# A NEW HIERARCHICAL SECRET SHARING SCHEME

*Meriem GHANEM, Sadek BOUROUBI*
L'IFORCE Laboratory, Faculty of Mathematics, USTHB, Algiers, Algeria.

**ABSTRACT**

In order to protect a secret key $K$ from any possible destruction, loss or theft, the notion of "shared cryptography" was initiated in 1979 through the first secret sharing system presented by Adi Shamir. A secret sharing scheme is a method that allows to share confidential information $K$ between several people, called "participants", so that no participant fully possesses the secret and 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 researchers whose main goal was to improve performance. Inspired by the hierarchical concept existing in a company and which is illustrated through its organizational chart, we are interested in this paper to present a new hierarchical secret sharing scheme, which is at the same time simple and secure. In order to show the efficiency of the proposed scheme, we analyzed all the possible types of attacks in order to verify that the security is ensured. In the end, we presented a detailed didactic example for the application of the proposed scheme within a small company.

## 1. INTRODUCTION

In order to protect a secret, several methods have been applied before, one of them is to encrypt data, but this will change the problem instead of solving it, since another method is required to protect the encrypted data. Its 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 [7, 6].

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 $\Gamma$ [3]. 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 $\Gamma_0$. 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 $P$ and then assumed to be honest. 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 [8]. The first one, called $(t,n)$-*threshold scheme*, was introduced independently by Shamir and Blakley [1, 2] 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 is 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*, since $x_i$ 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 in [3].

The information rate, noted $\rho$, 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, $\rho = \frac{\log_2(|K|)}{\log_2(|S|)}$ [3]. 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 $\widetilde{\rho} = \frac{n\log_2(|K|)}{\sum_{i=1}^{n}\log_2(|S_i|)}$ [5].

Shamir had specified that one of the useful properties of the proposed threshold scheme is that by using tuples of polynomial values as parts [1], 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. This was a motivation for another line of work, consisting in construction of ideal secret sharing scheme for families of access structures with interesting and special properties, which was introduced by Simmons in 1988. In [4], Simmons proposed two families of access structure : *the multilevel and the compartmented access structures* which are *multipartite*. In such access structures, participants are divided into several parts (levels and compartments) and the participants of each part play an equivalent role into the structure. In a multilevel access structure, each participant is assigned according to their importance. Participants are then hierarchically ordered and those in the higher level are more powerful than the ones in lower levels. In [3] 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 $GF(q)$.

Related to that previous works and inspired by the hierarchical concept existing in a company and which is illustrated through its organizational chart, we propose in this article a new simpler hierarchical secret sharing scheme.

## 2. THE PROPOSED SECRET SHARING SCHEME

The proposed scheme includes three phases, two phases for the construction of the sharing scheme and the last phase for the reconstruction of the secret. These phases are achieved by the dealer who can, for instance, be represented by the board of directors 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 $T$, correspond 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).

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

1. 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 :

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

The access structure $\Gamma$ is then :

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

Finally, the minimum access structure $\Gamma_0$ is then :

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

### 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 :

$$\left(x_{i1}, f(x_{i1})\right), \ldots, \left(x_{ij}, f(x_{ij})\right),$$

so that the number of participants who can pool their shares to reconstruct the secret depends on their importance.

### 2.3. The reconstruction phase

Interpolation is used for the reconstruction of the secret. Indeed, 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, $(x_1, f(x_1)), \ldots, (x_{h+1}, f(x_{h+1}))$.

To ensure the security of the proposed scheme, the following conditions $(3)$ and $(4)$ are checked before proceeding to the reconstruction phase. 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 phase.

For each given share $S_{ij} = \big(i, j, (x_{i1}, f(x_{i1})), (x_{i2}, f(x_{i2})), \ldots, \big(x_{ij}, f(x_{ij})\big)\big)$,
$i = 1, \ldots, n;\ j = 1, \ldots, h$ :

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 pair $(x_{im}, f(x_{im}))$, $m = 1, \ldots, j$, corresponds to the one sent by the dealer to the participant $i$ belonging to the level $j$. This condition is expressed by :
$\forall S_{ij}, \forall x_{im}, x_{im} = 1 \pmod{ih}$ and $\left\lfloor \frac{x_{im}}{ih} \right\rfloor \leq j$, for $i = 1, \ldots, n,\ j = 1, \ldots, h$ and $m = 1, \ldots, j$ ;
where $\lfloor . \rfloor$ denotes the floor function.

## 3. THE EFFICIENCY OF THE PROPOSED SCHEME

The proposed scheme is perfect as only predefined subsets of participants can recover the secret. Indeed, if $X$ is a qualified subset of participants, then the conditions (1) and (2) 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 $K$. while, if $X$ is an unqualified subset of participants, then one of the conditions (1) and (2) in the initialization phase 2.1, is not satisfied. If the condition (1) 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 $(2)$ is not satisfied, the system denies access.

The proposed scheme is also ideal as $\rho = 1$. Indeed, 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 $h \log_2(q)$.

## 4. 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 the proposed scheme, confidentiality is ensured by the fact that the 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 $(2)$ described in the initialization phase 2.1. This kind of attacks is blocked by the conditions $(3)$ and $(4)$ checked before the reconstruction phase 2.3 .
- 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 $(2)$, 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.

