Two-Level Threshold Secret Sharing Scheme and Monotone Functions

Jen-Chun Chang* Hsin-Lung Wu* Wah-Song Yeap†

Abstract

The threshold secret sharing scheme(SSS) has been studied widely in the last few years. The traditional threshold SSS such as Shamir's can only handle some simple monotone access structures. But there are some cases of monotone access structures are unable to be realized by traditional (one-level) threshold SSS. However those results are under the assumption of applying the traditional threshold SSS or one-level threshold SSS to monotone access structure.

In this paper, we apply the two-level threshold SSS to monotone access structure. The main purpose of using two-level threshold secret scheme is trying to divide a secret through two levels. In the first level, it only concerns on generating the shares based on the number of user groups. In the second level, it subdivides the secret share from the first level to each user inside the group. We consider the disjoint case where a user can be randomly assigned into a group only. In this paper, we prove that some monotone access structure cannot be realized by two-level threshold SSS.

1 Introduction

The computer networks and data communication systems play important roles in our life. Various types of data are transferred or accessed through the networks everyday. Therefore information security becomes an important issue. The threshold SSS is a powerful tool that is used to keep a data secret unless the number of cooperated shares reaches the threshold.

The concepts of Shamir (t, n) threshold SSS is introduced by Adi Shamir[Sha79]. It used a $t-1$ degree polynomial function to generate the shares and distributes among the users. The secret can only be reconstructed by a group of qualified users where the number of users is greater or equal to t. In the past few years, many people tried to apply the Shamir threshold SSS to the digital signature. The traditional digital signature is based on a public key cryptosystem that only involves one signer and one verifier. By applying the threshold concepts, the digital signature will be valid only when the number of qualified signers is at least t where t is the threshold. The paper [Har94] applied the Shamir threshold SSS to modified Elgamal digital signature.

Another way of threshold secret sharing is based on the Chinese Remainder Theorem, and the shares are the remainders through a set of prime modulo. The Asmuth-Bloom SSS is an example of applying Chinese Remainder Theorem to threshold secret sharing. The Chinese Remainder

*Department of Computer Science and Information Engineering, National Taipei University, Taipei Country 237, Taiwan. E-mail: {jcchang, hsinlung@mail.ntpu.edu.tw}. This work was supported in part by the National Science Council of Taiwan under contract NSC-97-2218-E-305-001-MY2.

†Graduate Institute of Communication Engineering, National Taipei University, Taipei County 237, Taiwan. E-mail: song.raymond@gmail.com.

Theorem has been applied into SSS in the papers [KST06],[Ift06],[IG07]. Some papers tried to implement different access structures in threshold SSS. The weighted access structure in [IG07] assumes there are different weights assigned to each user. The secret can only be reconstructed by a set of qualified users where the total weight of the users is greater than or equal to the threshold.

In the paper [Ift06], the compartmented access structure was studied where the users are assigned to different groups and share the secret in two levels, the first level is global level and the second, compartment level. The secret has been separated into a global share and a set of comparment shares. There have two shares for each user which are the global secret shares and the compartment shares. The secret can only be reconstructed when the number of qualified users greater than or equal to the threshold of the global level and also the compartment level. Here the secret sharing appeared twice and we can call it as two-level SSS for applying the compartmented access structure which considers a more complicated access structure.

Josh Benaloh and Jerry Leichter[BL88] proposed a general method for constructing SSS for any given secret sharing function. But they also proved that there exist monotone access structures for which there is no threshold scheme by giving a counterexample.

This paper makes a further study on two-level threshold SSS for the monotone access structure. The concept of two-level threshold secret sharing scheme is to try to divide a secret value s among two levels. Let m denote the total number of groups and n denote the total number of users and each user is assigned into a group only (disjoint case). In the first level, a (t, m) threshold SSS is used to transform the secret s into a set of shares $\{s_1, s_2, \ldots, s_m\}$ and distribute the shares among the m groups. In the second level, each group i performs a (t_i, n_i) threshold SSS to subdivide the group secret s_i into a set of shares $\{s_{i,1}, s_{i,2}, \ldots, s_{i,n_i}\}$ and distribute the share to each user inside the group.

2 Preliminaries

First, we need to define the access structure.

