A Simple Scheme for Hierarchical Threshold Access Structures

Kerem Kaşkaloğlu[1], Ferruh Özbudak[2]

[1]Department of Mathematics, Atilim University, Ankara
keremk@atilim.edu.tr
[2]Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey
ozbudak@metu.edu.tr

Abstract. One of the recent generalizations of (t, n) secret sharing for hierarchical threshold secret access structures is given by Tassa, where he answer the natural question of sharing a secret among three employees at least one of which is a manager. However, the schemes proposed to address this problem, require some significant amount of theoretical background. We give a simpler yet efficient method for hierarchical threshold access structures. Our scheme employs a different approach than previous works, as it involves a certain distribution of polynomials, where members of higher compartments are given a summation of evaluations of higher number of polynomials resulting in a hierarchical effect. The simplicity of our scheme is advantageous both in theory and in practical implementations.

Keywords: secret sharing scheme, multipartite access structures, hierarchical threshold access structures.

1 Introduction

The foundation of secret sharing is assumed to start with Shamir [1] and Blakley [2] who independently introduced t-out-of-n, or simply (t, n) secret sharing schemes (SSS's) that allow a set of at least t participants recover a secret while any t of less number of participants are expected to fail in such an attempt. Simmons [3] introduced t_i-out-of-n_i generalizations of the above scheme, namely hierarchical(multilevel) and compartmented threshold secret sharing. In both of these schemes, the trust is not distributed uniformly among the set of participants. Letting $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{C}_i$ be the set of participants which is partitioned into m disjoint subsets of compartments $\mathcal{C}_i$, $1 \leq i \leq m$, a multipartite access structure $\Gamma \in 2^{\mathcal{U}}$ is one that does not distinguish between members of the same compartment. It is reasonable to assume that access structures are *monotone*, i.e., if $A \in \Gamma$ and $A \subset B \subseteq \mathcal{U}$ then $B \in \Gamma$.

There are three main types of “hierarchy-involved” access structures in literature. Those are, in chronological order, Shamir’s weighted threshold access structures [1], Simmons’ hierarchical access structures [3] which answer the question of solving a secret by either two vice presidents or three bank tellers (where a vice president can always replace a bank teller) and Tassa’s hierarchical threshold access structures [4] raising an answer to the problem of sharing a secret among three employees (again composed of vice presidents and bank tellers) at least two of which are vice presidents. The main difference among the last two structures is that the former is a disjunction of different compartments representing distinct hierarchy levels, whereas the latter is a conjunction of such compartments. We would like to remind that all kinds of hierarchical access structures that admit an ideal secret sharing scheme are completely characterized in [9] by a unified framework. But constructing simple, ideal yet perfect secret sharing schemes for existing types of access structures is still a challenging problem. In this paper, we are only interested in the type access structure given in [4], definition of which is as follows. To obtain a definition Simmons’ version, one can replace the universal quantifier $\forall$ below with the existential quantifier $\exists$.

Definition 1 *Letting $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{C}_i$ be the set of participants with $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$, $1 \leq i < j \leq m$ and let*

$$\Gamma = \{\mathcal{V} \subset \mathcal{U} : |V \cap (\bigcup_{j=1}^{i} \mathcal{U}_j)| \geq k_i \;\; \forall i \in \{1, \ldots, m\}\} \tag{1}$$

Definition 2 *A secret sharing scheme is ideal if the domain of shares of each user equals to the domain of secrets. An access structure Γ is ideal if for some finite domain of shares, there exists an ideal secret sharing scheme realizing it.*

Previous Work. Besides proposing such hierarchical threshold access structures, Tassa gave an ideal SSS for realizing such structures in [4]. To reconstruct the secret, he used Birkhoff interpolation using some derivative values of a polynomial. This approach took attention and found place in recent applications, an example of which is employment in ad hoc networks [10]. Birkhoff interpolation is performed in a setting that the given values of the unknown polynomial, $P(x)$, also include derivative values. Specifically, participants from level $C_i, 1 \leq i \leq m$ receive the value of the $t_{i-1}th$ derivative ($t_0 = 0$) of P at the point that identifies them. Allowing participants from higher levels have shares such as derivatives of P of lower orders, naturally let shares of such participants carry more information on the coefficients of P than shares of participants from lower levels. Later on, Tassa and Dyn [5] proposed another SSS for threshold access structures, which demands calculation of t_m restrictions of a bivariate polynomial to a line each of which is followed by a univariate Lagrange interpolation.

