A Probabilistic Secret Sharing Scheme for a Compartmented Access Structure*

Yuyin Yu [1,2] and Mingsheng Wang [1,2]

[1,2] The State Key Laboratory of Information Security, Institute of Software Chinese Academy of Sciences, Beijing 100190, China
[1,2] Graduate University of the Chinese Academy of Sciences, Beijing 100049, China
yuyuyin@163.com, mswang@yahoo.cn

Abstract. In a compartmented access structure, there are disjoint participants $C_1, \ldots, C_m$. The access structure consists of subsets of participants containing at least t_i from C_i for $i = 1, \ldots, m$, 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] realized this access structure with the help of its dual access structure. Unlike the scheme constructed in [5], we propose a direct solution here, in the sense that it does not utilize the dual access structure. So our method is compact and simple.

Keywords: Secret sharing, Compartmented access structure, Ideality.

1 Introduction

Shamir [1] and Blake [6] proposed a (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] generalized this scheme, he described a new scheme: compartmented access structure. In this scheme, there are disjoint participants $C_1, \ldots, C_m$. The access structure consists of subsets of participants containing at least t_i from C_i for $i = 1, \ldots, m$, and a total of at least t_0 participants. We give a formal definition and some related concepts in the following.

Definition 1 (Ideality). *[3,5] 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 secrets $\mathcal{S}$, there exists an ideal secret sharing scheme realizing it.*

Definition 2 (Compartmented Access Structure). *[3,5] Let $\mathcal{C}$ be a set of n participants and assume that $\mathcal{C}$ is composed of compartments, i.e., $\mathcal{C} = \bigcup_{i=1}^{m} \mathcal{C}_i$*

* This work was partially supported by Natural Science Foundation of China under grant (60970134) and Innovation Foundation of Institute of Software under grant (ISCAS2009-QY04).

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 136–142, 2011.

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*

$$\Gamma = \{\mathcal{V} \subset \mathcal{C} : \mid \mathcal{V} \cap \mathcal{C}_i \mid \geq t_i \text{ for all } i \in \{1, \ldots, m\} \text{ and } \mid \mathcal{V} \mid \geq t_0\}. \quad (1)$$

Brickell [4] studied this scheme later, he proved that this access structure is ideal, but the secret sharing scheme that he proposed suffered from the same problem of inefficiency as Simmons's schemes [3] did (namely, the dealer must perform possibly exponentially many checks when assigning identities and shares to the participants). So Tassa [2] asked: whether there exists an efficient ideal secret sharing scheme for such access structures? In [5], Tassa and Dyn gave a positive answer. Their idea results from the following conclusion [8,9]: If an access structure Λ is computed by a monotone span program $\mathcal{M}$, then the dual access structure Λ^* 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 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 still can be improved. As a matter of fact, we do not need to use the idea of dual span program, just make a little amendment 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 access structure (1) here:

- The dealer generates a random polynomial $R(y) = \sum_{i=1}^{t_0} a_i y^i$, and then 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 $j \neq l$ and $y_{ij} \neq y_{kl}$ for $(i, j) \neq (k, l)$. The participant c_{ij}'s private share will be $(P_i(x_{ij}), R(y_{ij}))$.

This idea can be explained 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 solution. The solution uses similar idea as in [5], especially their proof techniques. The drawback of this solution is: although $\mathcal{V} \in \Gamma$, sometimes the participants in $\mathcal{V}$ cannot recover the secret either. To our exciting, it is only a small probability event, so this solution is useful. we will prove this result in the rest of this paper.

In the following context, we use $\mathbb{F}$ to denote the finite field of size q. We discuss problems in $\mathbb{F}$ throughout this paper. In this paper, the following lemma plays an important role:

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}.

2 New Solution and Proofs

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

2.1 New Solution

1. The dealer generates a random polynomial $R(y) = \sum_{i=1}^{l} a_i y^i$, where l[1] $= \deg(R(y)) = t_0 - \sum_{i=1}^{m} t_i$, and then 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 $j \neq l$ and $y_{ij} \neq y_{kl}$ for $(i, j) \neq (k, l)$. The participant c_{ij}'s private share will be $Q_i(x_{ij}, y_{ij})$.

Remark 1. It seems natural to start the indices with 0, but in that case, the scheme will fail all the times, so we do not use the constant terms in the above polynomials. The price is that we must select all the points to be nonzero. we will give a detailed explanation after Example 1.

The scheme is similar as "Secret Sharing Scheme 4" in [5], but we solve different problems here. In [5], Tassa and Dyn gave a solution for the dual access structure of (1) (See "Secret Sharing Scheme 2"). They stated that using the explicit construction described in [8], they can translate the dual access structure into (1). But they did not give the detailed process. We give a direct solution here, which means that we do not utilize the dual access structure. Note 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 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 all the polynomials 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 satisfies the constraints in Γ. Such a demonstration may not be convincing, we proceed to give a strict proof.

2.2 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. When the participants try to recover the secret from their shares, they have to solve the corresponding system of linear equations that is induced by the shares. Let $\mathcal{V}$ be a minimal set in Γ, then $|\mathcal{V}| = t_0$. We assume that $|\mathcal{V} \cap \mathcal{C}_i| = k_i \geq$

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

$t_i, 1 \le i \le m$. 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 $P_i(x)\,(1 \le i \le m)$ to the solution of the following linear equations:

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

where

$$M = \begin{pmatrix} M_1 & & & G_1 \\ & M_2 & & G_2 \\ & & \ddots & \\ & & & M_m \; G_m \end{pmatrix}, \tag{3}$$

$$A = \left(b_{11} \cdots b_{1t_1} \cdots b_{m1} \cdots b_{mt_m} \; a_1 \cdots a_l \right)^t,$$

and

$$Q = \left(Q_1(x_{11}, y_{11}) \cdots Q_1(x_{1k_1}, y_{1k_1}) \cdots Q_m(x_{m1}, y_{m1}) \cdots Q_m(x_{mk_m}, y_{mk_m}) \right)^t.$$

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

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

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. The size of M is $t_0 \times t_0$.

