Construction of Dynamic Threshold Scheme

Cheng Guo, Mingchu Li, Yizhi Ren†, Kouichi Sakurai‡

†Dalian University of Technology, School of Software, 116621 China
guo8016@gmail.com

‡ Kyushu University, Dept. of Informatics, 744 Motooka, Nishi-ku, Fukuoka 819-0395 JAPAN
sakurai@inf.kyushu-u.ac.jp

Abstract In this paper, we provide a new dynamic threshold secret sharing scheme based on Shamir's scheme and YCH's scheme. In our scheme, the participants just need to broadcast the r_j that is related to the secret that they want to obtain to other participants, and the corresponding threshold scheme will be constructed. And the whole reconstructed process doesn't need the trusted dealer's participation.

1 Introduction

1.1 Background

A secret sharing scheme is a technique to share a secret among a group of participants. In 1979, Shamir [1] and Blakley [2] firstly developed the threshold schemes based on the Lagrange interpolating polynomial and the Linear projective geometry, respectively. A secret sharing scheme contains a trusted dealer and n participants. The dealer divides the shared secret into n shadows and distributes them to these n participants over a secure channel. In the (t,n) threshold scheme, at least t honest participants can reconstruct the shared secret, but $(t\text{-}1)$ or fewer participants can not obtain anything about the secret.

1.2 Motivation

In multi-secret sharing schemes, there are multiple secrets shared among a group of participants. But in some situations, different secrets have distinct security requirements. Such as launching a nuclear missile, maybe two vice presidents can decide to launch a one million tons TNT equivalent explosion nuclear missile, and three vice presidents can decide to launch a five million tons TNT equivalent explosion nuclear missile. So, to solve the problem, dynamic threshold schemes have been proposed. In such schemes, that revealing each secret with different security requirement requires the cooperation of a different number of participants. In 1989, C.S. Laih, L. Harn and J.Y. Lee [3] proposed a so-called 'dynamic threshold scheme', in which the reconstructed secret can change dynamically, and the threshold value decreases in proportion to the number of different subshadows which have been revealed. However, the traditional dynamic threshold schemes [3-5] are all "on-line" secret sharing schemes. In order to realize dynamic threshold scheme according to secret's distinct security requirements, the dealer can not leave the system. Whenever the participants want to share another secret with distinct threshold value, the dealer needs to republish additional public information. The motivation of our work is to construct a dynamic threshold scheme that can automatically reconstruct different secrets according to the different number of cooperated participants without the dealer's participation.

1.3 Previous work

In 1994, H.-M. Sun and S.-P. Shieh [4] proposed a new (m,t) dynamic threshold scheme which allows the shared secret to be renewed without changing the shadows. Further more, L. Harn [5] presented the verifiable multi-secret sharing (VMSS) in 1995. He assumed that there are multiple secrets shared among a group of users and that revealing each secret requires the cooperation of a different number of participants. But in their scheme, assume that S_i is the secret with threshold value i. In order to reconstruct the secret S_i, the dealer needs to publish these n-i public subshadows. But, if participants want to share another secret, the dealer will have to republish the corresponding number of public subshadows according to its threshold value. In 2004, C.-C. Yang, T.-Y. Chang and M.-S. Hwang (YCH) [6] proposed a new MSS scheme based on Shamir's secret sharing scheme and the two-variable one-way function. In 2008, M.H. Dehkordi, S. Mashhadi [7] proposed an efficient threshold verifiable multi-secret sharing scheme based on YCH [6], intractability of Discrete Logarithm (DL) and RSA cryptosystem.

1.4 Our contributions

Our scheme is based on Shamir's secret sharing scheme and YCH's scheme. Our scheme has the following features:

1. Our scheme can share distinct secret among the participants according to the different number of cooperated participants without changing or redistributing new shadows securely. Meanwhile, only one shadow, which is reusable, should be kept by each participant.
2. Further more, additional public information doesn't need to be republished by the dealer, and the process of changing threshold value is automatic.
3. Additionally, our scheme also provides the capability to detect and identify cheaters.

