Ideal and Perfect Hierarchical Secret Sharing Schemes based on MDS codes ☆

Appala Naidu Tentu[a], Prabal Paul[b], V Ch Venkaiah[c,*]

[a]*C. R. Rao Advanced Institute of Mathematics, Statistics, and Computer Science*
University of Hyderabad Campus, Hyderabad-500046, India
[b]*Department of Mathematics*
Birla Institute of Technology & Science, Pilani, Goa Campus
GOA-403726, India
[c]*Department of Computer and Information Sciences*
University of Hyderabad, Hyderabad-500046, India

Abstract

An ideal conjunctive hierarchical secret sharing scheme, constructed based on the Maximum Distance Separable (MDS) codes, is proposed in this paper. The scheme, what we call, is computationally perfect. By computationally perfect, we mean, an authorized set can always reconstruct the secret in polynomial time whereas for an unauthorized set this is computationally hard. Also, in our scheme, the size of the ground field is independent of the parameters of the access structure. Further, it is efficient and requires $O(n^3)$, where n is the number of participants.

Keywords:
Computationally perfect, Ideal, Secret sharing scheme, Conjunctive hierarchical access structure, Disjunctive hierarchical access structure, MDS code.

AMS Classification: 94A62, 94B05.

☆authors names follow the alphabetical ordering

*Corresponding author

Email addresses: naidunit@gmail.com (Appala Naidu Tentu), prabal.paul@gmail.com (Prabal Paul), venkaiah@hotmail.com (V Ch Venkaiah)

1. Introduction

Secret sharing is a cryptographic primitive, which is used to distribute a secret among participants in such a way that an authorized subset of participants can uniquely reconstruct the secret and an unauthorized subset can get no information about the secret in the information theoretic sense. It is a fundamental method used in secure multiparty computations, where various distrusted participants cooperate and conduct computation tasks based on the private data they provide.

A secret sharing scheme is called ideal if the maximal length of shares and the length of the secret are identical. Secret sharing was first proposed independently by Blakley [5] and Shamir [23]. The scheme by Shamir relies on the standard Lagrange polynomial interpolation, whereas the scheme by Blakley is based on the geometric idea that uses the concept of intersecting hyper planes.

The family of authorized subsets is known as the access structure. An access structure is said to be monotone if a set is qualified then its superset must also be qualified. Several access structures are proposed in the literature. They include the (t, n)-threshold access structure, the Generalized access structure and the Multipartite access structure. In (t, n)-threshold access structure there are n shareholders, an authorized group consists of any t or more participants and any group of at most $t-1$ participants is an unauthorized group. Let $\mathbb{U}$ be the set of n participants and let $2^{\mathbb{U}}$ be its power set. Then 'Generalized access structure' refers to situations where the collection of permissible subsets of $\mathbb{U}$ may be any collection $\Gamma \subseteq 2^{\mathbb{U}}$ having the monotonicity property. In multipartite access structures, the set of players $\mathbb{U}$ is partitioned into m disjoint entities $\mathbb{U}_1, \mathbb{U}_2, \cdots, \mathbb{U}_m$, called levels and all players in each level play exactly the same role inside the access structure.

Conjunctive hierarchical access structure is a multipartite access structure in which each level $\mathbb{U}_i$ is assigned with a threshold t_i for $1 \leq i \leq m$, and the secret can be reconstructed when, for every i, there are at least t_i shareholders who all belong to levels smaller than or equal to $\mathbb{U}_i$. Formally,

$$\Gamma = \{\mathbb{V} \subseteq \mathbb{U} : |\mathbb{V} \cap (\bigcup_{j=1}^{i} \mathbb{U}_j)| \geq t_i, \text{ for all } i \in \{1, 2, \cdots, m\}\}.$$

Whereas in disjunctive hierarchical access structure we have

$$\Gamma = \{\mathbb{V} \subseteq \mathbb{U} : |\mathbb{V} \cap (\bigcup_{j=1}^{i} \mathbb{U}_j)| \geq t_i, \text{ for some } i \in \{1, 2, \cdots, m\}\}.$$

A secret sharing scheme is a perfect realization of Γ if for all $A \in \Gamma$, the users in A can always reconstruct the secret and for all B not in Γ, the users in B collectively cannot learn anything about the secret, in the information theoretic sense.

The motivation for this study is to come up with an hierarchical scheme that is ideal, efficient, that does not require the ground field to be extremely large, and that offers no restrictions in assigning identities to the users. The proposed scheme is computationally perfect. By computationally perfect, we mean, an authorized set can always reconstruct the secret in polynomial time whereas for an unauthorized set this is computationally hard. This is in contrast to the majority of the schemes found in the literature, which are perfect in a probabilistic manner. A scheme is perfect in a probabilistic manner if either an authorized set may not be able to reconstruct the secret or an unauthorized set may be able to reconstruct the secret with some probability [17].

