TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.6, June 2014, pp. 4463 ~ 4467
DOI: 10.11591/telkomnika.v12i6.5483

Improved Multi-secret Sharing Scheme Based on One-Way Function

Geng Yong-Jun*[1], Guo Li-Zheng[1], Zheng Ming-Hui[2]
[1]Department of Computer Science and Technology, Henan University of Urban Construction,
Pingdingshan 467036, Henan, China
[2]Information Academy Hubei University of Nationalities,
Enshi 445000, Hubei, China
*Corresponding author, e-mail: geng@hncj.edu.cn

Abstract

The weakness He-Dawson's threshold multi-secret sharing scheme is presented and analyzed. By using the one-way function thought in the He-Dawson scheme, a new multi-use and multi-secret sharing scheme is proposed. The improved scheme is multi-time-use of once secret shares distribution and can resist conspiring attack. Furthermore, the new scheme is multi-secret sharing, group secrets can be reconstructed in free order and different group secret is corresponding to different threshold value which can meet with different practical application. At last, the security and efficiency of the new proposed multi-secret sharing scheme are analyzed.

***Keywords**: Lagrange interpolating polynomial, linear projective geometry, secret sharing, threshold, one-way function*

1. Introduction

Secret sharing schemes based on Lagrange interpolating polynomial and linear projective geometry were proposed independently by Blakley [1] and Shamir [2]. In a (t, n) threshold secret sharing scheme, secret holder delivers the distinct secret values (called shares or shadows) to n participants. At least t or more participants can combine their shares and recover the secret, but only t-1 or less members cann't. Based on these properties, secret sharing has been used in many fields of modern cryptography and is an important part of modern cryptography.The motivation for secret sharing is secure key management. In some situations, there is usually a key that provides access to many important files. If such a key is lost (e.g., the person who knows the key is lost, or the computer that stores the key is destroyed), then all the important files become inaccessible. The basic idea in secret sharing is to divide the secret key into pieces and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the key. The thought can be realized by mathematics methods. A (t, n) threshold scheme is a technique to share a key among n users. A threshold scheme has many practical applications, such as opening a bank vault or authenticating an electronic funds transfer. However, there are several situations in which many different secrets need to be shared among a group of users. In a straightforward approach, we can solve the problem by using any exiting threshold scheme repeatedly and distributing multiple secret shadows to each user in the group. According to [3], when a group secret has been reconstructed, if another secret need to be reconstructed,it is required that the trusted center (TC) redistribute fresh shares to every participant, which is called a one-time-use scheme. To distribute shares is a very punctilious and costly process. For this reason, the property of multi-time-use of once secret shares distribution is necessary in secret sharing schemes. He-Dawson [4] proposed a multi-stage secret sharing scheme to share multiple secrets based on one-way function. They used the public shift technique to obtain the true shares and the successive applications of one-way function to make the secrets reconstructed stage-by-stage in special order. The scheme allows a group of users to share multiple secrets and each user only needs to keep one shadow. Later, Harn [5] proposed an alternative scheme to realize the same function. Chang [6] also proposed a scheme that he claimed it was superior to He-Dawson and Harn's two schemes. However, Chang declared his scheme reconstructed

Received December 24, 2013; Revised February 18, 2014; Accepted March 3, 2014

group secrets in the fixed order rather than free order. Recently, another several multi-secret scheme [7-9] were proposed, ther are less efficient than He-Dawson's scheme which uses one-way function to realize multi-secret sharing.

In this paper, we will show He-Dawson scheme's weakness that it is one-time-use scheme and can't endure conspiring attack. At the same time, we shall also use the one-way function thoughts in the He-Dawson scheme to propose a new multi-secret sharing scheme. The new scheme is multi-time-use of once secret shares distribution and secure. Furthermore, the new scheme is multi-secret sharing, group secrets can be reconstructed in free order and different group secret is corresponding to different threshold value which can meet with different practical application. At last, the security of the new proposed multi-secret sharing scheme between the new and the old scheme are analyzed.