2 New dynamic threshold scheme

In this section, we shall construct an efficient (m,n,t) dynamic threshold scheme which provides different threshold values according to the secrets' different security requirements. As a prerequisite, there are secure channels and a broadcast channel among participants. In our scheme, the secrets can be shared among t participants, and m and n denote lower limit and upper limit of the threshold values, respectively. The higher the secret's security requirement is, the higher the threshold value is. Thus, we set up a threshold value (m, or m+1, or,..., n) for each secret according to its security requirement. Our scheme not only resolves the problem that the dealer has to republish the corresponding number of subshadows, but also can detect the cheating and identify any cheater. Our scheme is based on Shamir's scheme and YCH's scheme and is comprised of three stages: (1) initialization, (2) shadow generation and distribution, (3) pseudo shadow verification and secret reconstruction. The details of three stages are as follows:

2.1 Initialization

The dealer first creates a public notice board (NB) which is used for storing necessary public parameters. The participants can access those parameters on the NB. The contents on the board can only be modified or updated by dealer. The parameters are defined by dealer as follows: Let $f(r,s)$ be a two-variable one-way function, whose definition is as same as that in YCH's scheme; Let p be a safe prime, such as $q \mid (p\text{-}1)$, where q is a big prime, and all the numbers are elements in the finite field $GF(p)$, and g is the generator of order q over $GF(p)$. The trusted dealer randomly selects t distinct integers, $s_1,s_2,...,s_t$, as participants' secret shadows and distributes them to every participants over a secure channel. Then the dealer selects n-m distinct integers, $r_1,r_2,...,r_{n\text{-}m}$ as $f(r,s)$'s parameters.

Here, we use $P_1,P_2,...,P_{n\text{-}m}$ to denote n-m secrets to be shared among t participants.

2.2 Shadow generation and distribution

In our scheme, there are multiple secrets shared among a group of participants and that revealing each secret requires the cooperation of a different number of participants. Thus, without loss of generality, we can set up a threshold value k (k=m, or m+1, or ... or n) for each secret according to its security requirement.

1. Firstly, construct a (m-1)th degree polynomial $A(x)= a_0+ a_1x+...+a_{m\text{-}1}x^{m\text{-}1} \ mod\ p$ where a_0 is the secret corresponding to the threshold value k=m, and a_1, a_2,..., $a_{m\text{-}1}$ are randomly chosen from $GF(p)$.

2. Choose an integer r_1 and compute $y_i^1 = A(f(r_1,s_i))$ for i=1,2,..., t.

3. Compute $G_i^1 = g^{f(r_1,s_i)} \bmod p$ for i=1,2,..., t.

4. Publish $(r_1, y_1^1, y_2^1,\ldots,y_t^1, G_1^1, G_2^1,\ldots,G_t^1)$ on the notice board.

From the above, we have already construct a (m,t) threshold secret sharing scheme. Now, we shall repeat the process to construct a (m+1,t) threshold secret sharing.

1. Construct a mth degree polynomial $B(x)=b_0+b_1x+...+b_{m\text{-}1}x^{m\text{-}1}+b_mx^m \ mod\ p$ where b_0 is the secret corresponding to the threshold value k=m+1, and $b_1,b_2,...,b_{m\text{-}1},b_m$ are randomly chosen from $GF(p)$.

2. Choose an integer r_2 and compute $y_i^2 = B(f(r_2,s_i))$ for i=1,2,..., t.

3. Compute $G_i^2 = g^{f(r_2,s_i)} \bmod p$ for i=1,2,..., t.

4. Publish $(r_2, y_1^2, y_2^2,\ldots,y_t^2, G_1^2, G_2^2,\ldots,G_t^2)$ on the notice board.

So, according to the above method, the dealer can construct n-m various polynomials which degree is from m-1 to n-1. The n-m different secrets are embedded in the n-m different interpolating polynomials and each participant just keeps one shadow associated to the n-m interpolating polynomials.

$A(x) = a_0+a_1x+...+a_{m\text{-}1}x^{m\text{-}1} \ mod\ p$;

$B(x) = b_0+b_1x+...+b_{m\text{-}1}x^{m\text{-}1}+b_mx^m \ mod\ p$;

......

$H(x) = h_0+h_1x+...+h_{m\text{-}1}x^{m\text{-}1}+h_mx^m+...+h_{n\text{-}1}x^{n\text{-}1} \ mod\ p$.

Then the dealer will publish

$(r_1, y_1^1, y_2^1,\ldots,y_t^1, G_1^1, G_2^1,\ldots,G_t^1)$;

$(r_2, y_1^2, y_2^2, \ldots, y_t^2, G_1^2, G_2^2, \ldots, G_t^2)$;

......

