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. 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 the \((t,n)\)-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 \(U\) be the set of \(n\) participants and let \(2^U\) be its power set. Then the 'Generalized access structure' refers to situations where the collection of permissible subsets of \(U\) may be any collection \(\Gamma \subseteq 2^U\) having the monotonicity property. In multipartite access structures, the set of players \(U\) is partitioned into \(m\) disjoint entities \(U_1, U_2, \ldots, U_m\), called levels and all players in each level play exactly the same role inside the access structure.
Disjunctive hierarchical access structure is a multipartite access structure in which each level $U_i$ is assigned with a threshold $t_i$ for $1 \leq i \leq m$, and the secret can be reconstructed when there are at least $t_i$ shareholders who all belong to levels smaller than or equal to $U_i$. Formally,

$$\Gamma = \{V \subseteq U : |V \cap \bigcup_{j=1}^{i} U_j| \geq t_i, \text{ for some } i \in \{1, 2, \ldots, m\}\}.$$  

Whereas in conjunctive hierarchical access structure we have

$$\Gamma = \{V \subseteq U : |V \cap \bigcup_{j=1}^{i} U_j| \geq t_i, \text{ for all } i \in \{1, 2, \ldots, m\}\}.$$  

A secret sharing scheme is a perfect realization of $\Gamma$ if for all $A \in \Gamma$, the users in $A$ can always reconstruct the secret and for all $B$ not in $\Gamma$, 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 hierarchical schemes that are ideal, efficient, that do not require the ground field to be extremely large, and that offer no restrictions in assigning the identities to the users. One of the proposed scheme is perfect and the other 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 the probabilistic manner. A scheme is perfect in the 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 $[n, t, d]$ block code over $\mathbb{F}_q$ is called MDS if $d = n - t + 1$. Two important properties, namely, any $t$ columns of a generator matrix of the $[n, t, n - t + 1]$ MDS code are linearly independent and any $t$ 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 counterpart. 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] [11] or perfect in a probabilistic manner [17].

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 two secret sharing schemes, one each for disjunctive and conjunctive cases of hierarchical access structure. Both the schemes are ideal. Disjunctive scheme is perfect and the conjunctive scheme, what we call, is computationally perfect.

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 the identities to the participants. Our schemes are applicable for any number of shareholders (participants). They are efficient and require $O(n^3)$, where $n$ is the number of participants, computation for Setup, Distribution, and Recovery phases.

The construction of these schemes is based on the maximum distance separable (MDS) codes.
1.3 Overview of Proposed Schemes

In the proposed disjunctive scheme the dealer selects an \([n, N, n - N + 1]\) MDS code, where \(N = \sum_{i=1}^{m} n_i + 1\), \(m\) is the number of levels, \(n_i, 1 \leq i \leq m\), is the number of participants in the \(i^{th}\) level, \(n = 2*N - t_m, t_i, 1 \leq i \leq m\), is a positive integer such that \(t_i < t_{i+1}, 1 \leq i \leq m - 1\). The dealer chooses \(m\), the number of levels of the scheme, codewords of the above 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 the secret itself, the next \(n_1\) components of the codeword are the shares of the first level participants, next \(n_2\) components are the shares of the second level participants and so on it goes up to the shares of the \(i^{th}\) level. 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 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 of this codeword, which is the desired secret.

The proposed conjunctive scheme is also similar to the disjunctive scheme explained above except in the choice of the components of the chosen codewords. To fix some of the components of each chosen codeword (as previously), the dealer splits the secret \(s\) to be shared as \(s = s_1 + s_2 + \cdots + s_m\) and selects \(m\) distinct one way functions \(f_i, 1 \leq i \leq m\). Now 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 up to 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. As in the case of disjunctive scheme \(N - t_i\) of these arbitrarily chosen components of the \(i^{th}\) codeword are made public.

References