Definition 1. *Given a set of users $P = \{u_1, u_2, \ldots, u_n\}$, a monotone access structure on P is a family of subsets $\Gamma \subseteq 2^P$ such that*

$$A \in \Gamma, A \subseteq A' \subseteq P \longrightarrow A' \in \Gamma$$

Definition 2. *Let S be a set of possible secret values, a (t, n)-threshold scheme on S is a method of dividing each $s \in S$ into a set of shares $\{s_1, s_2, \ldots, s_n\}$ such that*

i. The secret value s can be reconstructed by any set of s_i whose size is t or more.

ii. The secret value s is completely undetermined in an information theoretic sense for any set of s_i whose size is less than t.

There are some useful (t, n)-threshold scheme available such as Shamir SSS. Shamir SSS is a polynomial-based threshold scheme which generates shares by using a polynomial function which consists of $t-1$ degree. The Lagrange Interpolation is applied by Shamir SSS to reconstruct the secret. Another way of SSS generates shares through a set of prime modulo and recovers the secret by Chinese Remainder Theorem.

For a general (t, n)-threshold scheme, previous published schemes only consider the users as a group and try to divide the secret s among the n users. But it has some limitations while applied to the monotone access structure and it is proved to be insufficient by Benaloh.

Definition 3. *Let S be a set of possible secret values, a two-level threshold scheme is a method of dividing each $s \in S$ through two levels such that*

i. In the first level, a (t, m) threshold scheme is used to divide a secret value $s \in S$ into a set of shares $\{s_1, s_2, \ldots, s_m\}$, where m denotes the number of groups of users.

ii. In the second level, each group i applies a (t_i, n_i) threshold scheme to subdivide the sub-secret value s_i, where t_i is a threshold value for group i and n_i is the total number of users assigned to the group.

3 Monotone Functions which cannot be implemented by two-level threshold scheme

Let's consider the function

$$f(A, B, C, D, E) \doteq (A \wedge B) \vee (B \wedge C) \vee (C \wedge D) \vee (D \wedge E) \vee (E \wedge A).$$

The function f defines a monotone function on variables labeled by a set of users $P = \{A, B, C, D, E\}$. The access structure defined by f is the set of subsets T of P for which f is true precisely when the variables labeled by T are set to true.

Theorem 1. *The access structure f cannot be realized by a two-level threshold secret sharing scheme.*

Proof. Assume that there is a threshold SSS which can divide a secret value s among A, B, C, D, and E such that only those subset of $\{A, B, C, D, E\}$ which fulfill the function f can reconstruct the secret.

Let w_a, w_b, w_c, w_d, and w_e denote the weight or number of shares for each of A, B, C, D, and E. There has m groups and each group has a threshold value t_i and a weight of group w_{G_i}. We try to apply a two-level threshold scheme by assigning the users into different groups. Now we try to prove that for any assignment of the users into groups, the function f cannot be realized by a two-level threshold SSS.

We divided the cases as follows:

Case 1: $\{\{A, B, C, D, E\}\}$ or $\{\{A\}, \{B\}, \{C\}, \{D\}, \{E\}\}$

The structure of $\{A, B, C, D, E\}$ and $\{\{A\}, \{B\}, \{C\}, \{D\}, \{E\}\}$ are the same. The subset $\{A, B, C, D, E\}$ considers as a special case in two-level threshold scheme by assign all member into a group. It considers as a normal SSS which only have a threshold t.

From the function f we know that A and B together can compute the secret, it must be $w_a + w_b \geq t$. Similarly, since C and D together can compute the secret, it is true that $w_c + w_d \geq t$.

Now assume without loss of generality, $w_a \geq w_b$ and $w_c \geq w_d$. Since $w_a + w_b \geq t$ and $w_a \geq w_b$, $w_a + w_a \geq w_a + w_b \geq t$, therefore $a \geq t/2$. Similarly, $w_c \geq t/2$, then $w_a + w_c \geq t$. But for the function f, $f(10100) = 0$. Then it is a contradiction.

For the subset $\{\{A\},\{B\},\{C\},\{D\},\{E\}\}$, each member assigned to a group in the lower level of two-level threshold scheme. It also considers as one level scheme and the proof just same with previous case by assuming the weight of user as the weight of the group. For example, $w_a = w_{G_1}$, $w_b = w_{G_2}$, and etc.