Recently after publication of [5], Yu and Wang [6] proposed a simpler version of Tassa’s scheme for compartmented access structures, which constitutes the first part of the work set forth in [5]. We continue in this manner and give an alternative version of the second part of [5], namely we propose a simpler scheme for hierarchical threshold access structures. We would like to note that all the aforementioned works [4],[5] and [6] together with ours are ideal and linear in the sense of Brickell's [7], which can be described as follows.

Definition 3 *In an ideal linear secret sharing scheme over a finite field $\mathbb{F}$, the domain of secrets is equal to $\mathbb{F}$ (so that the scheme is ideal) and the scheme is specified by $n + 1$ vectors in $\mathbb{F}^d$, $d \in \mathbb{Z}$. The dealer uses a vector $\mathbf{u}_j$ for each participant $u_j \in \mathcal{U}, 1 \leq i \leq n$ and a vector $\mathbf{t}$ which is kept private. To share a secret $S \in \mathbb{F}$ the dealer chooses a random vector $\mathbf{w} \in \mathbb{F}^d$ such that the inner product $\mathbf{w}.\mathbf{t} = S$ and distribute each share $\mathbf{w}.\mathbf{u_i}$ to participant u_i.*

The reconstruction phase of a linear SSS in essence corresponds to solving some linear system. And again all the mentioned schemes and ours are perfect in a probabilistic manner, that is both the reconstruction of the secret by an authorized set of participants and failure of gaining any information about the secret by a nonauthorized set is accomplished with a high probability instead of certainity.

Our Strategy. The only two schemes for hierarchical threshold access structures [4] and [5] apply Birkhoff interpolation and subsequent univariate Lagrange interpolation respectively. In essence, both methods correspond to solving some linear system of equations at the end. Instead of applying any kind of direct interpolation techniques, we present a scheme that leads us again to some linear system of equations. While our scheme is quite different when compared with [4],[5] and [6], all the aforementioned schemes together with ours are linear and hence the proof techniques we employ agree with ones used in [4],[5] and [6]. Letting m be the number of compartments, we give summation of evaluations of m polynomials at some public points to the highest compartment in the hierarchy, summation of evaluations of m-1 polynomials in the second highest level, and continuing this manner, evaluation of only 1 polynomial to the lowest compartment of the hierarchy. They are combined in a manner that participants from the highest levels can always replace the lower-leveled ones whereas the converse does not hold.

Organization of the Paper. After introducing some preliminaries in section 2, we give our ideal scheme for hierarchical threshold access structures in section 3, provide a probabilistic proof of perfectness where an example together with a table of experimental results is included. We conclude with some remarks on section 4.

2 Preliminaries

Shamir's SSS. The basic scheme proposed by Shamir [1] uses standard Lagrange's polynomial interpolation. The scheme works as follows: Let q be a large prime and $S \in \mathbb{Z}_q$ be the secret to be shared. The dealer chooses a random univariate polynomial

$$f(x) = S + \sum_{i=1}^{t-1} a_i x^i \in \mathbb{Z}_q[x]$$

of degree $t-1$ where the constant term is the secret. In order to distribute S among n participants given by $\{u_1, \ldots, u_n\}$ assign to the j-th participant the share $f(u_j) = S + \sum_{i=1}^{t-1} a_i {u_j}^i,\ 1 \leq j \leq n$.