An $[n, k, d]$ block code over $\mathbb{F}_q$ is called Maximum Distance Separable (MDS) code if $d = n - k + 1$. Two important properties, namely, any k columns of a generator matrix are linearly independent and any k symbols of a codeword may be taken as message symbols, of MDS codes have been exploited in the construction of our schemes. It may be noted that for any $k, 1 \leq k \leq q - 1$, and $k \leq n \leq q - 1$ there is an $[n, k, n - k + 1]$ MDS code and an $[q, k, q - k + 1]$ extended Reed Solomon code. Also, for any $k, 1 \leq k \leq q + 1$, there is an $[q + 1, k, q - k + 1]$ code over $\mathbb{F}_q$.

1.1. Related Work

Shamir [23] pointed out that a hierarchical variant of threshold secret sharing scheme can be introduced simply by assigning larger number of shares to higher level participants. However, such a solution can be easily seen to be not ideal.

Kothari [16] introduced a scheme that is a generalization of schemes of Blakley, Shamir, Bloom, and Karnin et al. [5, 23, 14, 16]. This generalized scheme is used to arrive at a hierarchical scheme, which provides different levels of shares [16]. At each level a set of linear equations is to be solved to obtain the secret. The size of the set of linear equations to be solved is a function of the level.

The earliest disjunctive secret sharing scheme is due to Simmons [24, 3], which is not ideal [15]. It is also inefficient because the dealer needs to check, possibly exponentially, many matrices for non-singularity [3] [26]. It is mentioned in [17] that finding an efficient, ideal, and linear solution for the disjunctive case of Simmons' has remained a long standing open problem and its realization became possible only when some duality techniques were employed to the efficient and perfect vector space construction of its conjunctive counter part. Brickell [7] offered two schemes for the disjunctive case, both ideal [26]. Both the schemes are inefficient [15]. One of the schemes suffers from the same problem as that of Simmons', while the other scheme requires to find an algebraic number satisfying an irreducible polynomial over the finite field [26]. The multilevel threshold scheme by Ghodosi et al. [12] work only for small number of shareholders [18, 3].

Tassa [26] and Tassa and Dyn [27] proposed ideal secret sharing schemes, based on Birkhoff interpolation and bivariate interpolation respectively, for several families of multipartite access structures that contain the multilevel and compartmented ones. These schemes either require a large finite field with some restrictions in assigning identities to the users [3] [27] [26] [1] or perfect in a probabilistic manner [17]. A scheme is perfect in a probabilistic manner if either an authorized set may not be able to reconstruct the secret or an unauthorized set may be able to reconstruct the secret with some probability.

Constructions of ideal secret sharing schemes for variants of the multilevel access structures and for some tripartite access structures have been given also in [2, 3, 13, 21, 10, 11]. The problem of secret sharing in hierarchical (or multilevel) structures, was studied under different assumptions also in [4, 8, 9, 25].

Linear codes have been used earlier in some constructions of threshold schemes [20, 14, 19, 22]. Blakley and Kabatianski [6] have established that ideal perfect threshold secret sharing schemes and MDS codes are equivalent.

1.2. Our Results

In this paper, we propose an ideal secret sharing scheme for conjunctive access structure. In fact, we have another scheme which is both ideal and perfect in the information theoretic sense for the disjunctive access structure. However, we present only the former scheme because of the space constraints.

This scheme, what we call, is computationally perfect and relies on the following hardness assumption. The construction of these schemes is based on the maximum distance separable (MDS) codes.

1.2.1. Assumption

Let $a \in \mathbb{F}_q$ and $f_i : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $1 \leq i \leq m$, be a set of distinct one way functions. Also, let $f_i(a) = b_i$ for $1 \leq i \leq m$. Then the computation of a from the knowledge of b_i, $i \in S$, where $S \subseteq \{1, 2, \cdots, m\}$ is computationally hard.

Novelty of our schemes is that they overcome all the limitations present in most of the existing schemes. The size of the ground field, in our schemes, is independent of the parameters of the access structure and there are no restrictions in assigning identities to the participants. Our schemes are applicable for any number of participants. They are efficient and require $O(n^3)$, where n is the number of participants, computation for Setup, Distribution, and Recovery phases.

1.3. Organization of the Paper

Section 2 describes the proposed conjunctive hierarchical secret sharing scheme and has an example that illustrates the scheme. Complexity analysis and correctness of the scheme is discussed in section 3. Conclusions are given in section 4.

