \{P_{82}, P_{11}, P_{61}\},\\ &\{P_{82},\ P_{21},\ P_{31}\},\ \{P_{82},\ P_{21},\ P_{41}\},\ \{P_{82},\ P_{21},\ P_{51}\},\ \{P_{82},\ P_{21},\ P_{61}\},\ \{P_{82},\ P_{31},\ P_{41}\},\\ &\{P_{82},\ P_{31},\ P_{51}\},\ \{P_{82},\ P_{31},\ P_{61}\},\ \{P_{82},\ P_{41},\ P_{51}\},\ \{P_{82},\ P_{41},\ P_{61}\},\ \{P_{82},\ P_{51},\ P_{61}\},\\ &\{P_{72},\ P_{11},\ P_{21}\},\ \{P_{72},\ P_{11},\ P_{31}\},\ \{P_{72},\ P_{11},\ P_{41}\},\ \{P_{72},\ P_{11},\ P_{51}\},\ \{P_{72},\ P_{11},\ P_{61}\},\\ &\{P_{72},\ P_{21},\ P_{31}\},\ \{P_{72},\ P_{21},\ P_{41}\},\ \{P_{72},\ P_{21},\ P_{51}\},\ \{P_{72},\ P_{21},\ P_{61}\},\ \{P_{72},\ P_{31},\ P_{41}\},\\ &\{P_{72},\ P_{31},\ P_{51}\},\ \{P_{72},\ P_{31},\ P_{61}\},\ \{P_{72},\ P_{41},\ P_{51}\},\ \{P_{72},\ P_{41},\ P_{61}\},\ \{P_{72},\ P_{51},\ P_{61}\}\}\end{aligned}$$

Suppose for instance that the key K is 32-bit integer and $q = 4294967311$ a prime number greater than $2^{32} - 1$. Based on the decomposition phase 2.2, let consider $k_1 = 4967295$, $k_2 = 94967$, $k_3 = 9496729$ and $a_0 = 429496$. The polynomial chosen by the dealer is then

$$f(x) = 429496 + 4967295x + 94967x^2 + 9496729x^3,$$

and the shares given to participants are:

$$\begin{aligned}S_{93} &= (9, 3, (x_{91}, f(x_{91})), (x_{92}, f(x_{92})), (x_{93}, f(x_{93})))\\ &= (9, 3, (28, 2527731964), (55, 31222823), (82, 1673628957));\end{aligned}$$

$$\begin{aligned}S_{72} &= (7, 2, (x_{71}, f(x_{71})), (x_{72}, f(x_{72})))\\ &= (7, 2, (22, 2492596253), (43, 3826770342));\end{aligned}$$

$$\begin{aligned}S_{82} &= (8, 2, (x_{81}, f(x_{81})), (x_{82}, f(x_{82}))\\ &= (8, 2, (25, 2541468297), (49, 1061011979));\end{aligned}$$

$$\begin{aligned}S_{11} &= (1, 1, (x_{11}, f(x_{11})))\\ &= (1, 1, (4, 629608804));\end{aligned}$$

$$\begin{aligned}S_{21} &= (2, 1, (x_{21}, f(x_{21})))\\ &= (2, 1, (7, 3297231991));\end{aligned}$$

$$\begin{aligned}S_{31} &= (3, 1, (x_{31}, f(x_{31})))\\ &= (3, 1, (10, 966393524));\end{aligned}$$

$$\begin{aligned}S_{41} &= (4, 1, (x_{41}, f(x_{41})))\\ &= (4, 1, (13, 3765498123));\end{aligned}$$

$$\begin{aligned}S_{51} &= (5, 1, (x_{51}, f(x_{51})))\\ &= (5, 1, (16, 348113953));\end{aligned}$$

$$\begin{aligned}S_{61} &= (6, 1, (x_{61}, f(x_{61})))\\ &= (6, 1, (19, 842645734)).\end{aligned}$$

It's clear that each qualified subset belonging to Γ_0 can recover the secret K.

Let's take for instance the qualified subset $X = \{P_{82}, P_{11}, P_{21}\}$. According to the reconstruction Algorithm 3, the polynomial f can be reconstruct by applying interpolation.