While the reconstruction of the secret can be described by a formula resulting from Lagrange's polynomial interpolation, a linear algebra point of view heads us towards the following linear system that the authorized subset of participants $\{u_{i_1}, \ldots, u_{i_t}\},\ 1 \leq i_1 < i_2 < \ldots < i_t \leq n$ must solve,

$$\begin{pmatrix} 1\ u_{i_1}\ \ldots\ u_{i_1}^{t-1} \\ \vdots \\ 1\ u_{i_t}\ \ldots\ u_{i_t}^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} f(u_{i_1}) \\ \vdots \\ f(u_{i_t}) \end{pmatrix}$$

As pointed out by Shamir himself in [1], a hierarchical variant can be introduced by simply assigning a higher number of shares to higher level participants. However such a solution is far away from being ideal. While Shamir's SSS, having a Vandermonde matrix on its basis, enjoys the property of reconstructibility of the secret with probability exactly 1 by an authorized subset, the schemes given in [4],[5] and [6] and the scheme we propose in the next section claims this property with a probability merely close to 1 depending on the field size and some constants. The following lemma, a proof of which is given in [5], will be helpful in that context.

Lemma 4 *(Schwartz-Zippel Lemma). [5] Let $G(z_1, z_2, ..., z_k)$ be a nonzero polynomial of k variables over a finite field $\mathbb{F}_q$. Assume that the highest degree of each of the variables z_j that G is based on is no larger than d. Then the number of zeros of G in $\mathbb{F}_q^k$ is bounded from above by kdq^{k-1}.*

3 The Scheme

To extract the allowance of maximum number of participants from each compartment while recalling (1), define

$$t_i = k_i - k_{i-1},\ 1 \leq i \leq m \quad (\text{assume } k_0 = 0) \tag{2}$$

Observe that $\sum_{i=1}^{m} t_i = k_m$. Now the following describes a SSS to Realize (1), namely hierarchical threshold access structures.

Secret sharing scheme 1.
1. The dealer generates m random polynomials $P_i(x) = \sum_{j=1}^{t_i} a_{ij} x^j,\ 1 \leq i \leq m$

so that $deg(P_i(x)) = t_i$ and the secret $S = \sum_{i=1}^{m} a_{i1}$.
2. Each participant c_{ij} from compartment $\mathcal{C}_i$ will be identified by a unique public point (x_{ij}, y_{ij}), where $x_{ij} \neq x_{i\ell}$ for $j \neq \ell$ and $y_{ij} \neq y_{ik}$ for $j \neq k$. The private share of the participant c_{ij} will be $Q_i(x_{ij}, y_{ij}) = \sum_{\ell=i}^{m} y_{ij}^{\ell} P_\ell(x_{ij})$.

Our scheme is similar to both the scheme4 given in [5] and the scheme given in [6]. The main difference is that, in the reconstruction phase, we let the rows of participants from higher compartments involve more variables by such a distribution of polynomials. In more detail, the row given to members of compartment $\mathcal{C}_1$ involves a summation of all polynomials $P_i(x)$, hence involving $\sum_{i=1}^{m} t_i$ variables. Similarly, the row given to members of compartment $\mathcal{C}_2$ involves $\sum_{i=2}^{m} t_i$ variables, whereas the polynomial corresponding to the lowest level compartment C_m involves only t_m variables. This decreasing number of variables constitutes the main idea that produces a hierarchical effect. Obviously, the scheme is ideal as the shares of participants are taken from the domain of secrets $\mathbb{F}$. Observe that the problem of recovering the secret in the above scheme is equivalent to solving the whole system, that is, there is no easy shortcut of obtaining only the polynomial coefficients $a_{i1}, i = 1, \ldots, m$ that sum up to the secret S.