2. Conjunctive Hierarchical secret sharing scheme

Let $U = \bigcup_{i=1}^{m} U_i$ be the set of participants partitioned into m disjoint sets $U_i, 1 \leq i \leq m$. Also, let $|U_i| = n_i$, for $i \in \{1, 2, \cdots, m\}$. Further, let t_1, t_2, $\cdots$, t_{m-1} and t_m be m positive integers such that $t_i < t_{i+1}$ for $1 \leq i \leq m-1$. Denote $\sum_{i=1}^{m} n_i + 1$ by N and $2N - t_m$ by n. Let $s \in \mathbb{F}_q$ be the secret to be shared. Also, let $f_i : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $1 \leq i \leq m$, be a set of distinct one way functions.

2.1. Overview of the scheme

Here the secret s to be shared is split as $s = s_1 + s_2 + \cdots + s_m \mod q$. The dealer then selects an $[n, N, n - N + 1]$ MDS code, m distinct one way functions $f_i, 1 \leq i \leq m$, and chooses m codewords of the selected MDS code. The choice of the $i^{th}, 1 \leq i \leq m$, codeword is such that the first component of the codeword is s_i, next n_1 components of the codeword are the images of the shares of the first level participants under the one way function f_i, next n_2 components of the codeword are the images of the shares of the second level participants under the same one way function f_i, and so on it goes upto the images of the shares of the i^{th} level participants under the same one way function f_i. The rest of the components of the codeword are chosen arbitrarily.

$N - t_i$ of these arbitrarily chosen components of the i^{th} codeword are made public so that if any t_i participants from the first i levels cooperate they can, with the help of the $N - t_i$ public shares, reconstruct the i^{th} codeword uniquely and hence can recover the first component, s_i, of this codeword, which is a term in the sum of the partial secrets.

2.2. Setup and Distribution phase

Following steps constitute this phase.

step 1 Select an $[n, N, n - N + 1]$ MDS code over $\mathbb{F}_q$.

step 2 Choose arbitrarily $s_i \in \mathbb{F}_q, 1 \leq i \leq m$, such that $s = s_1 + s_2 + \cdots + s_m$.

Step 3 Choose $v_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n_i$, from the elements of $\mathbb{F}_q$. Compute $v^k_{i,j} = f_k(v_{i,j})$, $1 \leq i \leq m$, $1 \leq j \leq n_i$, $i \leq k \leq m$. Distribute $v_{i,j}, 1 \leq i \leq m, 1 \leq j \leq n_i$, to the j^{th} player in the i^{th} compartment.

step 4 Choose m codewords

$$C_i = (s_i, v^i_{1,1}, v^i_{1,2}, \cdots, v^i_{1,n_1}, v^i_{2,1}, \cdots, v^i_{2,n_2}, \cdots, v^i_{i,1}, v^i_{i,2}, \cdots, v^i_{i,n_i}, \\ u_{i,\sum_{j=1}^{i} n_j+2}, u_{i,\sum_{j=1}^{i} n_j+3}, \cdots, u_{i,\sum_{j=1}^{m} n_j+\sum_{j=1}^{m}(n_j)-t_m+2}), \quad 1 \leq i \leq m,$$

of the above mentioned MDS code.

step 5 Publish f_i, $1 \leq i \leq m$.

step 6 Publish $u_{i,j}, j \in S_i$, as public shares corresponding to the codeword C_i, $1 \leq i \leq m$, where $S_i \subseteq \{\ell : \sum_{j=1}^{i} n_j + 2 \leq \ell \leq n\}$ and $\mid S_i \mid = N - t_i$.

step 7 Also publish the generator matrix of the MDS code.

2.3. Recovery phase

If at least t_i players cooperate they will be able to reconstruct the codeword C_i, $1 \leq i \leq m$, and hence its first component s_i, which is a term in the sum of the secret s. So, if at least t_i players participate for every i, $1 \leq i \leq m$, they will be able to recover all the terms of the sum and hence the secret. Assume that $j_r, 1 \leq r \leq m$, such that $\sum_{r=1}^{k} j_r \geq t_k$ for every $k, 1 \leq k \leq m$, players participate from the r^{th} level in the recovery phase. Also, assume that $l_{1,r}$, $l_{2,r}$, $\cdots$, $l_{j_r,r}$, be the corresponding indices of the cooperating players of the r^{th}, $1 \leq r \leq m$, level. Then the recovery phase consists of the following steps:

step 1 Fix i such that $1 \leq i \leq m$. Select $N - \sum_{k=1}^{i} j_k$ public shares to recover the codeword C_i. Let the indices of these public shares be $l_{1,m+1}, l_{2,m+1}, \cdots, l_{(N-\sum_{k=1}^{i} j_k),m+1}$.