$(r_{n-m}, y_1^{n-m}, y_2^{n-m}, \ldots, y_t^{n-m}, G_1^{n-m}, G_2^{n-m}, \ldots, G_t^{n-m})$

on the notice board corresponding to *n-m* various polynomials *A*(*x*), *B*(*x*), ... , *H*(*x*).

2.3 Pseudo shadow verification and secret reconstruction

To recover some secret, the combiner or the participants firstly broadcast the corresponding r_j to other participants and we assume that the corresponding threshold value is *k* and the (*k*-1)th degree polynomial *F*(*x*) is relative to r_j. Then every participant will compute their pseudo shadow $f(r_j,s_i)$ according to the r_j and his own secret shadow s_i, *i*=1,2,…,*t*. Without loss of generality, assume that at least *k* participants pool their pseudo shadow $f(r_j,s_i)$s (for *i*=1,2,...,*k*), and every participants can check whether others' pseudo shadows are valid by the following equations:

$$g^{f(r_j,s_i)} = G_i^j \bmod p, \quad i=1,2,...,k.$$

By using the Lagrange interpolation polynomial, with the knowledge of *k* pairs of ($f(r_j,s_i), y_i^j$), the (*k*-1)th degree polynomial *F*(*x*) can be uniquely determined as follows:

$$\begin{aligned} F(x) &= \sum_{i=1}^{k} y_i^j \prod_{i'=1, i'\neq i}^{k} \frac{x - f(r_j, s_{i'})}{f(r_j, s_i) - f(r_j, s_{i'})} \bmod q \\ &= f_0 + f_1 x + \ldots + f_{k-1} x^{k-1} \bmod p \end{aligned} .$$

From the obtained polynomial *F*(*x*), we can easily get the corresponding secret f_0.

If the combiner or the participants want to reconstruct another secret with distinct threshold value, they will broadcast the corresponding *r* value to other participants, and repeat the above work according to the Section 2.3's description. The whole process of changing threshold value and sharing other secrets can be initiated by the combiner or participant instead of the dealer.

3 Feasibility and security analysis

3.1 Feasibility analysis

Because our dynamic threshold scheme is based on Shamir's scheme and YCH's scheme, and the verification algorithm is the same as that of the M.H. Dehkordi and S. Mashhadi's scheme [7], we will just analyze the construction of dynamic threshold scheme as follows.

Our scheme provides an efficient and dynamic way for sharing information. The threshold value can change dynamically according to the shared secret's change with distinct security requirements. We set up the dynamic threshold scheme by constructing *n-m* different polynomials which degree is from *m*-1 to *n*-1. And each polynomial is related to a secret and a threshold value *k*, and each polynomial can be located by corresponding two-variable one-way function $f(r_j,s_i)$'s parameter r_j ($1 \leq j \leq n\text{-}m$). Apparently, compared with L. Harn's dynamic threshold scheme [5] that requires *n-i* additional public subshadows to obtain secret S_i, our scheme does not need to republish additional public information for the updated threshold value. The participant just broadcasts the r_j corresponding to the secret that they want to obtain to other participants, then other participants will compute their pseudo shadow $f(r_j,s_i)$. Consequently, a big enough number of participants pool their pseudo shadows together, then we can automatically construct the corresponding polynomial. We assume that the corresponding threshold value is k. Without loss of generality, if at least k participants pool their pseudo shadows $f(r_j,s_i)$ (for i=1,2,…,k), then k pairs ($f(r_j,s_i),y_i^j$) (for i=1,2,…,k and $1\leq j\leq n-m$) can reconstruct the corresponding polynomial, whose reconstruction process is as same as that in Shamir's scheme. So, in our scheme, we use the two-variable one-way function $f(r,s)$'s parameter r to locate the corresponding polynomial, and determine which secret will be reconstructed.

In shadow generation and distribution phase, the dealer needs to construct multiple interpolating polynomials, and publish a great amount of public values. The number of polynomials depends on the shared secrets' security requirements. In our scheme, we can assume that the number is l (l=n-m), and in order to share l secrets with different security requirements, the dealer has to publish $l(2t+1)$ public values. Maybe, overmany public values will affect the storage and communication complexity of the scheme. However, when the dealer finished the shadow generation and distribution phase, the dealer may be revoked. The following work, such as pseudo shadow verification, secret reconstruction and threshold value's change, is quite efficient and simple. From the perspective of participants, the pseudo shadow generation and verification is the same as that of the M.H. Dehkordi and S. Mashhadi's scheme [7]. And the secrets are reconstructed only by using Lagrange interpolation polynomial. Therefore our secret reconstruction is as easy as Shamir's scheme. In particular, we need to specially emphasize that the process of changing threshold value is efficient and automatic compared with traditional schemes. The combiner or the participant just needs to broadcast corresponding r value to other participants, then the specified threshold value and the shared secret will be confirmed. Based on the above views, our dynamic threshold scheme is efficient and feasible.