The unknown variables are the components of A. According to the knowledge of linear algebra, the equation (2) 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 $2t_0 d q^{2t_0 - 1}$. But in $\det(M)$, the $2t_0$ variables can have q^{2t_0} values. So the probability that $\det(M) = 0$ is bounded by $2t_0 d q^{2t_0 - 1} \cdot q^{-2t_0} = 2t_0 d q^{-1}$. □

Example 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

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

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 results in tables only, without any more details. In the following two tables, q is the size of the finite field $\mathbb{F}$, other parameters are as in the above. The column "Times" denotes how many experiments have we made, "Results" denotes the probability of $\det(M) = 0$ in the experiments, "Theoretical" denotes 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%	$> 98.91\%$

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%	$> 1 - 7 \times 10^{-8}$

From the tables above, it can be seen 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.

The results imply that if we want to put the above idea into practice, we must chose a large finite field $\mathbb{F}$.

We explain why we choose to start the indices with 0 in our new solution (See Setc. 2.1). For example, if we use constant terms in those polynomials, then the matrix M in Example 1 will be changed into:

$$M = \begin{pmatrix} 1 & x_{11} & 0 & 0 & 0 & 0 & 0 & 1 & y_{11} \\ 1 & x_{12} & 0 & 0 & 0 & 0 & 0 & 1 & y_{12} \\ 1 & x_{13} & 0 & 0 & 0 & 0 & 0 & 1 & y_{13} \\ 0 & 0 & 1 & x_{21} & 0 & 0 & 0 & 1 & y_{21} \\ 0 & 0 & 1 & x_{22} & 0 & 0 & 0 & 1 & y_{22} \\ 0 & 0 & 0 & 0 & 1 & x_{31} & x_{31}^2 & 1 & y_{31} \\ 0 & 0 & 0 & 0 & 1 & x_{32} & x_{32}^2 & 1 & y_{32} \\ 0 & 0 & 0 & 0 & 1 & x_{33} & x_{33}^2 & 1 & y_{33} \\ 0 & 0 & 0 & 0 & 1 & x_{34} & x_{34}^2 & 1 & y_{34} \end{pmatrix}.$$

Note that the first three constant columns span the fourth, so $\det(M) = 0$, according to the proof of Theorem 1, we cannot recover the secret in this case, the scheme will fail under such condition. As a matter of fact, $\det(M) \equiv 0$ if we start the indices with 0, these situation should be avoided in our scheme, so we start the indices with 1.

In [5], Tassa and Dyn chose to start the indices with 0, but in practice, their scheme cannot handle the case when there needs only one partiticipant in some compartment $\mathcal{C}_i$, that is, when $\min(t_1, \cdots, t_m) = 1$, their scheme will fail. Moreover, according to our experiments, the probability that $\det(M) \neq 0$ will become a little higher when we start the indices with 1, so it is a better choice.

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 $\mathcal{V} \notin \Gamma$, we choose $\mathcal{V}$ to be a maximal unauthorized subset, namely, a subset that lacks only one participant to becoming an authorized subset, then there are only two situations to be considered: $|\mathcal{V} \cap \mathcal{C}_i| = k_i < t_i$ for some $1 \leq i \leq m$ or $|\mathcal{V}| < t_0$ but $|\mathcal{V} \cap \mathcal{C}_i| \geq t_i$ for all $1 \leq i \leq m$. In the first case, let $k_i = t_i - 1$ for some i. 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:

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

$M_i^{'}$ is a matrix of size $t_i \times t_i$. If we can recover the value of b_{i1}, then the first row must be spanned by the rest, which implies 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

$$e = \left(1 \cdots 0 \cdots 1 \cdots 0\, 1 \cdots 0\right)^t.$$

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. Similar as the proof of Theorem 1, we can get a matrix $M^{'}$, the differences are: in equation (3) the size of M is $t_0 \times t_0$, but here the size of $M^{'}$ is $(t_0 - 1) \times t_0$. 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. □

3 Conclusions

We give a probabilistic solution of the open problem proposed in [2], using the similar idea as in [5]. 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 be ideal. In such case, the scheme proposed in the introduction of this paper will be a good choice.

References

1. Shamir, A.: How to share a secret. Commun. ACM 22, 612–613 (1979)
2. Tassa, T.: Hierarchical threshold secret sharing. J. Cryptology 20, 237–264 (2007)
3. Simmons, G.J.: How to (Really) Share a Secret. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 390–448. Springer, Heidelberg (1990)
4. Brickell, E.F.: Some ideal secret sharing schemes. Journal of Combinatorial Mathematics and Combinatorial Computing 6, 105–113 (1989)
5. Tassa, T., Dyn, N.: Multipartite secret sharing by bivarite interpolation. J. Cryptology 22, 227–258 (2009)
6. Blakley, G.R.: Safeguarding cryptographic keys. In: Proc. AFIPS 1979 NCC, Arlington, Va, vol. 48, pp. 313–317 (June 1979)
7. Herranz, J., Sáez, G.: New results on multipartite access structures. IEE Proc. Inf. Secur. 153, 153–162 (2006)
8. Fehr, S.: Efficient construction of the dual span program (May 1999) (manuscript)
9. Karchmer, M., Wigderson, A.: On Span Programs. In: The Eighth Annual Structure in Complexity Theory, pp. 102–111 (1993)