A Probabilistic Secret Sharing Scheme for a Compartmented Access Structure

Yuyin Yu and Mingsheng Wang

The State Key Laboratory of Information Security, Institute of Software Chinese
Academy of Sciences, Beijing 100190, China
yuyuyin@163.com;mswang@yahoo.cn

Abstract. In a compartmented access structure, there are disjoint participants $C_1, \dots, C_m$. The access structure consists of subsets of participants containing at least t_i from C_i for $i = 1, \dots, m$, and a total of at least t_0 participants. Tassa [2] asked: whether there exists an efficient ideal secret sharing scheme for such an access structure? Tassa and Dyn [5] presented a solution using the idea of bivariate interpolation and the concept of dual program [9, 10]. For the purpose of practical applications, it is advantageous to have a simple scheme solving the problem. In this paper a simple scheme is given for this problem using the similar idea from [5].

Key words: Secret sharing, Compartmented access structure, Ideality

1 Introduction

Shamir [1] and Blake [7] proposed (t, n) threshold secret sharing scheme, that is, sharing a secret among a given set of n participants, such that every $k (k \leq n)$ of those participants could recover the secret by pooling their shares together, while no subset of less than k participants can do so. Simmons [3] studied a new structure: compartmented access structure. In this structure, there are different compartments, say $C_1, \dots, C_m$, and positive integers $t_1, \dots, t_m$ and t_0, the access structure consists of all subsets containing at least t_i participants from C_i for $1 \leq i \leq m$, and a total of at least t_0 participants. We will restate a formal definition [2] and the related conception [5] here.

Remark 1. Simmons' original notion had $t_0 = \sum_{i=1}^{m}$, Brickell [4] generalized his notion to $t_0 \geq \sum_{i=1}^{m}$, and we use Brickell's definition.

Definition 1 (Ideality). *A secret sharing scheme with domain of secrets $\mathcal{S}$ is ideal if the domain of shares of each user is $\mathcal{S}$. An access structure Γ is ideal if for some finite domain of shares $\mathcal{S}$, there exists an ideal secret sharing scheme realizing it.*

Definition 2 (Compartmented Access Structure). *Let $\mathcal{C}$ be a set of n participants and assume that $\mathcal{C}$ is composed of compartments, i.e., $\mathcal{C} = \bigcup_{i=1}^{m} \mathcal{C}_i$ where*

$\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ for all $1 \leq i < j \leq m$. Let $\mathbf{t} = \{t_i\}_{i=0}^m$ be a sequence of integers such that $t_0 \geq \sum_{i=1}^m t_i$. Then the $(\mathbf{t}, n)$-compartmented access structure is

$$\mathit{\Gamma} = \{\mathcal{V} \subset \mathcal{C} : | \mathcal{V} \cap \mathcal{C}_i | \geq t_i \quad \forall i \in \{1, \ldots, m\} and \mid \mathcal{V} \mid \geq t_0\} \tag{1}$$

Brickell [4] studied this structure later, he proved that this access structure is ideal, but the solution scheme he proposed suffered from the same problem of inefficiency as Simmons' schemes [3] did (namely, the dealer must perform possibly exponentially many checks when assigning identities and shares the participants). So Tassa [2] asked: whether there exists an efficient ideal secret sharing scheme for such access structures? Tassa and Dyn [5] answered this question positively. Their idea result from the following conclusion [9, 10]: If an access structure $\mathit{\Lambda}$ is computed by a monotone span program $\mathcal{M}$, then the dual access structure $\mathit{\Lambda}^*$ is computed by a monotone span program $\mathcal{M}^*$ of the same size, and $\mathcal{M}^*$ can be efficiently computed from $\mathcal{M}$. Tassa and Dyn [5] gave a solution to the dual access structure of (1), so they can efficiently construct a solution for (1). This is a good idea, but hard to understand, and computing $\mathcal{M}^*$ from $\mathcal{M}$ is not an easy work. As a matter of fact, we need not to use the idea of dual span program, just make a little modification of the idea from [5], then we can get an easier solution for the compartmented access structure (1). First let us neglect the restriction of ideality, then there is nothing difficult, we describe a solution to realize the weaken version of the compartmented access structure (1) here :