step 2 Reduce, using the elementary row operations, the generator matrix to another matrix that has the following structure:
a) $(l_{t,1}+1)^{th}, 1 \leq t \leq j_1$, column of the generator matrix has 1 in the t^{th} row and zeros elsewhere,
b)$(\sum_{j=1}^{k-1} n_j + l_{t,k} + 1)^{th}, 2 \leq k \leq i, 1 \leq t \leq j_k$, column of the generator matrix has 1 in the $(\sum_{r=1}^{k-1} j_r + t)^{th}$ row and zeros elsewhere,
c) $(\sum_{j=1}^{i} n_j + l_{t,m+1} + 1)^{th}, 1 \leq t \leq \sum_{k=1}^{m} n_k + 1 - \sum_{k=1}^{i} j_k$, column of the generator matrix has 1 in the $(\sum_{r=1}^{i} j_r + t)^{th}$ row and zeros elsewhere.

step 3 Cooperating participant computes $f_i(v_{k,l_{tk}})$, $1 \leq k \leq i$, $1 \leq t \leq j_k$, and sends it as the participant's share in the recovery of the codeword C_i.

step 4 Form the message vector as
$(v_{1,l_{11}}^{i}, v_{1,l_{21}}^{i}, \cdots, v_{1,l_{j_11}}^{i}, v_{2,l_{12}}^{i}, v_{2,l_{22}}^{i}, \cdots, v_{2,l_{j_22}}^{i}, \cdots v_{i,l_{1i}}^{i}, v_{i,l_{2i}}^{i}, \cdots, v_{i,l_{j_ii}}^{i},$
$u_{i,\sum_{j=1}^{i}(n_j)+1+l_{1,m+1}}, u_{i,\sum_{j=1}^{i}(n_j)+1+l_{2,m+1}}, \cdots, u_{i,\sum_{j=1}^{i}(n_j)+1+l_{(\sum_{k=1}^{m} n_k+1-\sum_{k=1}^{i} j_k),m+1}})$.

step 5 Multiply the reduced generator matrix computed in step 2 by the message vector formed in step 4 to arrive at a codeword. First component of the resulting codeword is the i^{th} component (i.e.,s_i) in the sum of the secret to be recovered, which is s.

step 6 Do steps 1 to 5 to recover s_i, $1 \leq i \leq m$.

step 7 Recover the secret $s = \sum_{i=1}^{m} s_i$.

2.4. Example

Let $n_1 = 2, n_2 = 3, n_3 = 2$ and $t_1 = 1, t_2 = 2, t_3 = 4$. So, we consider a $[12, 8, 5]$ MDS code over $\mathbb{F}_{19}$. Let the chosen one way functions $f_i, 1 \leq i \leq 3$

be the modulo exponentials of the primitive elements 2,3 and 13 respectively. Further, let the secret s to be shared be 8.

2.4.1. Distribution phase

step 2 Choose arbitrarily $s_1 = 5$, $s_2 = 7$ and $s_3 = 15$ so that $s_1 + s_2 + s_3 = 8$.

step 3 Choose $v_{1,1} = 5, v_{1,2} = 17$ and distribute as the shares of the participants of the 1^{st} level. Similarly, choose $v_{2,1} = 6, v_{2,2} = 10, v_{2,3} = 9$ to 2^{nd} level $v_{3,1} = 16, v_{3,2} = 18$ to 3^{rd} level.
Compute $v^1_{1,1} = f_1(v_{1,1}) = 2^5 = 13, v^1_{1,2} = f_1(v_{1,2}) = 2^{17} = 10; v^2_{1,1} = f_2(v_{1,1}) = 3^5 = 15, v^2_{1,2} = f_2(v_{1,2}) = 3^{17} = 13, v^2_{2,1} = f_2(v_{2,1}) = 3^6 = 7, v^2_{2,2} = f_2(v_{2,2}) = 3^{10} = 16, v^2_{2,3} = f_2(v_{2,3}) = 3^9 = 18$. Similarly $v^3_{1,1} = 14, v^3_{1,2} = 3, v^3_{2,1} = 11, v^3_{2,2} = 6, v^3_{2,3} = 18, v^3_{3,1} = 9$, and $v^3_{3,2} = 1$.

step 4 Choose 3 codewords as
$C_1 = (s_1, v^1_{1,1}, v^1_{1,2}, u_{1,4}, u_{1,5}, \cdots, u_{1,11}, u_{1,12})$
$= (5, 13, 10, 2, 4, 17, 15, 14, 10, 10, 0, 17)$
$C_2 = (s_2, v^2_{1,1}, v^2_{1,2}, v^2_{2,1}, v^2_{2,2}, v^2_{2,3}, u_{2,7}, u_{2,8}, \cdots, u_{2,11}, u_{2,12})$
$= (7, 15, 13, 7, 16, 18, 1, 12, 2, 6, 0, 12)$
$C_3 = (s_3, v^3_{1,1}, v^3_{1,2}, v^3_{2,1}, v^3_{2,2}, v^3_{2,3}, v^3_{3,1}, v^3_{3,2}, u_{3,9}, \cdots, u_{3,12})$
$= (15, 14, 3, 11, 6, 18, 9, 1, 4, 8, 18, 16)$.

step 5 Publish the chosen one way functions $f_1(a) = 2^a \mod 19, f_2(a) = 3^a \mod 19$, and $f_3(a) = 13^a \mod 19$.

step 6 Choose S_1 such that $|S_1| = N - t_1 = 8 - 1 = 7$ and is a subset of $\{l : 4 \leq l \leq 12\}$. Let $S_1 = \{4, 5, 7, 8, 9, 11, 12\}$.

