Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080349

A Secret Sharing Scheme to Recover Secret Unnecessary Calculating

Yanbo Wang[*], *Wanlin Li, Min He, Jian Yang and Liang Chen*

Institute of Communications Engineering PLA University of Science and Technology, Nanjing, 210007, China

Received: 20 Jun. 2013, Revised: 25 Oct. 2013, Accepted: 26 Oct. 2013
Published online: 1 May. 2014

Abstract: In general, traditional secret sharing threshold schemes require substantial computation when recover the secret. This paper represents a secret sharing threshold scheme based on direct partitioning and combining of set which avoids any computation. This scheme shares the same authority, but different secret shadows, thus extends to general access structures. (w,t) threshold scheme is used to confirm as a special case.

Keywords: Secret sharing, threshold scheme, secret recovery, access structure

1 Introduction

In 1979, A.Shamir[1] and G.R.Blakley[2] represented a secret sharing scheme that divides a secret into many sub-secrets and dispenses them to the participants. The union of certain amounts of participants recovers the secret. If the number of the participants is w, the minimum number of the participants needed to recover the secret is $t(1 < t \leq w)$, then we call the scheme as (w,t) threshold secret sharing scheme.

As Shamir's (w,t) threshold secret sharing scheme is based on polynomial method, Blakley represented a similar scheme using the system of linear equations. These schemes have a common shortcoming that substantial computation required in secret recovery is quite time-consuming when with big w and t, being extremely not suitable for equipments lack of storage and computing resources[3][4]. This paper is going to represent a secret sharing scheme based on the idea of set division-merger be called the set method or set scheme, which means, mapping the secret information as a set, assign each participant one subset, so that the recovery of the secret can be realized by combining the subsets, thus computing discarded.

2 Threshold secret sharing set scheme

Assume that the number of the participants is w, now we can construct a (w,t) threshold secret sharing scheme based on direct partitioning and recombining of set.

Set the w participants as $A_1,A_2,\ldots,A_w$. The (w,t) threshold scheme claims that t or more than t participants is the minimum requirement to secret recovery, less than t participants will lead to recovery failure.

First mapping the secret information as a set, the number of the elements in the set could be determined by secure needing. Next, assign each participant one subset according to certain scheme. When t or more than t participants decide to recovery the secret, contribution of own subsets would gather all the elements required. Less than t participants mean element absence. i.e. the union of $t-1$ participants' subsets lacks one element at least.

There are $s = C_w^{t-1}$ possible combinations of the $t-1$ participants. Assume that the s possible combinations are $B_1,B_2,\ldots,B_s$, meanwhile, without loss of generality, assume that $A_1,A_2,\ldots,A_w$ represent corresponding subsets of the participants. $B_1,B_2,\ldots,B_s$ also represent the union set of all the subsets, brief write down for

$$B_1 = A_1A_2\ldots A_{t-1},$$

$$B_2 = A_1A_3\ldots A_t,$$

$$\ldots\ldots\ldots,$$

$$B_s = A_{w-t+1}A_{w-t+2}\ldots A_w.$$

[*] Corresponding author e-mail: foliation@yeah.net

For convenient, we might as well call it maximum forbidden access team.

Assume that teams $B_1, B_2, \ldots, B_s$ lack $d_1, d_2, \ldots, d_s$ elements separately, $d_1, d_2, \ldots, d_s$ are chosen random positive integers. For more convenient calculation, set the $d_1, d_2, \ldots, d_s$ elements are different, in that way, the minimum secret set is the union of the $d_1, d_2, \ldots, d_s$ elements, the number of the elements is $d = d_1 + d_2 + \ldots + d_s$.

Accordinglythe secret set K is a set of d elements, $K = \{a_1, a_2, \ldots, a_d\}$. So, when executing the scheme, mapping the secret information as a set of d elements at the first place, if the secret is itself a set, but the number of the elements is not d, then certain methods should be taken to expense or compression till the number of the elements is exactly d.

Divide K randomly into subsets of $d_1, d_2, \ldots, d_s$ elements:

$$D_1 = D(1, 2, \ldots, t-1),$$

$$D_2 = D(1, 3, 4, \ldots, t),$$

$$\ldots\ldots\ldots,$$

$$D_s = D(w-t+1, w-t+2, \ldots w);$$

i.e. $K = D_1 \bigcup D_2 \bigcup \ldots \bigcup D_s, D_i \bigcap D_j = \varnothing, i \neq j$, $i, j = 1, 2, \ldots, s$.
So,

$$B_1 = K \backslash D_1,$$

$$B_2 = K \backslash D_2,$$

$$\ldots\ldots\ldots,$$

$$B_s = K \backslash D_s.$$

Apparently,

$$\begin{aligned} A_1 &= A_1A_2\ldots A_{t-1} \bigcap A_1A_3\ldots A_t \bigcap \ldots \bigcap A_1A_{w-t+2}\ldots A_w \\ &= \bigcap_{1=i_1<i_2<\ldots<i_{t-1}\leq w} A_1A_{i_2}\ldots A_{i_{t-1}} \\ &= \bigcap_{1=i_1<i_2<\ldots<i_{t-1}\leq w} K \backslash D(1, i_1, i_2, \ldots, i_{t-1}) \\ &= K - \bigcup_{1=i_1<i_2<\ldots<i_{t-1}\leq w} D(1, i_1, i_2, \ldots, i_{t-1}) \end{aligned}$$