The polynomial L defined bellow is the unique polynomial of degree at most h satisfying $L(x_i) = y_i = f(x_i)$:

$$L(x) = \sum_{j=0}^{h} f(x_j) l_j(x), \text{ where } l_j(x) = \prod_{\substack{i=0\\ i\neq j}}^{h} \left(\frac{x - x_i}{x_j - x_i}\right).$$

For the considered qualified subset X, the h known values of $(x, f(x))$ are:

$x_0 = x_{81} = 25$	$f(x_0) = 2541468297$
$x_1 = x_{82} = 49$	$f(x_1) = 1061011979$
$x_2 = x_{11} = 4$	$f(x_2) = 629608804$
$x_3 = x_{21} = 7$	$f(x_3) = 3297231991$

Table 1: $(x, f(x))$ values of qualified subset.

Lagrange polynomials are calculated as follow:

$$\begin{aligned}
l_0(x) &= \frac{(x-49)(x-4)(x-7)}{(25-49)(25-4)(25-7)} = \frac{1}{9072}\,(-x^3+60x^2-567x+1372),\\
l_1(x) &= \frac{(x-25)(x-4)(x-7)}{(49-25)(49-4)(49-7)} = \frac{1}{45360}\,(x^3-36x^2+303x-700),\\
l_2(x) &= \frac{(x-25)(x-49)(x-7)}{(4-25)(4-49)(4-7)} = \frac{1}{2835}\,(-x^3+81x^2-1743x+8575),\\
l_3(x) &= \frac{(x-25)(x-49)(x-4)}{(7-25)(7-49)(7-4)} = \frac{1}{2268}\,(x^3-78x^2+1521x-4900)\,.
\end{aligned}$$

Hence

$$\begin{aligned}
L(x) &= 2541468297\; l_0(x) + 1061011979\; l_1(x) + 629608804\; l_2(x) + 3297231991\; l_3(x) \pmod q\\
&= f(x).
\end{aligned}$$

Therefore

	Decimal value	Binary value
k_1	4967295	010010111100101101111111
k_2	94967	000000010111001011110111
k_3	9496729	100100001110100010011001
$K = k_1 \oplus k_2 \oplus k_3$	14307601	110110100101000100010001

Table 2: Reconstruction of the secret K.

In case of insider attacks: as a first case of an insider attack, let's take the case in which the subset $\{P_{82}, P_{72}\}$, who is not qualified, try to reconstruct the secret by using the P_{82} share's as if it concerned those corresponding to participants P_{11} and P_{21}. For instance, instead of introducing the share S_{82} given above, P_{82} will introduce the following vectors S'_{11} and S'_{21} as shares of P_{11} and P_{21}, respectively:

$$\begin{aligned}
S'_{11} &= (1, 1, (x_{81}, f(x_{81}))) = (1, 1, (25, 2541468297)),\\
S'_{21} &= (1, 1, (x_{82}, f(x_{82}))) = (2, 1, (49, 1061011979)).
\end{aligned}$$

The condition (*iv*), in Section 5, is not satisfied in this case, since:

$$x_{81} = 1 \pmod 3, \text{ but } \left\lfloor \frac{x_{81}}{3} \right\rfloor > 1,$$

$$x_{82} = 1 \pmod 6, \text{ but } \left\lfloor \frac{x_{82}}{6} \right\rfloor > 1.$$

The system generates then an authentication error and display an attack attempt message.

As a second case of an insider attack, let's take the case in which the subset $\{P_{11}, P_{21}, P_{31}, P_{41}\}$, who is not qualified, according to condition (*ii*), in Section 2.1, try to reconstruct the secret by merging the shares of P_{31} and P_{41} and pretending to be the subset $\{P_{11}, P_{21}, P_{72}\}$ for instance.

In this case, instead of introducing the shares S_{31} and S_{41} given above, a merged share S'_{72} is introduced as if it was the one corresponding to the participant P_{72}:

$$S'_{72} = (7, 2, (x_{31}, f(x_{31})), (x_{41}, f(x_{41}))) = (7, 2, (10, 966393524), (13, 3765498123)).$$

The condition (*iv*), in Section 5, is not satisfied in this case, since

$$\left\lfloor \frac{x_{31}}{21} \right\rfloor < 2, \text{ but } x_{31} \neq 1 \pmod{21},$$

$$\left\lfloor \frac{x_{41}}{21} \right\rfloor < 2, \text{ but } x_{41} \neq 1 \pmod{21}.$$

The system generates then an authentication error and display an attack attempt message.