- The dealer generates a random polynomial $R(y) = \sum_{i=1}^{t_0} a_i y^i$, the dealer generates other random polynomials $P_i(x) = \sum_{j=1}^{t_i} b_{ij} x^j (1 \leq i \leq m)$.
- The secret is $S = a_1 + \sum_{i=1}^m b_{i1}$
- Each participant c_{ij} from compartment $\mathcal{C}_i$ will be identified by a unique public point (x_{ij}, y_{ij}), where $x_{ij} \neq x_{il}$ for $j \neq l$; $y_{ij} \neq y_{kl}$ for $(i, j) \neq (k, l)$. and his private share will be $(P_i(x_{ij}), R(y_{ij}))$.

This idea can be seen as a compound version of shamir's (t,n) threshold, but it is not ideal. In this paper, we try to modify this idea and finally get an ideal scheme, the scheme borrows idea from [5], especially its proof skills, and the scheme is probabilistic, that is, although $\mathcal{V} \in \mathit{\Gamma}$, sometimes the participants in $\mathcal{V}$ cannot recover the secret either, but that is only a small probability event, we will prove this result in the rest of the paper, so the scheme is useful. The paper is organized as follows: in Sect.2, we provide the necessary notation agreements and background, in Sect.3, we will give the revised scheme and prove its validity.

2 Preliminaries

We begin this section by the description of some notation agreements. Let:

- $\mathbb{F}$ is a finite field of size q, and all the operations execute in $\mathbb{F}$.

Next we will introduce a lemma, which provides an upper bound for the number of zeros of a multivariate polynomial over a finite field. and it will play a key role throughout this paper.

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

Proof. The claim is obviously true for $k = 1$. Proceeding by induction, we assume that it holds for $k - 1$ variables and prove the claim for k variables. The polynomial G may be written as follows:

$$G(z_1, z_2, \ldots, z_k) = \sum_{j=0}^{d} G_j(z_1, z_2, \ldots, z_{k-1}) z_k^j \tag{2}$$

For every selection of $(z_1, z_2, \ldots, z_{k-1}) \in \mathbb{F}^{k-1}$, there are two possibilities: Either $G_j(z_1, z_2, \ldots, z_{k-1}) \neq 0$ for at least one $0 \leq j \leq d$, or $G_j(z_1, z_2, \ldots, z_{k-1}) = 0$ for all $0 \leq j \leq d$. In the first case, there are at most d values of z_k for which $G(z_1, z_2, \ldots, z_k) = 0$; in the second case, on the other hand, $G(z_1, z_2, \ldots, z_k) = 0$ for all $z_k \in \mathbb{F}$. By the induction assumption, the number of points $(z_1, z_2, \ldots, z_{k-1})$ $\in \mathbf{F}^{k-1}$ of the second kind, denoted herein ℓ, satisfies $\ell \leq (k-1)dq^{k-2}$. Hence, the number of points $(z_1, z_2, \ldots, z_k) \in \mathbf{F}^k$ at which $G_j(z_1, z_2, \ldots, z_k) = 0$ is bounded by
$(q^{k-1} - \ell) \cdot d + \ell \cdot q = dq^{k-1} + \ell \cdot (q - d) < dq^{k-1} + (k-1)dq^{k-1} = kdq^{k-1}$ □

3 New solution and proofs

In this section we will describe a probabilistic scheme to realize the compartmented access structure Γ and give its proof.

3.1 New solution

1. The dealer generates a random polynomial $R(y) = \sum_{i=1}^{l} a_i y^i$, l^1 =deg($R(y)$) $= t_0 - \sum_{i=1}^{m} t_i$, the dealer generates other m random polynomials $P_i(x) = \sum_{j=1}^{t_i} b_{ij} x^j$, let $Q_i(x, y) = P_i(x) + R(y)$ $(1 \leq i \leq m)$.
2. The secret is $S = a_1 + \sum_{i=1}^{m} b_{i1}$.
3. Each participant c_{ij} from compartment $\mathcal{C}_i$ will be identified by a unique public point (x_{ij}, y_{ij}), where $x_{ij} \neq x_{il}$ for $j \neq l$; $y_{ij} \neq y_{kl}$ for $(i, j) \neq (k, l)$. And his private share will be $Q_i(x_{ij}, y_{ij})$.