Also choose S_2 such that $|S_2| = 8 - t_2 = 8 - 2 = 6$ and is subset of $\{l : 7 \leq l \leq 12\}$. Let $S_2 = \{7, 8, 9, 10, 11, 12\}$.

Finally choose S_3 such that $|S_3| = 8 - t_3 = 4$ and is a subset of $\{l : 9 \leq l \leq 12\}$. Let $S_3 = \{9, 10, 11, 12\}$.

Publish $u_{1,4} = 2, u_{1,5} = 4, u_{1,7} = 15, u_{1,8} = 14, u_{1,9} = 10, u_{1,11} = 0$ and $u_{1,12} = 17$ as the public shares corresponding to C_1.

Also publish $u_{2,7} = 1, u_{2,8} = 12, u_{2,9} = 2, u_{2,10} = 6, u_{2,11} = 0, u_{2,12} = 12$ as the public shares corresponding to C_2.

Finally publish $u_{3,9} = 4, u_{3,10} = 8, u_{3,11} = 18, u_{3,12} = 16$ as the public shares corresponding to C_3.

2.4.2. Recovery phase

Assume that one participant from the first level, two participants from the 2^{nd} level, and two participants from the 3^{rd} level are cooperating to recover the secret. That is, $j_1 = 1$,$j_2 = 2$, and $j_3 = 2$. Also, assume that $l_{1,1} = 2$, $l_{1,2} = 1$, $l_{2,2} = 3$, $l_{1,3} = 1$ and $l_{2,3} = 2$.

step 1 Fix $i = 1$. Select $8 - 1 = 7$ public shares to recover the codeword C_1. Let the indices of these public shares be $l_{1,4} = 1, l_{2,4} = 2, l_{3,4} = 4, l_{4,4} = 5, l_{5,4} = 6, l_{6,4} = 8, l_{7,4} = 9$.

step 2 Reduce, using the elementary row operations, the generator matrix to another matrix that has the following structure: $(l_{11} + 1)^{th} = 3^{rd}$ column of the generator matrix has 1 in the 1^{st} row and zeros elsewhere. Similarly $(n_1 + l_{14} + 1)^{th} = 4^{th}, (n_1 + l_{24} + 1)^{th} = 5^{th}, (n_1 + l_{34} + 1)^{th} = 7^{th}, (n_1 + l_{44} + 1)^{th} = 8^{th}, (n_1 + l_{54} + 1)^{th} = 9^{th}, (n_1 + l_{64} + 1)^{th} = 11^{th}$, and $(n_1 + l_{74} + 1)^{th} = 12^{th}$ columns of the generator matrix has 1 in the $2^{nd}, 3^{rd}, 4^{th}, 5^{th}, 6^{th}, 7^{th}$ and 8^{th} rows and zeros elsewhere.
After carrying out the specified reduction, we arrive at the following matrix,

$$\begin{bmatrix} 13 & 3 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 17 & 0 & 0 \\ 7 & 14 & 0 & 1 & 0 & 9 & 0 & 0 & 0 & 12 & 0 & 0 \\ 15 & 14 & 0 & 0 & 1 & 8 & 0 & 0 & 0 & 14 & 0 & 0 \\ 17 & 12 & 0 & 0 & 0 & 13 & 1 & 0 & 0 & 8 & 0 & 0 \\ 5 & 12 & 0 & 0 & 0 & 4 & 0 & 1 & 0 & 3 & 0 & 0 \\ 18 & 3 & 0 & 0 & 0 & 5 & 0 & 0 & 1 & 16 & 0 & 0 \\ 11 & 17 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 11 & 1 & 0 \\ 10 & 2 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 15 & 0 & 1 \end{bmatrix}$$

step 3 $l_{11}^{th} = 2^{nd}$ participant in the 1^{st} level computes $v_{1,l_{11}}^1 = v_{1,2}^1 = 2^{17}$ mod $19 = 10$ and sends it as the participant's share in the recovery of the codeword C_1.

step 4 Form the message vector with the participants share and together with the public shares selected in step 1. we have
$(v_{1,2}^1, u_{1,4}, u_{1,5}, u_{1,7}, u_{1,8}, u_{1,9}, u_{1,11}, u_{1,12}) = (10, 2, 4, 15, 14, 10, 0, 17)$.

step 5 Multiplying the reduced generator matrix computed in step 2 by the message vector formed in step 4 we get $(5, 13, 10, 2, 4, 17, 15, 14, 10, 10, 0, 17)$.