3.2 Security analysis

In this section, the security of our scheme can be analyzed from the following different views.

1. The security of our scheme in reconstructing polynomial $F(x)$ for fewer than k ($m \leq k \leq n$) participants, similar to YCH's scheme, is based on the security of Shamir's scheme. Any (k-1) or fewer participants cannot determine the polynomial $F(x)$ and derive anything about the secret.

2. In our scheme, even though n pseudo shadow $f(r_j,s_i)$s have been revealed among cooperating participants, the real secret shadow s_i is still well protected by the two-variable one-way function $f(r_j,s_i)$. Therefore, the trusted dealer does not need to redistribute fresh secret shadows to every participant in the next secret sharing session. The dealer only has to publish another random integer r_j.

3. Our scheme's verification phase is the same as that of M.H. Dehkordi and S. Mashhadi's scheme [7] that can well identify the cheaters. An adversary cannot derive the secret shadow $f(r_j,s_i)$ from G_i^j ($g^{f(r_j,s_i)}=G_i^j$) because it is based on the

intractability of discrete logarithm in the finite field $GF(p)$.

4. The reconstruction of a secret cannot reveal anything of the remaining secrets that haven't been reconstructed. We assume that the combiner broadcasts r_j corresponding to the threshold value k to other participants. If more than k participants pool their pseudo shadow $f(r_j,s_i)$s, whether the combiner can reveal additional information except the secret that are relative to the threshold value k. In our scheme, the different r values are related to different threshold values. Consequently, based on the properties of the two-variable one-way function $f(r,s)$, given s, it is hard to find two different values r_i and r_j such that $f(r_i,s) = f(r_j,s)$. So, with the knowledge of more than k pairs of $(f(r_j,s_i),y_i)$, the combiner can not reconstruct other polynomials that are related to the additional secrets.

4 Conclusion

In this paper, we propose a new dynamic threshold secret sharing scheme based on Shamir's and YCH's secret sharing scheme. Our scheme can provide different threshold values according to secrets' security requirements and the process of reconstructing different secrets doesn't need to republish additional public values provided by dealer. Furthermore, each participant just keeps one secret shadow. The participants just need to broadcast the r_j corresponding to the secret that they want to obtain to other participants, the corresponding threshold secret sharing scheme will be constructed, and reconstructed process is the same simple as that of Shamir's scheme. Meanwhile, our scheme gives a verification algorithm. Finally we propose several applications of our dynamic threshold scheme. Owing to construct n-m different polynomials according to n-m variable threshold values, the computation quantity and the number of public values also increase unavoidably. But we have shown a secret sharing scheme that can automatically provide dynamic threshold value according to different secrets' security requirements. The feasibility and security analysis shows that our scheme is secure and practical.

参考文献

[1] A. Shamir, "How to share a secret," Communications of the ACM, vol.22, no.11, pp.612-613, 1979.

[2] G. Blakley, "Safeguarding cryptographic keys," Proc. The National Computer Conference, Montvale: NCC, pp.313-317, 1979.

[3] C.S. Laih, L. Harn and J.Y. Lee, "Dynamic Threshold Scheme Based on the Definition of Cross-Product in an N-Dimensional Linear Space," Proc. Advances in Cryptology: Eurocrypt'89, Springer-Verlag, Berlin, pp. 286-298, 1990.

[4] H.-M. Sun and S.-P. Shieh. Construction of dynamic threshold schemes, Electronics Letters, vol.30, no.24, pp. 2023-2025, 1994.

[5] L. Harn, "Efficient sharing (broadcasting) of multiple secret," IEE Proc. Comput. Digit. Tech., vol.142, no. 3, pp. 237-240, 1995.

[6] C.-C. Yang, T.-Y. Chang and M.-S. Hwang, "A (*t*,*n*) multi-secret sharing scheme," Applied Mathematics and Computation, vol.151, no.2, pp. 483-490, 2004.

[7] M.H. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multi-secret sharing," Computer Standards & Interfaces, vol.30, no.3, pp.187-190, 2008.