Likewise:

$$A_2 = K - \bigcup_{1\leq i_2<\ldots<i_{t-1}\leq w, i_1=2, i_2i_3\ldots i_{t-1}\neq 2} D(2, i_2, \ldots, i_{t-1})$$

$$A_3 = K - \bigcup_{1\leq i_2<\ldots<i_{t-1}\leq w, i_1=3, i_2i_3\ldots i_{t-1}\neq 3} D(3, i_2, \ldots, i_{t-1})$$

$$\ldots\ldots\ldots$$

$$A_w = K - \bigcup_{1\leq i_2<\ldots<i_{t-1}\leq w, i_1=w, i_2i_3\ldots i_{t-1}\neq w} D(w, i_2, \ldots, i_{t-1}).$$

Thus, we get a (w,t) threshold secret sharing scheme denoting $(A_1, A_2, \ldots, A_w; t; \{K, d\}, \{D_1, d_1\}, \ldots, \{D_s, d_s\})$ based on direct partitioning and recombining of set.

Take the following as an example of a $(5,4)$ threshold secret sharing scheme.

For the $(5,4)$ threshold $s = C_5^3 = 10$, as a matter of convenience, assume that $d_1 = d_2 = \ldots = d_{10} = 1$, then the number d of the elements of set $K, d = 10$, the secret set could be set as $K = \{a_1, a_2, \ldots, a_{10}\}$.

All teams are

$$A_1A_2A_3, A_1A_2A_4, A_1A_2A_5, A_1A_3A_4, A_1A_3A_5,$$

$$A_1A_4A_5, A_2A_3A_4, A_2A_3A_5, A_2A_4A_5, A_3A_4A_5.$$

Let each team lack one elements, might as well set. Set

$$A_1A_2A_3 = K \setminus \{a_1\},$$

$$A_1A_2A_4 = K \setminus \{a_2\},$$

$$A_1A_2A_5 = K \setminus \{a_3\},$$

$$A_1A_3A_4 = K \setminus \{a_4\},$$

$$A_1A_3A_5 = K \setminus \{a_5\},$$

$$A_1A_4A_5 = K \setminus \{a_6\},$$

$$A_2A_3A_4 = K \setminus \{a_7\},$$

$$A_2A_3A_5 = K \setminus \{a_8\},$$

$$A_2A_4A_5 = K \setminus \{a_9\},$$

$$A_3A_4A_5 = K \setminus \{a_{10}\}.$$

Then

$$\begin{aligned} A_1 &= \bigcap_{i,j\neq 1} A_1A_iA_j = K \setminus \{a_1, a_2, a_3, a_4, a_5, a_6\} \\ &= \{a_7, a_8, a_9, a_{10}\}, \\ A_2 &= \bigcap_{i,j\neq 2} A_2A_iA_j = K \setminus \{a_1, a_2, a_3, a_7, a_8, a_9\} \\ &= \{a_4, a_5, a_6, a_{10}\}, \\ A_3 &= \bigcap_{i,j\neq 3} A_3A_iA_j = K \setminus \{a_1, a_4, a_5, a_7, a_8, a_{10}\} \\ &= a_2, a_3, a_6, a_9, \\ A_4 &= \bigcap_{i,j\neq 4} A_4A_iA_j = K \setminus \{a_2, a_4, a_6, a_7, a_9, a_{10}\} \\ &= a_1, a_3, a_5, a_8, \\ A_5 &= \bigcap_{i,j\neq 5} A_5A_iA_j = K \setminus \{a_3, a_5, a_6, a_8, a_9, a_{10}\} \\ &= \{a_1, a_2, a_4, a_7\}. \end{aligned}$$

So there are

$$\begin{aligned} &(A_1, A_2, A_3, A_4, A_5) \\ &\quad = (\{a_7, a_8, a_9, a_{10}\}, \{a_4, a_5, a_6, a_{10}\}, \\ &\quad \{a_2, a_3, a_6, a_9\}, \{a_1, a_3, a_5, a_8\}, \{a_1, a_2, a_4, a_7\}). \end{aligned}$$

Dispense the elements of the subsets to the corresponding participants, we will get a $(5,4)$ threshold secret sharing scheme. Contribution of own secret subsets would realize the secret recovery.