Theorem 5. *An authorized set $\mathcal{V} \in \varGamma$ may recover the secret S with probability $1 - Cq^{-1}$, where the constant C depends on t_i, $1 \leq i \leq m$.*

Proof. Let $\mathcal{V} \in \varGamma$ be a minimal set such that $|V| = t_m$ and $|V \cap \mathcal{U}_i| = s_i, \ i \in \{1, \ldots, m\}$. Then the recovery of the polynomials $P_i(x)$ corresponds to the solution of the system of linear equations

$$M\,A = Q \tag{2}$$

where

$$M = \begin{pmatrix} M_{11} & M_{12} & \ldots & M_{1m} \\ 0 & M_{12} & \ldots & M_{1m} \\ \vdots & \vdots & \ddots & \\ 0 & \ldots & 0 & M_{mm} \end{pmatrix}$$

such that

$$M_{ij} = \begin{pmatrix} x_{i1} y_{i1}^{j} & x_{i1}^{2} y_{i1}^{j} & \ldots & x_{i1}^{t_i} y_{i1}^{j} \\ \vdots & & & \vdots \\ x_{is_i} y_{is_i}^{j} & x_{is_i}^{2} y_{is_i}^{j} & \ldots & x_{is_i}^{t_i} y_{is_i}^{j} \end{pmatrix}_{s_i \times t_i},$$

$$\mathrm{A} = (a_{11} \ldots a_{1t_1} a_{21} \ldots a_{2t_2} \ . \ . \ . \ a_{m1} \ldots a_{mt_m})^t \ ,$$

$$Q = (Q_1(x_{11}, y_{11}) \ldots Q_1(x_{1s_1}, y_{1s_1}) \ . \ . \ . \ Q_m(x_{m1}, y_{m1}) \ldots Q_m(x_{ms_m}, y_{ms_m}))^t.$$

Notice that the matrix M is $k_m \times k_m$ where $k_m = \sum_{i=1}^{m} t_i$. Employing basic linear algebra, we know that equation (2) has a unique solution if and only if $det(M) \neq 0$. That is, the probability that an authorized set can reconstruct the secret equals to the probability of $det(M) \neq 0$ where M is their corresponding reconstruction matrix given above. We observe that there are 2 distinct variables in each of the k_m rows. So considering the expansion of M, we see that $det(M)$ is a nonzero polynomial of $2k_m$ variables over the finite field $\mathbb{F}$, where the highest degree of the variables in $det(M)$ can be expressed as $d = max(t_i)$, $1 \leq i \leq m$. Now applying lemma 1, we see that the number of zeros of $det(M)$ in $\mathbb{F}^{2k_m}$ is bounded by $2k_m dq^{2k_m-1}$. Indeed, these are all the choices that make $det(M) = 0$ among all possible q^{2k_m} selections of the $2k_m$ variables. So the probability that $det(M) = 0$ is bounded by $2k_m dq^{2k_m-1}.q^{-2k_m} = 2k_m dq^{-1}$. □

Remark 6 *The reader might have observed the similarity between the the distribution of entries of M with an upper triangular matrix. The reconstruction matrix employed in the proof of theorem4 in [4] also has a triangular structure which seems to be rather in lower triangular-like form. Indeed this triangularity is the main specialty that gives a scheme characteristics of a hierarchical threshold secret sharing.*

Theorem 7. *An non-authorized set $\mathcal{V} \notin \Gamma$ may not learn any information about the secret S with probability $1-Cq^{-1}$, where the constant C depends on $t_1, \ldots, t_m$.*

Proof. If $V \notin \Gamma$ then there exists i with $1 \leq i \leq m$ such that $|V \cap (\bigcup_{j=1}^{i} \mathcal{U}_j)| = \ell_i < k_i$. There are two cases to consider, namely either $1 \leq i < m$ or $i = m$. For the first case, consider the submatrix M' formed by first ℓ_i rows and first $k_i > \ell_i$ columns of M. Observe that all entries below this submatrix are zero. Now add $k_i - \ell_i$ of the zero rows from below to obtain a square submatrix M'' of M. Now $det(M'') = 0$ as it contains one or more zero rows. A partitioning of M gives;