First component, which is 5, is the 1^{st} term in the sum of the secret to be recovered. Similarly, fix $i = 2$ and $i = 3$ repeat above steps 1 to 5 then we get 2^{nd} and 3^{rd} term in the sum of the secret to be recovered which are 7 and 15.

step 6 Finally, recover the secret $s = 5 + 7 + 15 = 8$.

3. Complexity analysis and correctness of the proposed scheme

This section analyzes the computational requirements and discusses the correctness of the proposed scheme.

3.1. Complexity Analysis

Computational requirements of the Setup, Distribution, and Reconstruction phases of the proposed scheme are as follows. Assuming that the Vandermonde matrix is chosen as the generator matrix of the code, it can be seen that the reduction of each element requires atmost $2\log n$, where n is the size of the largest exponent, operations. So, reduction of all the elements of the generator matrix requires $2Nn\log n$ operations. Note that the i^{th} codeword to be chosen in Step 4 of the distribution phase contains images of the shares of the participants from the first i levels under i^{th} one way function f_i. Assuming that the one-way function to be used at this step is modulo exponentiation of a field element and the codeword is selected by first reducing the generator matrix so that the reduced matrix contains columns corresponding to the i^{th} component is a partial identity matrix, the computational requirement of step 3 and step 4 (i.e., computing the images of the shares of the participants and choosing all of the codewords) is $2\sum_{i=1}^{m} n_i \log q + 2N^2n - Nn + 2mNn$, where the term $2\sum_{i=1}^{m} n_i \log q$ corresponds to the computation of the images of the shares under one way functions, the term $2N^2n - Nn$ corresponds to the reduction of the generator matrix, and the term $2mNn$ corresponds to the multiplication of the generator matrix by m different N element vectors to arrive at m codewords.

Step 1 of the recovery phase selects the required number of publicized shares and hence requires no computation. Reduction of the generator matrix in step 2 requires $2N^2n - nN$ operations. Since the one-way functions are assumed to be modulo exponentiations, it follows that the computation of the images of the shares of the participants under one-way function in step 3 requires $2j_i \log q \leq 2n_i \log q$ for a fixed i. So, the total computational requirement of step 3 can be seen to be $\sum_{i=1}^{m} 2j_i \log q \leq \sum_{i=1}^{m} 2n_i \log q = 2(N-1)\log q$. Computational requirement of step 5 to arrive at one codeword is $2Nn$ operations. So, formation of all the m codewords is then $2Nnm$ operatons. Hence the computational requirement of the recovery phase is $2N^2n - Nn + 2(N-1)\log q + 2Nnm$ operations. This is either $O(N^3)$ or $O(N \log q)$ depending on the value of the q, which is the field size. If this happens to outweigh the complexity one may choose to opt for other one-way functions so that the complexity remains $O(N^3)$.

3.2. Correctness of the Scheme

Following theorems establish that the proposed scheme is ideal and always recovers the secret in polynomial time if and only if the set of participants is an authorized set. Also the probability that an unauthorized set being able to recover the secret is equal to that of the exhaustive search.

Theorem 3.1. *The secret can be recovered by the recovery phase described above if and only if the set of participants recovering the secret is an authorized set and the hardness assumption stated earlier is fulfilled.*

Proof : (if) It can be seen that the codeword C_i, $1 \leq i \leq m$, can be reconstructed by specifying any of its N components. This is because in an $[n, k, d]$ MDS code any k symbols can be treated as message symbols. So, if $\sum_{k=1}^{i} j_k \geq t_i$, players cooperate they can recover s_i with the help of $N - \sum_{k=1}^{i} j_k$ public shares, for every $i \in \{1, 2, \cdots, m\}$. Hence they can recover the secret $s = s_1 + s_2 + \cdots + s_m$.

(only if) It may be noted that an unauthorized set in the conjunctive case corresponds to a subset S of $\{1, 2, \cdots, m\}$ such that for every $i \in S$, we have $\sum_{k=1}^{i} j_k < t_i$ shareholders only cooperate in the recovery process.

Case 1: $m \in S$. Then $\sum_{k=1}^{m} j_k < t_m$. That is the number of shares specified including the $N - t_m$ public shares corresponding to the codeword C_m is less than N shares. Since any N columns are linearly independent, it follows that the first column of the generator matrix, which corresponds to the partial secret s_m, is not in the span of less than N columns of the generator matrix. Therefore, it is not possible to recover the partial secret s_m and hence not possible to arrive at the secret uniquely with less than N shares specified.