## 5. DIDACTIC EXAMPLE

Let consider the case of a company whose organization chart is represented by the tree $T$ given in Figure 1 below.

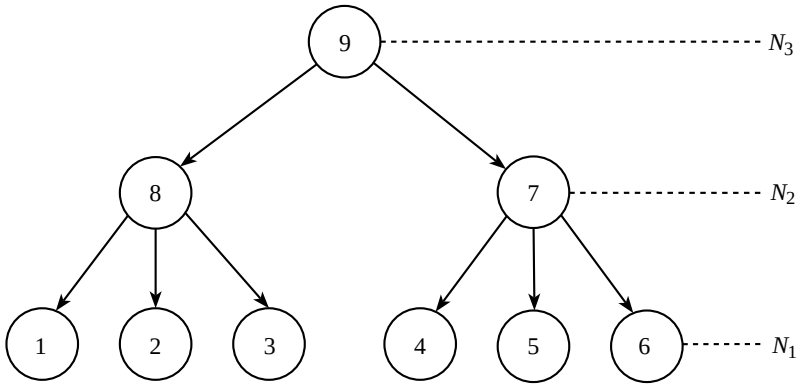


FIGURE 1 – Company organization chart $T$ with 9 employees.

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 :

$N_1 = \{P_{11}, P_{21}, P_{31}, P_{41}, P_{51}, P_{61}\}$, $N_2 = \{P_{72}, P_{82}\}$ and $N_3 = \{P_{93}\}$.

— The access structure $\Gamma_0$ 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 a 3-tuple of 32-bit integers 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 :

$$\begin{aligned}
S_{93} &= (9, 3, (x_{91}, f(x_{91})), (x_{92}, f(x_{92})), (x_{93}, f(x_{93})))\\
&= (9, 3, (28, 2527731964), (55, 31222823), (82, 1673628957));\\
S_{72} &= (7, 2, (x_{71}, f(x_{71})), (x_{72}, f(x_{72})))\\
&= (7, 2, (22, 2492596253), (43, 3826770342));\\
S_{82} &= (8, 2, (x_{81}, f(x_{81})), (x_{82}, f(x_{82}))\\
&= (8, 2, (25, 2541468297), (49, 1061011979));\\
S_{11} &= (1, 1, (x_{11}, f(x_{11})))\\
&= (1, 1, (4, 629608804));\\
S_{21} &= (2, 1, (x_{21}, f(x_{21})))\\
&= (2, 1, (7, 3297231991));\\
S_{31} &= (3, 1, (x_{31}, f(x_{31})))\\
&= (3, 1, (10, 966393524));\\
S_{41} &= (4, 1, (x_{41}, f(x_{41})))\\
&= (4, 1, (13, 3765498123));\\
S_{41} &= (4, 1, (x_{41}, f(x_{41})))\\
&= (4, 1, (13, 3765498123));\\
S_{41} &= (4, 1, (x_{41}, f(x_{41})))\\
&= (4, 1, (13, 3765498123));\\
S_{51} &= (5, 1, (x_{51}, f(x_{51})))\\
&= (5, 1, (16, 348113953));\\
S_{61} &= (6, 1, (x_{61}, f(x_{61})))\\
&= (6, 1, (19, 842645734)).
\end{aligned}$$

It's clear that each qualified subset belonging to $\Gamma_0$ can recover the secret $K$.

Let's take for instance the qualified subset $X = \{P_{82}, P_{11}, P_{21}\}$. According to the reconstruction phase 2.3, 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 : Lagrange polynomials

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

TABLE 1 – $(x, f(x))$ values of qualified subset $X = \{P_{82}, P_{11}, P_{21}\}$.

are calculated as follow :

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

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 **In case of insider attacks** : as a first case of an insider attack, let's take the case in

| | $k_i$'s value |
|---|---|
| $k_1$ | 4967295 |
| $k_2$ | 94967 |
| $k_3$ | 9496729 |

TABLE 2 – Reconstruction of the secret $K$.

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 :

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

The condition (4), in Section 2.3, is not satisfied in this case, since :

$$x_{81} = 1 \ (\mathrm{mod}\ 3), \text{ but } \left\lfloor \frac{x_{81}}{3} \right\rfloor > 1,$$

$$x_{82} = 1 \ (\mathrm{mod}\ 6), \text{ but } \left\lfloor \frac{x_{82}}{6} \right\rfloor > 1.$$

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 (2) 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 (4), in Section 2.3, is not satisfied in this case, since

$$\left\lfloor \frac{x_{31}}{21} \right\rfloor < 2, \text{ but } x_{31} = 10 \ (\mathrm{mod}\ 21),$$

$$\left\lfloor \frac{x_{41}}{21} \right\rfloor < 2, \text{ but } x_{41} = 13 \ (\mathrm{mod}\ 21).$$

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 $2^{128}$.

## 6. CONCLUSIONS

In this paper, we were interested on the hierarchical concept of companies illustrated through its organization char. We propose a novel simple hierarchical secret sharing scheme, where the access structure is a tree and not uniform since the number of parts needed to reconstruct the secret depends on the importance of the participants within the company. We show that the proposed scheme is perfect and ideal. Furthermore, the security of the proposed scheme is analysed 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.

## 7. REFERENCES

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

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

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

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

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

[6] 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)

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

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