In case of outsider attacks: as all coefficients of f are taken in $GF(q)$, the attackers should try q^{h+1} possible combinations to reconstruct f. In our example, this requires 4294967311^4 possibilities, that exceeds 2^{116}.

7 Conclusion

In this paper, we first propose a novel construction of a secret sharing scheme, which is based on the hierarchical concept of companies. In the proposed scheme, polynomials are used over $GF(q)$ and the considered access structure is not uniform, since the number of parts needed to reconstruct the secret depends on the importance of the participants. We also present a reconstruction algorithm, in which the interpolation and the logical XOR are used to reconstruct the polynomial and recover the secret K, respectively. We show that the proposed scheme is perfect and ideal. Furthermore, the security of the proposed scheme is analyzed by discussing all possible kinds of attacks (insider and outsider) and proofing that confidentiality and authentication are ensured. Finally, we conclude by a detailed didactic example.

References

[1] Adi Shamir, How to share a secret, Communications of the ACM, 22, 612-613 (1979)

[2] AL-Saidi NMG, Rajab NA, Said MRMd, Kadhim KA, Perfect secret sharing scheme based on vertex domination set. International Journal of Computer Mathematics, 92, 1755-1763 (2014)

[3] Blundo C, De Santis A, Stinson DR, Vaccaro U, Graph decomposition and secret sharing schemes, Journal of Cryptology, 8, 39-64 (1995)

[4] Brickell EF, Stinson DR, Some improved bounds on the information rate of perfect secret sharing schemes, Journal of Cryptology, 5, 153-166 (1992)

[5] Blakley GR, Safeguarding cryptographic keys, AFIPS National Computer Conference, 313-317 (1979)

[6] Di Crescenzo G, Galdi C, Hyper-graph decomposition and secret sharing. Discrete Applied Mathematics, 157, 928-946 (2009)

[7] Ernest F, Brickell, Some ideal secret sharing schemes, Advances in Cryptology EUROCRYPT 89, 468-475. Springer, Berlin, Heidelberg (1990)

[8] Gustavus J, Simmons, How to (really) share a secret, Advances in Cryptology-CRYPTO'88, 390-448.Springer, New York, NY (1990)

[9] Ito M, Saito A, Nishizeki T, Multiple assignment scheme for sharing secret, Journal of Cryptology, 6, 15-20 (1993)

[10] Ito M, Saito A, Nishizeki T, Secret sharing scheme realizing general access structure, Electronics Communications in Japan, 72, 56-64 (1989)

[11] Josh C, Benaloh, Leichter Jerry, Generalized secret sharing and monotone functions, Advances in Cryptology-CRYPTO'88, 27-35.Springer, New York, NY (1990)

[12] Martin KM, New secret sharing schemes from old, Journal of Combinatorial Mathematics and Combinatorial Computing, 14, 65-77 (1993)

[13] Sun H, Wang H, Ku B, Pieprzyk J, Decomposition construction for secret sharing schemes with graph access structures in polynomial time, SIAM Journal on Discrete Mathematics, 24, 617-638 (2010)

[14] Sun H, Shieh S, Constructing Perfect Secret Sharing Schemes for General And Uniform Access Structure, Journal of information science and engineering, 15, 679-689 (1999)

[15] Simmons GJ, An introduction to shared secret and/or shared control schemes and their application, Contemporary Cryptology: The Science of Information Integrity, IEEE Press, 441-497 (1992)

[16] Simmons GJ, Jackson WA, Martin KM, The geometry of shared secret schemes, Bulletin of the Institute of Combinatorial Applications, 1, 71-88 (1991)

[17] Stinson DR, An Explication of Secret Sharing Schemes, Designs, Codes and Cryptography, 2, 357-390 (1992)

[18] Van Dijk M, On the information rate of perfect secret sharing schemes, Designs, Codes and Cryptography, 6, 143-169 (1995)