Case 2: $m \notin S$. Let $i, 1 \leq i \leq m$, be such $i \in S$ and $i + 1 \notin S$. Then $\sum_{k=1}^{i} j_k < t_i$ and $\sum_{k=1}^{i+1} j_k \geq t_{i+1}$. Now the values computed in step 3 of

Recovery phase from the shares of the cooperating participants using the one way function together with the $N - t_i$ public shares, we only have $N - t_i + \sum_{k=1}^{i} j_k < N$ components of the codeword C_i. Since any N columns of a generator matrix of the MDS code are linearly independent, it follows that the codeword C_i can not be uniquely determined. But, since $\sum_{k=1}^{i+1} j_k > t_{i+1}$, we can recover the codeword C_{i+1}. Though the common set of components of C_i and C_{i+1} are derived from the same set of shares, they are different because of two different one way functions employed in arriving at the codewords C_i and C_{i+1}. So, from the hardness assumption, recovering the elements of C_i and hence C_i from the corresponding elements of C_{i+1} or for that matter any C_j, $j > i$, is computationally hard.

Therefore, the secret can be recovered only by an authorized set whereas for an unauthorized set this is computationally hard.

Theorem 3.2. *The Proposed scheme is ideal.*

Proof : As can be visualized from the scheme each participant is given exactly one share. Also, the space of secrets and the space of shares is $\mathbb{F}_q$. So, the proposed sheme is ideal.

Theorem 3.3. *The probability that an unauthorized set being able to recover the secret is equal to that of the exhaustive search, which is* $1/q$.

Proof : It may be noted that an unauthorized set in the conjunctive case corresponds to a subset S of $\{1, 2, \cdots, m\}$ such that for every $i \in S$, we have $\sum_{k=1}^{i} j_k = l_i < t_i$ shareholders only cooperate in the recovery process. So, with $N - t_i$ public values the unauthorized set can only know $N - t_i + l_i < N$ components of the codeword C_i, for any $i \in S$. This leaves $t_i - l_i$ degrees of freedom to determine a codeword. So, there are $q^{t_i - l_i}$ codewords that match with the $N - t_i + l_i$ components in their positions. Among these $q^{t_i - l_i - 1}$ codewords contain s_i as their first component. This is beacause in an $[n, k, d]$ MDS code any k symbols can be treated as the message symbols and hence the first component of a corword $C_i, 1 \leq i \leq m$, which corresponds to s_i, is the weighted sum of the N message symbols. From the above discussion this sum consists of $t_i - l_i$ unknowns. So, $t_i - l_i$ degrees of freedom together with a linear constraint become $t_i - l_i - 1$ degrees of freedom. Thus the probability that the partial secret $s_i, i \in S$ can be recovered is $\frac{q^{t_i - l_i - 1}}{q^{t_i - l_i}} = \frac{1}{q}$. So the probability that an unauthorized set being able to recover all the partial secrets $s_i, 1 \leq i \leq m$, and hence the secret is $(\frac{1}{q})^{|S|}$, where $|S|$ denotes the cardinality of S. Since $(\frac{1}{q})^{|S|} \leq \frac{1}{q}$, an unauthorized set may opt for other kind of searches, whose probability of recovering the secret is $\frac{1}{q}$.

4. Conclusions

An ideal secret sharing scheme is proposed for a conjunctive hierarchical access structure. In fact, we have disjunctive secret sharing scheme, which is both ideal and perfect in the classical sense, as well. However, because of the space constraints, we choose to present only the conjunctive scheme.

The Conjunctive scheme, what we call, is computationally perfect and is based on the hardness assumption stated earlier. By computationally perfect, we mean, an authorized set can always reconstruct the secret in polynomial time whereas for an unauthorized set this is computationally hard. This is in contrast to the majority of the schemes found in the literature, which are perfect in the probabilistic manner. A scheme is perfect in a probabilistic manner if either an authorized set may not be able to reconstruct the secret or an unauthorized set may be able to reconstruct the secret with some probability. The proposed schemes overcome all the limitations present in most of the existing schemes. The size of the ground field in our schemes is independent of the parameters of the access structure and there are no restrictions in assigning the identities to the participants. Our schemes are applicable for any number of shareholders. They are efficient and require $O(n^3)$, where n is the number of participants, operations. The schemes are based on MDS codes and the constructions exploit some of the important properties of these codes.

Acknowledgements

V Ch Venkaiah would like to acknowledge the support received by the Department of Science and Technology, Govt. of India, New Delhi. under Project No. SR/s4/MS:516/07 dated 21st April 2008 during his tenure at C R Rao Advanced Institute of Mathematics, Statistics and Computer Science, Hyderabad.