Case 2: $\{\{A,B\},\{C,D,E\}\}$ or $\{\{A,C\},\{B,D,E\}\}$

In this case, we try to assign the users into two groups by randomly assign any two users in a group and another three users as a group. We consider another two conditions which are the two users assigned in a group together can compute the secret or not.

First, we consider the subset $\{\{A,B\},\{C,D,E\}\}$. Since A and E together can compute the secret, then it is true that $w_a \geq t_1$ and $w_e \geq t_2$. In the first level, A represents as group one that has the weight w_{G_1} and E represent as group two that has the weight w_{G_2}. Similarly, B and C together also can compute the secret, then $w_b \geq t_1$ and $w_c \geq t_2$. In the first level, B also represent as group one that has the weight w_{G_1} and C represent as group two that has the weight w_{G_2}

Of course we have $w_{G_1} + w_{G_2} \geq t$. Since $w_a \geq t_1 \geq w_{G_1}$ and $w_c \geq t_2 \geq w_{G_2}$, then A and C together can compute the secret. But f(10100)=0. It is a contradiction.

The proof for the subset $\{\{A,C\},\{B,D,E\}\}$ is similar.

Case 3: $\{\{A,B,C\},\ \{D\},\{E\}\}$ or $\{\{A,B,D\},\{C\},\{E\}\}$

In this case, we try to assign the users in three groups by randomly assign any three users in a group and another two users as two single groups. we consider the subset $\{A,B,C\},\{D\},\{E\}$. Since B and C together can compute the secret, it is true that $w_{G_1} \geq t$. But C and D together also can compute the secret, then it is true that $w_c \geq t_1$ and $w_d \geq t_2$. In the first level, C can represent as group one that has the weight w_{G_1} and D as group two that has the weight w_{G_2}. Since C can represent as group one and $w_{G_1} \geq t$, this shows that C alone can compute the secret. But f(00100)=0. It is a contradiction.

The proof for the subset $\{\{A,B,D\},\{C\},\{E\}\}$ is similar.

Case 4: $\{\{A,B\},\{C\},\{D\},\{E\}\}$ or $\{\{A,C\},\{B\},\{D\},\{E\}\}$

In this case, we try to assign the users in four groups by randomly assign any two users in a group and another three users as a single group. We consider the subset $\{\{A,B\},\{C\},\{D\},\{E\}\}$. We know that A and B together can compute the secret, then it is true that $w_{G_1} \geq t$. But A together with E can compute the secret as well. So $w_a \geq t_1$ and $w_e \geq t_2$. In the first level, A can represent as group one that has the weight w_{G_1} and E can represent as group four that has the weight w_{G_4}. Since A can represent as group one and $w_{G_1} \geq t$, this shows that A alone can compute the secret. But f(10000)=0. Again, it is a contradiction.

Another case, we consider the subset $\{\{A,C\},\{B\},\{D\},\{E\}\}$. We know that A and B together can compute the secret, then it is true that $w_a \geq t_1$ and $w_b \geq t_2$. We also know that C and D together can compute the secret, so it is true that $w_c \geq t_1$ and $w_d \geq t_3$. In the first level, A and C can represent as group one that has the weight w_{G_1} while B can represent as group two that has the weight w_{G_2} and D can represent as group three that has the weight w_{G_3}.

Again, now we have $w_{G_1} + w_{G_3} \geq t$. This shows that A together with D can compute the secret. But f(10010)=0. It is a contradiction.

Case 5: $\{\{A,C\},\{B,D\},\{E\}\}$ or $\{\{A,B\},\{C,D\},\{E\}\}$ or $\{\{A,B\},\{C,E\},\{D\}\}$

In this case, we assign the users in three groups by randomly assign one user in a group and another four users as two different groups. We consider the subset $\{\{A, C\}, \{B, D\}, \{E\}\}$. We know that A and B together can compute the secret, so it is true that $w_A \geq t_1$ and $w_b \geq t_2$. We also know that C and D together can compute the secret, so $w_c \geq t_1$ and $w_d \geq t_2$. In the first level, A and C can represent as group one that has weight w_{G_1} while B and D can represent as group two that has weight w_{G_2}.
Now we assume $w_{G_1} + w_{G_2} \geq t$. This shows that A and C together can compute the secret. But f(10100)=0. So it is a contradiction.