The scheme is similar with "Secret Sharing Scheme4" in [5]. The difference is that there are m random polynomials here, but only one in [5]. So we can do more things here. Obviously, this is an ideal scheme since the private shares of

[1] if l=0, then it it a trivial problem, we omit such situation.

all users are taken from the domain of secrets $\mathbb{F}$. The unknown variables are coefficients of all the polynomials $R(y)$ and $P_i(x)\,(1 \leq i \leq m)$, the total number of these variables is t_0. In view of the above, if any participants want to recover the secret $\mathcal{S}$, they must recover every polynomial before-mentioned, so the total number of these participants is at least t_0, and the members from $\mathcal{C}_i$ is at least t_i, in brief, this scheme agrees with the constraints in Γ. Such demonstration may not be convincingly enough, we proceed to give a strict proof.

3.2 Proofs

Theorem 1. *If $\mathcal{V} \in \Gamma$, it may recover the secret $\mathcal{S}$ with probability $1 - Cq^{-1}$, where the constant C depends on $t_0, t_1, \cdots t_m$.*

Proof. Let $\mathcal{V}$ be a minimal set in Γ, then $|\mathcal{V}| = t_0$. We assume that $|\mathcal{V} \cap \mathcal{C}_i| = k_i \geq t_i, 1 \leq i \leq m$. If $\mathcal{V} \cap \mathcal{C}_i = \{c_{i1}, \cdots, c_{ik_i}\}$ and c_{ij} is identified by the point (x_{ij}, y_{ij}), then we can reduce the recover of the polynomials $R(y)$ and $P_i(x)\,(1 \leq i \leq m)$ to the solution of the following linear equations:

$$M \cdot A = Q \tag{3}$$

Where

$$M = \begin{pmatrix} M_1 & & & & G_1 \\ & M_2 & & & G_2 \\ & & \ddots & & \\ & & & M_m & G_m \end{pmatrix} \tag{4}$$

$$A = \begin{pmatrix} b_{11} \cdots b_{1t_1} \cdots b_{m1} \cdots b_{mt_m} \; a_1 \cdots a_l \end{pmatrix}^t \tag{5}$$

$$Q = \begin{pmatrix} Q_1(x_{11}, y_{11}) \cdots Q_1(x_{1k_1}, y_{1k_1}) \cdots Q_m(x_{m1}, y_{m1}) \cdots Q_m(x_{mk_m}, y_{mk_m}) \end{pmatrix}^t$$

The pair of blocks M_i and G_i, $1 \leq i \leq m$, represents the equations that are contributed by the k_i participants from compartment $\mathcal{C}_i$. They have the following form:

$$(M_i \cdots G_i) = \begin{pmatrix} x_{i1} & x_{i1}^2 & \cdots & x_{i1}^{t_i} & \cdots & y_{i1} & y_{i1}^2 & \cdots & y_{i1}^l \\ x_{i2} & x_{i2}^2 & \cdots & x_{i2}^{t_i} & \cdots & y_{i2} & y_{i2}^2 & \cdots & y_{i2}^l \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ x_{ik_i} & x_{ik_i}^2 & \cdots & x_{ik_i}^{t_i} & \cdots & y_{ik_i} & y_{ik_i}^2 & \cdots & y_{ik_i}^l \end{pmatrix} \tag{6}$$

Here, M_i is a block of size $k_i \times t_i$, and G_i is a block of size $k_i \times l$(We omit the trivial situation $l = 0$, so G always exists). Besides M_i and G_i, all the other places of M is 0. M is of size $t_0 \times t_0$. The unknown variables are the components of A. According to the knowledge of linear algebra, the equation (3) has only one solution only when $det(M) \neq 0$, so the probability that we can solve A is equal to the probability that $det(M) \neq 0$. Now we will consider the expansion of $det(M)$. Clearly, it has the following properties:

(1) $det(M)$ is a nonzero polynomial of $2t_0$ variables over the finite field $\mathbb{F}$.

(2) The highest degree of each of the variables in $det(M)$ is no larger than $d = MAX(t_1, \cdots, t_m, l)$.