References

[1] Ballico, E., Boato, G., Fontanari, C., Granelli, F., Hierarchical secret sharing in ad hoc networks through birkhoff interpolation. Advances in Comp., Infor., and Syst. Sci., and Engg, 157 - 164, Springer, 2006.

[2] Beimel, A., Tassa, T., Weinreb, E., Characterizing ideal weighted threshold secret sharing. SIAM J. Discrete Math, 22, 600 - 619, 2008.

[3] Belenkiy, M., Disjunctive multi-level secret sharing.document http://eprint.iacr.org/2008/018.

[4] Beutelspacjer, A., Vedder, K., Geometric structures as threshold schemes. in Cryptography and Coding, 255 - 268, Clarendon Press, 1989.

[5] Blakley, G. R., Safeguarding cryptographic keys. In: AFIPS conference proceedings, vol. 48, 313 - 317, 1979.

[6] G. R. Blakley and G. A. Kabatianski., Ideal perfect threshold schemes and MDS codes, in IEEE Conf. Proc., Int. Symp. Information Theory, ISIT95, 1995, p. 488.

[7] Brickell, E. F., Some ideal secret sharing schemes. J. Comb. Math. Comb. Comput., 9, 105 - 113, 1989.

[8] Charnes, C., Martin, K., Pieprzyk, J., Safavi - Naini, R., Sharing secret information in hierarchical groups. Inform. and Commu. Security, LNCS 1334, 81 - 86, Springer, 1997.

[9] Dawson, E., Donovan, D., The breadth of Shamir's secret sharing scheme. Computers and Security, 13, 69 - 78, 1994.

[10] Farras,O., Marte-Farre, J.,Padro,C., Ideal multipartite secret sharing schemes. J. Cryptology, 1 - 30, 2011.

[11] Farras,O., Padro,C., Ideal hierarchical secret sharing schemes. IEEE Trans. Inf. Theory, Jan. 2012.document

[12] Ghodosi, H., Pieprzyk, J., Safavi-Naini, R., Secret sharing in multilevel and compartmented groups. in: Proc. ACISP 1998, LNCS, vol. 1438, 367 - 378, Springer Verlag, 1998

[13] Herranz,J., Saez,G., New results on multipartite access structures. IEEE Proc.Inf.Secur.153, 153-162, 2006.

[14] Karnin, E. D., Greene, J. W., Hellman, M. E., *On secret sharing systems.* IEEE Trans. Inf. Theory, 29, 35 - 41, 1983.

[15] Kasper, E., Nikov, V., Nikova, S., Strongly multiplicative hierarchical threshold secret sharing. In 2nd Intl. Conf. on Inf. Theor. Security, ICITS 2007.

[16] Kothari, S. C., Generalized linear threshold scheme. Advances in Cryptology - CRYPTO 84, LNCS 196, 231 - 241, 1985.

[17] Kaskaloglu, K., Ozbudak, F., On hierarchical threshold access structures. IST panel symposium, Tallinn, Estonia, Nov.document 2010 (www.rto.nato.int/Pubs/rdp.asp?RDP=RTO-MP-IST-091)

[18] Lin, C., Harn, L., Ideal perfect multilevel threshold secret sharing scheme. in Proc. Fifth Intl. Conf. Inf. Assur. and Security, 118-121, 2009.

[19] Massey, J. L., Minimal codewords and secret sharing. in Proc. 6^{th} joint Swedish - Russian Workshop on Inform. Theory, 269 - 279, 1993.

[20] McEliece, R. J., Sarwate, D. V., On sharing secrets and Reed Solomon codes. Comm. of ACM, 24, 583 - 584, 1981.

[21] Ng., S. -L., Ideal secret sharing schemes with multipartite access structures. IEEE. Proc. Commun. 153, 165 - 168, 2006.

[22] Ozadam, H., Ozbudak, F., Saygi, Z., Secret sharing schemes and linear codes. in Proc. Inform. Security and Crypto. conference, Ankara 2007, 101 - 106, 2007.

[23] Shamir, A.,document How to share a secret. Comm. ACM, 22, 612 - 613, 1979.

[24] Simmons, G. J., How to (Really) Share a secret. Advances in Cryptology-CRYPTO'88,LNCS,403(1990),390-448.

[25] Simmons, G. J., An introduction to shared secret and / or shared control schemes and their applications. in Contemporary Cryptology, The Science of Information Integrity, 441 - 497, IEEE Press, 1991.

[26] Tamir Tassa., Hierarchical Threshold Secret Sharing. Journal of Cryptology, 20, pp. 237-264, 2007.

[27] Tamir Tassa and Nira Dyn., Multipartite Secret Sharing by Bivariate Interpolation. Journal of Cryptology, 22, pp. 227-258, 2009.