Express the $(5,4)$ threshold secret sharing scheme based on direct partitioning and recombining of set as:

$$(A_1, A_2, A_3, A_4, A_5; 4; K, 10, D_1, 1, \ldots, D_{10}, 1).$$

3 Threshold schemes of same authority but different responsibility

If we set $d_1 = d_2 = \ldots = d_s$, then the secret shadows we dispense to the participants would be the same by the above method. If $d_1 = d_2 = \ldots = d_s$ are false, participants share different secret shadows, but how many the secret shadows would be cannot be confirmed beforehand.

The core of the set method is to dispense the elements of the set reasonably to the participants so that the distribution would match threshold requirements. The design idea is to solve the distributed elements reversely by setting lacking elements that impede the secret recovery. On the other way round, how can we match the threshold scheme by assigning specified shares to the participants?

It seems unreasonable that participants with different shares take different responsibility while they hold the same authority if assigned with specified shares. Still, there is no lack of suiting cases. For example, it can be applied by some of the secret managers who only want to keep very little secret in order to reduce routine maintenance workload, but same authority.

The key to implement this scheme is to work out the number of lacking elements in the maximum forbidden access teams $B_1, B_2, , B_s$. Solve the equation:

$$A_1 = K - \bigcup_{1=i_1<i_2<\ldots<i_{t-1}\leq w} D(1, i_2, i_3, \ldots, i_{t-1}).$$

Because

$$d = \sum_{1\leq i_1<i_2<\ldots<i_{t-1}\leq w} \#D(i_1, i_2, i_3, \ldots, i_{t-1}).$$

so

$$\begin{aligned}\#A_1 = & \sum_{1\leq i_1<i_2<\ldots<i_{t-1}\leq w} \#D(i_1, i_2, i_3, \ldots, i_{t-1}) \\ & - \sum_{1=i_1<i_2<\ldots<i_{t-1}\leq w} \#D(1, i_2, i_3, \ldots, i_{t-1}) \\ & = \sum_{1\leq i_1<i_2<\ldots<i_{t-1}\leq w, i_1, i_2, \ldots, i_w \neq 1} \#D(i_1, i_2, i_3, \ldots, i_{t-1})\end{aligned}$$

Likewise

$$\#A_2 = \sum_{1\leq i_1<i_2<\ldots<i_{t-1}\leq w, i_1, i_2, \ldots, i_w \neq 2} \#D(i_1, i_2, i_3, \ldots, i_{t-1})$$

$$\cdots\cdots\cdots$$

$$\#A_w = \sum_{1\leq i_1<i_2<\ldots<i_{t-1}\leq w, i_1, i_2, \ldots, i_w \neq w} \#D(i_1, i_2, i_3, \ldots, i_{t-1})$$

Now we can set the value of $\#A_1, \#A_2, \ldots, \#A_w$ due to the share requirement. Solve the system equations

$$\begin{cases} \sum_{1\leq i_1<i_2<\ldots<i_{t-1}\leq w, i_1, i_2, \ldots, i_w \neq 1} \#D(i_1, i_2, i_3, \ldots, i_{t-1}) = \#A_1; \\ \sum_{1\leq i_1<i_2<\ldots<i_{t-1}\leq w, i_1, i_2, \ldots, i_w \neq 2} \#D(i_1, i_2, i_3, \ldots, i_{t-1}) = \#A_2; \\ \cdots\cdots\cdots \\ \sum_{1\leq i_1<i_2<\ldots<i_{t-1}\leq w, i_1, i_2, \ldots, i_w \neq w} \#D(i_1, i_2, i_3, \ldots, i_{t-1}) = \#A_w; \end{cases}$$

There are $s = C_w^{t-1}$ variables and contains w equations, the sufficient and necessary condition of the solution existence is $s \geq w$.
But

$$\begin{aligned} s = C_w^{t-1} = & \frac{w!}{(t-1)!(w-(t-1))!} \\ = & \frac{w(w-1)\cdots(w-(t-1))}{(t-1)!} \\ \geq & w \\ \Longleftrightarrow & (w-1)\cdots(w-t-2) \geq (t-1)! \\ \Longleftarrow & w \geq t. \end{aligned}$$

So, the solution exists.

According to the threshold requirement, all variables in solutions of the equations should be nonzero, i.e.

$$\#D(i_1, i_2, \ldots, i_{t-1}) > 0, 1 \leq i_1 < i_2 < \ldots < i_{t-1} \leq w.$$

It is hard to get the sufficient and necessary condition of working out the solutions with all variables nonzero in general cases. Further study is needed.