According to Lemma 1, we may conclude that the number of zeros of $det(M)$ in $\mathbb{F}^{2t_0}$ is bounded by $2t_0 dq^{2t_0-1}$, but in $det(M)$, the $2t_0$ variables can have q^{2t_0} values. So the probability that $det(M) = 0$ is bounded by $2t_0 dq^{2t_0-1} \cdot q^{-2t_0} = 2t_0 dq^{-1}$. □

We give an example here, suppose $m = 3, t_0 = 9, t_1 = 2, t_2 = 2, t_3 = 3, k_1 = 3, k_2 = 2, k_3 = 4$, then

$$M = \begin{pmatrix} x_{11} & x_{11}^2 & 0 & 0 & 0 & 0 & 0 & y_{11} & y_{11}^2 \\ x_{12} & x_{12}^2 & 0 & 0 & 0 & 0 & 0 & y_{12} & y_{12}^2 \\ x_{13} & x_{13}^2 & 0 & 0 & 0 & 0 & 0 & y_{13} & y_{13}^2 \\ 0 & 0 & x_{21} & x_{21}^2 & 0 & 0 & 0 & y_{21} & y_{21}^2 \\ 0 & 0 & x_{22} & x_{22}^2 & 0 & 0 & 0 & y_{22} & y_{22}^2 \\ 0 & 0 & 0 & 0 & x_{31} & x_{31}^2 & x_{31}^3 & y_{31} & y_{31}^2 \\ 0 & 0 & 0 & 0 & x_{32} & x_{32}^2 & x_{32}^3 & y_{32} & y_{32}^2 \\ 0 & 0 & 0 & 0 & x_{33} & x_{33}^2 & x_{33}^3 & y_{33} & y_{33}^2 \\ 0 & 0 & 0 & 0 & x_{34} & x_{34}^2 & x_{34}^3 & y_{31} & y_{34}^2 \end{pmatrix} \tag{7}$$

and $d = MAX(2, 2, 3, 2) = 3$. We just give the form of M here, and it will be helpful to understand this theorem. In the next part of this section, we will use computer to illustrate the validity of the above theorem. We give the result in tables only, without any details. In the following two tables, q is the size of the finite field $\mathbb{F}$, other parameters are as in above. The column of "Times" stands for how many experiments have we make, "Results" stands for the probability of $det(M) = 0$ when we make experiments, "Theoretical" stands for the lower bound probability of $det(M) = 0$ under Theorem 1

Table 1. $q = 4999$

Parameters	Times	Results	Theoretical
$t_1 = 2, t_2 = 3, m = 2$			
$k_1 = 3, k_2 = 6, t_0 = 9$	10000	99.98%	> 98.55%
$t_1 = 1, t_2 = 1, t_3 = 1, m = 3$			
$k_1 = 1, k_2 = 1, k_3 = 2, t_0 = 4$	10000	99.96%	> 99.83%
$t_1 = 2, t_2 = 2, t_3 = 3, m = 3$			
$k_1 = 3, k_2 = 2, k_3 = 4, t_0 = 9$	10000	99.93%	> 98.91%

From the tables above, we can see that if q is large enough, then we can recover the secret with probability very close to 1. That is, when q is larger, the probability will be closer to 1. The results is in accord with the theorem. It provide us with the information that if we want to put the above idea into practice, we must chose a enough large finite field $\mathbb{F}$.

Table 2. $q = 832809541$

Parameters	Times	Results	Theoretical
$t_1 = 2, t_2 = 3, m = 2$ $k_1 = 3, k_2 = 6, t_0 = 9$	10000	100%	$> 1 - 9 \times 10^{-8}$
$t_1 = 1, t_2 = 1, t_3 = 1, m = 3$ $k_1 = 1, k_2 = 1, k_3 = 2, t_0 = 4$	10000	100%	$> 1 - 1 \times 10^{-8}$
$t_1 = 2, t_2 = 2, t_3 = 3, m = 3$ $k_1 = 3, k_2 = 2, k_3 = 4, t_0 = 9$	10000	100%	$> 1 - 7 \times 10^{-8}$

Theorem 2. *If $\mathcal{V} \notin \Gamma$, then with probability $1 - Cq^{-1}$ it may not learn any information about the secret $\mathcal{S}$, where the constant C depends on $t_0, t_1, \cdots, t_m$.*