$$M = \begin{pmatrix} M'' & A \\ 0 & B \end{pmatrix}$$

such that M'' and B are square matrices whereas A and the zero matrix in the lower left corner are not. From linear algebra, we know that such a partitioning implies $det(M) = det(M')det(B) = 0$.
For the second case where $i = m$, since $\mathcal{V} \notin \Gamma$, we infer that $|V| < k_m$. Without loss of generality, assume that $|V| = k_m - 1$, which is the best possible situation. Now that M is a $(k_m - 1) \times k_m$ matrix, we will show that, with very high probability, the k_m dimensional vector $\mathbf{e} = (1, 1, \ldots, 1)$ is not spanned by rows of M. To show this, add $\mathbf{e}$ to the first row of M to obtain a square matrix M', and show that with probability $1-Cq^{-1}$, M' has full rank. The rest of the proof follows the same routine with theorem 1. □

The following is a direct result of theorems 4 and 6.

Corollary 8 *The secret sharing scheme1 is a perfect scheme that realizes the access structure (1) with probability $1 - Cq^{-1}$, where the constant C depends on t_i, $1 \leq i \leq m$.*

Example. Let $m = 3$ be the number of compartments where, $k_1 = 2, k_2 = 5, k_3 = 8$ yielding polynomials $P_1(x), P_2(x), P_3(x)$ of degrees respectively $t_1 =$

$2, t_2 = 3, t_3 = 3$. Finally, let $s_1 = 2, s_2 = 4, s_3 = 2$ be the number of participants from compartments $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ respectively. Then M is of the form;

$$M = \begin{pmatrix} x_{11}y_{11} & x_{11}^2y_{11} & x_{11}y_{11}^2 & x_{11}^2y_{11}^2 & x_{11}^3y_{11}^2 & x_{11}y_{11}^3 & x_{11}^2y_{11}^3 & x_{11}^3y_{11}^3 \\ x_{12}y_{12} & x_{12}^2y_{12} & x_{12}y_{12}^2 & x_{12}^2y_{12}^2 & x_{12}^3y_{12}^2 & x_{12}y_{12}^3 & x_{12}^2y_{12}^3 & x_{12}^3y_{12}^3 \\ 0 & 0 & x_{21}y_{21}^2 & x_{21}^2y_{21}^2 & x_{21}^3y_{21}^2 & x_{21}y_{21}^3 & x_{21}^2y_{21}^3 & x_{21}^3y_{21}^3 \\ 0 & 0 & x_{22}y_{22}^2 & x_{22}^2y_{22}^2 & x_{22}^3y_{22}^2 & x_{22}y_{22}^3 & x_{22}^2y_{22}^3 & x_{22}^3y_{22}^3 \\ 0 & 0 & x_{23}y_{23}^2 & x_{23}^2y_{23}^2 & x_{23}^3y_{23}^2 & x_{23}y_{23}^3 & x_{23}^2y_{23}^3 & x_{23}^3y_{23}^3 \\ 0 & 0 & x_{24}y_{24}^2 & x_{24}^2y_{24}^2 & x_{24}^3y_{24}^2 & x_{24}y_{24}^3 & x_{24}^2y_{24}^3 & x_{24}^3y_{24}^3 \\ 0 & 0 & 0 & 0 & 0 & x_{31}y_{31}^3 & x_{31}^2y_{31}^3 & x_{31}^3y_{31}^3 \\ 0 & 0 & 0 & 0 & 0 & x_{32}y_{32}^3 & x_{32}^2y_{32}^3 & x_{32}^3y_{32}^3 \end{pmatrix}_{8\times 8}$$

We leave the fulfillment of polynomials and arbitrary parameters of the scheme to the reader. We provide an extensive table of probabilistic results regarding secret sharing scheme1 with assistance of a computer algebra system [11] where results in each of the entries are obtained by 10^5 experiments with distinct random allocation of x_{ij} and y_{ij} values.