4 Threshold schemes with different authority and access structure

Threshold scheme [5] with different authority is an extension to simple threshold schemes. Participants could have different authority and share different secret shadows in this threshold scheme. Shamir's scheme uses a simple threshold scheme to realize the threshold scheme with authority, they quantify the authority with number of participants: choose the participant who holds the least authority as base, sharing only one secret shadow; bigger authority, more secret shadows.

Here if set $\#A_1 = \#A_2 = \ldots = \#A_w$, when every participant shares same number of elements, which leads to same authority. Take this as basic threshold scheme; we can as well realize threshold scheme with different authority by the set method just like Shamir and others did.

Access structure [6] is generalization to the threshold scheme.

Set (M, Γ) as an access structure, M is the collection of all participants, $M = \{A_1, A_2, \ldots, A_w\}$, Γ is the collection of minimum qualified access subsets, the sets in Γ should not contain each other. Now we are going to use the set method to assign the secret elements so that all the members in the minimum qualified access subsets could recover the secret set, any members subset that contain the minimum qualified access subsets as well, other members subsets not.

Assume that $\Gamma = \{C_1, C_2, \ldots, C_k\}$, if $H \subset M, H \cap C_i \neq C_i, i = 1, 2, \ldots, k$, then members in H cannot recover the secret set, as we called forbidden access subset. Set the entire maximum forbidden access subsets in all the forbidden access subsets as

$\Omega, \Omega = \{B_j, j = 1,2,\ldots,h\}$, i.e. any forbidden access subset must be one subset of B_j, B_j shouldn't contain each other.

Just like simple threshold sharing scheme, we might as well construct the access structure using the set method, as follows.

The union of the secret shadows of all participants from the maximum forbidden access subset B_j must not equal to the secret set K, d_j elements missing at least, $d_j > 0, j = 1,2,\ldots,h.$

We set

$$K = \bigcup_{j=1}^{h} D_j . d = d_1 + d_2 + \ldots + d_h.$$

Assume that

$$\bigcup_{A_i \in B_j} A_i = K \backslash D_i, \# D_j = d_j,$$

and D_j don't contain each other, $j = 1,2,\ldots,h.$

Then

$$A_i = \bigcap_{A_i \in B_j} B_j = \bigcap_{A_i \in B_j} K \backslash D_j = K \backslash \bigcup_{A_i \in B_j} D_j,$$

$$\# A_i = d - \sum_{A_i \in B_j} d_j, j = 1,2,\ldots,h.$$

Thus, we get a set scheme for the access structure $(M, \Gamma, A_1, A_2, \ldots, A_w)$.

As a special case, the collection of maximum forbidden access subsets from the (w,t) threshold scheme is the collection of all combinations of the possible $t-1$ participants. So it's noticeable that above is just the same as how we construct the threshold scheme.

5 Conclusions

Secret sharing is the key technology of key management and identity authentication. This paper represents a method using set to construct the secret sharing scheme that could avoid computing when recovering the secret, so it can be applied to equipments lack of storage and computing resources. The Distribution, recovery and security of the secret in the method are straightforward. The method can be applied to non-professionals as a method to anti-counterfeit and verify mass market products.

Acknowledgement

The authors gratefully acknowledge the support of the National Natural Science Foundation of China under Grant No. 61072042.

References

[1] A. Shamir, How to Share a secret, Comm. ACM, **22**, 612-613 (1979).

[2] G. R. Blakley, Safeguarding cryptographic keys. Proc. National Computer Conference'79, AFIPS Proceedings, **48**, 313- 317 (1979).

[3] R. M.Capocelli, A. De Santis,L.Gargano and U.Vaccaro, On the Size of Secret Sharing Schemes, J.Cryptology, **6**, 157-169 (1993).

[4] J. C.Benaloh and J. Leichter, Generalized Secret Sharing and Monotone Functions, Advances in Cryptology-CRYPTO'88, S. Goldwasser, Ed., Lecture Notes in Computer Science, Springer Verlag, Berlin, **403**, 27-35 (1990).

[5] Desmedt Y, Frakel Y. Threshold Cryptosystems, In G. Brassard, editor, Advances in Cryptology, Proc. Of Crypto'89, LNCS, Berlin: Springer-Verlag, **435**, 307-315 (1990).

[6] M Ito, A Saito, T Nishizcki. Secret Sharing Scheme Realizing General Access Structure, Proc. of IEEE Global Telecommunication Conf. Globecom, **87**, 99-102 (1987).

Yanbo Wang received the MS degree in the Department of Mathematics from Northeast Normal University in 1983. He is currently a professor in PLA University of Science and Technology. His research interests are in the areas of cryptography and information security.