Proof. Assume that $\mathcal{V} \notin \Gamma$, then we will have two situations to consider: $|\mathcal{V} \cap \mathcal{C}_i| = k_i < t_i$ for some $1 \leq i \leq m$ or $|\mathcal{V}| < t_0$ but $|\mathcal{V} \cap \mathcal{C}_i| > t_i$ for all $1 \leq i \leq m$, in the first case, let k_i chose the maximal value, that is, $k_i = t_i - 1$. If $\mathcal{V} \cap \mathcal{C}_i = \{c_{i1}, c_{i2}, \cdots, c_{i(t_i-1)}\}$ and c_{ij} is identified by the point (x_{ij}, y_{ij}), consider the matrix as follows:

$$M_i^{'} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ x_{i1} & x_{i1}^2 & \cdots & x_{i1}^{t_i} \\ x_{i2} & x_{i2}^2 & \cdots & x_{i2}^{t_i} \\ \vdots & \vdots & \vdots & \vdots \\ x_{i(t_i-1)} & x_{i(t_i-1)}^2 & \cdots & x_{i(t_i-1)}^{t_i} \end{pmatrix} \tag{8}$$

$M_i^{'}$ is a matrix of size $t_i \times t_i$. Solving the value of b_{i1} is equal to say that $det(M^{'}) = 0$, but according to the property of vandermonde determinant, it is easy to conclude that $det(M^{'}) \neq 0$. So we cannot get b_{i1}, nor can we recover the secret $\mathcal{S}$. In the second case, without lose of generality, suppose $|\mathcal{V}| = t_0 - 1$, define a t_0 dimension vector

$$e = \begin{pmatrix} 1 \cdots 0 \cdots 1 \cdots 0\, 1 \cdots 0 \end{pmatrix}^t \tag{9}$$

e can be seen as a vector transformed from A, if we replace b_{i1} $(1 \leq i \leq m)$ and a_1 by 1, replace other components by 0, we will get e. Similiarly as the proof of Theorem 1, we can get a matrix $M^{'}$,the differences are: in (4) the size of M is $t_0 \times t_0$, but here $M^{'}$ is of size $(t_0 - 1) \times t_0$. We need to show that the vector e is, most probably, not spanned by the rows of $M^{'}$. In order to show this, we augment $M^{'}$ by adding to it the vector e as the first row and note the augmented matrix as $M^{''}$, we need to show that the probability of $det(M^{''}) = 0$ is $1 - Cq^{-1}$. The proof goes along the same as in the proof of Theorem 1. □

4 Conclusions

We use the similar idea of [5], give a probabilistic solution for the open problem proposed in [2]. The solution result from Tassa's idea, but easier than his. In practical application, q, the size of the finite field $\mathbb{F}$, is large, so the value of $1 - Cq^{-1}$ is close to 1, which implies the practicability of this scheme. Moreover, ideality is a theoretic notation, in practical application, we need not restrict the scheme to ideality. In such case, the scheme proposed in the introduction of this paper will be a good choice.

References

1. A.shamir, How to share a secret, Commun. ACM22,612-613 (1979)
2. T.Tassa, Hierarchical threshold secret sharing, J.Cryptology. 20,237-264 (2007)
3. G.J.Simmons, How to (really) share a secret, in Advances in Cryptology-CRYPTO 88.LNCS, vol.403(Springer,Berlin,1990, pp.390-448
4. E.F.Brickell, Some ideal secret sharing schemes, J. Comb. Math. Comb. Comput. .9,pp.105-113 (1989)
5. T.Tassa, N.Dyn, Multipartite secret sharing by bivarite interpolation, J.Cryptology. 22,227-258 (2009)
6. S.Runhua, Z.Hong, A hierarchical threshold multi-secret sharing scheme, ASID 2008. 2nd International Conference on, pp.231-234
7. G.R.Blakley, Safeguarding cryptographic keys, The National Computer Conference 1979, AFIPS 48(1979), pp.313-317.
8. J.Herranz, G.Sáez, New results on multipartite access structures. IEE Proc. Inf. Secur.153, 153-162 (2006)
9. S. Fehr, Efficient construction of the dual span program. Manuscript, May 1999
10. M.Karchmer A.Wigderson, On span programs. In 8th Annual Conference on Structure in Complexity Theory(SCTC'93), San Diego, CA, USA, May 1993. IEEE Computer Society Press.