$k_i, t_i,\ 1 \leq i \leq m$	$s_i,\ 1 \leq i \leq m$	q=101	q=100003
$k_1 = 2, k_2 = 5, k_3 = 9$ $(t_1 = 2, t_2 = 3, t_3 = 4)$	$s_1 = 4, s_2 = 4, s_3 = 1$	impl: 0.9876	impl: 0.9999
	$s_1 = 2, s_2 = 3, s_3 = 4$	impl: 0.9039	impl: 0.9998
	$s_1 = 9, s_2 = 0, s_3 = 0$	impl: 0.9867 theo: 0.2872	impl: 0.9999 theo: 0.9993
$k_1 = 1, k_2 = 4, k_3 = 10, k_4 = 23$ $(t_1 = 1, t_2 = 3, t_3 = 6, t_4 = 13)$	$s_1 = 4, s_2 = 2, s_3 = 8, s_4 = 9$	impl: 0.8668	impl: 0.9995
	$s_1 = 1, s_2 = 5, s_3 = 12, s_4 = 5$	impl: 0.8441	impl: 0.9992
	$s_1 = 23, s_2 = 0, s_3 = 0, s_4 = 0$	impl: 0.9650 theo:0.0	impl: 0.9999 theo: 0.9940

Table 1. Table for Success Rates of Reconstructibility of the Secret

Observe that all the experimental results (impl.) in table1 are greater than theretical bounds (theo.) obtained by the complement of the formula given at the end of the proof of theorem4. It can also be seen that, for artificially small values of q, the given bound is loose and sometimes it does not provide any information. Even in this cases, our scheme yields quite acceptable results for small m valuescxc. As $q \to \infty$, the aforementioned probabilities get closer to 1. Indeed, as k_i values increase, higher q values will be needed to keep the probability of the success rate constant. The table, considering some extreme cases, also visualizes the fact that the distribution of s_i values, $1 \leq i \leq m$ affects the experimental probabilistic results.

4 Conclusion

Our contribution. We propose a simple secret sharing scheme for hierarchical threshold access structures and believe that our scheme provides an elegant, practical way of realizing such structures.

Acknowledgments. The authors thank Mehmet Turan and Ali Aydın Selçuk for useful discussions and suggestions that contributed throughout this work.

References

1. A. Shamir, How to Share a Secret, *Comm. ACM*, vol. 22, no. 11, 1979, pp. 612-613.
2. G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of the National Computer Conference*, 1979, American Federation of Information Processing Societies Proceedings 48. 1979, pp. 313-317.
3. G.J. Simmons, How to (really) share a secret, *Advances in Cryptology - CRYPTO 88*, LNCS 403, 1990, pp. 390-448.
4. T.Tassa, Hierarchical Threshold Secret Sharing, *J, Cryptology.* 20, 237-264, 2007. An earlier version appeared in the proceedings of the First Theory of Cryptography Conference 2004, February, (MIT-Cambridge), 2004, pp. 473-490.
5. T.Tassa, Multipartite Secret Sharing by Bivariate Interpolation, *J, Cryptology.* 22, 2009, 227-258.
6. A Probabilistic Secret Sharing Scheme for a Compartmented Access Structure, Y.Yu, M. Wang, *Cryptology ePrint Archive*: Report 2009/301.
7. E.F. Brickell, Some ideal secret sharing schemes, *Journal of Combinatorial Mathematics and Combinatorial Computing*, 9, 1989, pp. 105-113.
8. S.Fehr, Efficient construction of the dual span program. *Manuscript*, May 1999.
9. Ideal Hierarchical Secret Sharing Schemes, Oriol Farras and Carles Padro, *Cryptology ePrint Archive*: Report 2009, 141.
10. Hierarchical Secret Sharing in Ad Hoc Networks through Birkhoff Interpolation, K. Elleithy et al. (eds.), *Advances in Computer, Information, and Systems Sciences, and Engineering*, 2006, pp. 157-164.
11. Bosma W., Cannon J.: *The MAGMA Computational Algebra System for Algebra, Number Theory and Geometry* (version 2.11-14). University of Sydney, School of Mathematics and Statistics, Computational Algebra Group(2002).