For the subset $\{\{A, B\}, \{C, D\}, \{E\}\}$. We know that A and B together can compute the secret, it is true that $w_{G_1} \geq t$. But A together with E also can compute the secret as well. So it is also true that $w_a \geq t_1$ and $w_e \geq t_3$. In the first level, A alone can represent as group one that has the weight w_{G_1} and E can represent as group three that has the weight w_{G_3}. Since A can represent as group one and $w_{G_1} \geq t$, This shows that A alone can compute the secret. But f(10000)=0. It is a contradiction too.
The proof for the subset $\{\{A, B\}, \{C, E\}, \{D\}\}$ is similar with the subset $\{\{A, B\}, \{C, D\}, \{E\}\}$.

Case 6: $\{\{A, B, C, D\}, \{E\}\}$
In this case we assign the users in two groups by randomly assign one user in a group and another four users in a group. We consider the subset $\{A, B, C, D\}, \{E\}$. From the function f we know that A together with B can compute the secret. It is true that $w_{G_1} \geq t$. We also know that A and E together can compute the secret as well. So $w_a \geq t_1 \geq w_{G_1}$ and $w_e \geq t_2 \geq w_{G_2}$.
Since $w_a \geq t_1 \geq w_{G_1}$ and $w_{G_1} \geq t$, this show that A alone can compute the secret. But f(10000)=0. Again, it is a contradiction.

□

4 Conclusion

From [BL88], we know that there exist monotone access structures for which there is no threshold scheme. They give an example by applying the traditional threshold SSS(one-level) for a group of users and it is proved to be insufficient. In this paper, we apply the two-level threshold SSS to the monotone access structure and we consider disjoint case which each user can be assigned into a group only. With a function f which defines as a monotone function on variables labeled by a set of users $P = \{A, B, C, D, E\}$, we give the proof to show that the access structure f cannot be realized by a two-level threshold SSS.

References

[BL88] Josh Benaloh and Jerry Leichter. "Generalized Secret Sharing and Monotone Functions". In *Crypto'88.*

[IST87] Mitsuru Ito, Akira Saito, and Takao Nishizeki. "Secret Sharing Scheme Realizing General Access Structure". In *Proc. Glob. Com,(1987).*

[AB83] C. A. Asmuth and J. Bloom. “A modular approach to key safeguarding”. IEEE Transactions on Information Theory, IT-29(2):208V210, 1983

[Sho00] V. Shoup. “Practical threshold signatures”. In B. Preneel, editor, Advances in Cryptology - EUROCRYPT 2000, volume 1807 of Lecture Notes in Computer Science, pages 207V220. Springer-Verlag, 2000.

[IG07] S. Iftene and M. Grindei. “Weighted threshold RSA based on the Chinese Remainder Theorem”. In Proceedings of the 9th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2007, pages 175V 181. IEEE Computer Society Press, 2007.

[Ift06] S. Iftene. General secret sharing based on the Chinese Remainder Theorem with applications in E-voting. In C. Dima, M. Minea, and F. L. TM iplea, editors, ICS 2006, International Workshop on Information and Computer Security, Timisoara, Romania, September, 2006.

[KST06] K. Kaya, A. A. SelcMuk, and Z. Tezcan. “Threshold cryptography based on Asmuth-Bloom secret sharing”. In A. Levi, E. Savas, H. YenigLun, S. Balcisoy, and Y. Saygin, editors, Proceedings of Computer and Information Sciences - ISCIS 2006, volume 4263 of Lecture Notes in Computer Science, pages 935V942. Springer-Verlag, 2006.

[Har94] L. Harn. “Group-oriented (t, n) threshold digitial signature scheme and digital multisignature”. IEE Proc.-Comput. Digit. Tech., 141(5):307-313, 1994.

[ELG85] T. ElGamal. “A public key cryptosystem and signature scheme based on discrete logarithms”. IEEE Trans. Inform. Theory, 31:469-472, 1985.

[Rab98] T. Rabin. “A simplified approach to threshold and proactive RSA”. In Advances in Cryptology-Crypto ‘98, 1998.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. Communications of the ACM, pages 120-126, 1978.

[Sha79] A. Shamir. “How to Share a Secret”. In *ACM 22, 11 (Nov. 1979), 612-613.*