2. Characeristics of One-way Hash Function

A hash function *h* () is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value *h* (that is, *h* = *h*(m)). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties. The basic requirements for a cryptographic hash function are: the input can be of any length, the output has a fixed length, *h* (x) is relatively easy to compute for any given *x* , *h* (x) is one-way, *h* (x) is collision-free. A hash function *h* () is said to be one-way if it is hard to invert, where "hard to invert" means that given a hash value *h*, it is computationally infeasible to find some input *x* such that h (x) = *h*. If given a message *x*, it is computationally infeasible to find a message *y* not equal to *x* such that *h* (x) = *h* (y) then *h ()* is said to be a weakly collision-free hash function.A strongly collision-free hash function *h()* is one for which it is computationally infeasible to find any two messages x and y such that *h(x) = h(y)*. The hash value represents concisely the longer message or document from which it was computed; one can think of a message digest as a "digital fingerprint" of the larger document. Examples of well-known hash functions are MD2 and MD5 and SHA. Perhaps the main role of a cryptographic hash function is in the provision of digital signatures. The following schemes use the characteristics of the hash function to realize efficient multi-secret sharing.

3. He-Dawson's Multi-secret Sharing Scheme

In He-Dawson's scheme, the trusted center (TC) generates the group secrets and makes group members reconstruct group secrets in special order. They claimed their scheme to be a multi-time-use scheme of once secret shares distribution. Their scheme notations are defined as follows. Let $h : Z_p \to Z_p$ be any one-way function and p is a big prime integer while $h^k(m)$ denotes k successive applications of h to m; i.e., $h^0(m) = m$, and $h^k(m) = h(h^{k-1}(m))$. Assume the TC wants to share k secrets s_i (for $i = 1,2,\cdots,k$) and at least t participants can reconstruct the secrets. Then, the TC randomly chooses n distinct integers ID_i (for $ID_i \in Z_p^*$) as the participants' public identity information and performs the following steps:

Step 1: Randomly choose $x_1, x_2, \cdots, x_n$ $(x_i \in Z_p^*)$ as the secret shares.

Step 2: For $i = 1,2,\cdots,k$ executes the following steps:

1. Constructs a polynomial $P_i(x)$ of degree (t-1) and $P_i(0) = s_i$.

2. Computes $Z_{ij} = P_i(ID_j)$,for $j = 1,2,\cdots,n$.

3. Computes $d_{ij} = Z_{ij} - h^{i-1}(x_j)$ as the shift values and $h^{i-1}(x_j)$ as the pseudo shares , for $j = 1,2,\cdots,n$.

Step 3: Delivers x_i to each participant secretly and publishes all d_{ij} , for $i = 1,2,\cdots,k$ and $j = 1,2,\cdots,n$.

At least t participants provide their pseudo shares in the special order: $h^{k-1}(x_j), h^{k-2}(x_j), \cdots, h^0(x_j)$ (for $j = 1,2,\cdots,t$), to reconstruct the polynomials $P_i(x)$ for $i=k,k-1,\cdots,1.$

Then each secret is reconstructed through the following formula ($i = k, k-1, \cdots, 1.$):

$$s_i = P_i(0) = \sum_{a=1}^{t} (h^{l-1}(x_a) + d_{ia}) \prod_{b=1, b\neq a}^{l} \frac{-ID_b}{ID_a - ID_b} \quad (1)$$

The secret are reconstructed in the special order; $s_k, s_{k-1}, \cdots, s_1$.

4. The Shortage of He-Dawson's Scheme

He-Dawson's Scheme isn't multi-time-use scheme. To reconstruct the final secret s_1, at least t participants must provide their pseudo shares $h^0(x_i)$ for $i = 1,2,\cdots,t$. Note that $h^0(x_i) = x_i$. So, after reconstructing all the secrets, the TC must distribute new secret shadow x_i' to each participant over a secret channel because old member secret shares x_i has been publicized. Thus, their schemes belongs to the one-time-use scheme.

He-Dawson's scheme can't endure conspiring attack. If someone first provides her/his pseudo share $h^1(x_1)$, the other participants can easily obtain her/his pseudo shares $h^2(x_1), h^3(x_1), \cdots, h^{k-1}(x_1)$. Then only (t-1) other participants can cooperate to reconstruct the secrets $s_2, s_3, \cdots, s_k$.

5. The Improved Multi-time-use Multi-secret Sharing Scheme

5.1. System parameters Initialization and Secret Shadows distribution

The proposed scheme notations are defined as follows. Let $h: Z_p \to Z_p$ be a secure one-way function and p is a big prime integer while $h^k(m)$ denotes k successive applications of h to m and g is a primitive element of Z_p^*. Assume the TC wants to share k group secrets s_i (for $i = 1,2,\cdots,k$) and different t participants can reconstruct the corresponding group secrets. the trusted center (TC) randomly chooses n distinct integers ID_i $(ID_i \in Z_p^*)$ as the participants' public information and performs the following steps:

Step 1: Randomly choose $x_1, x_2, \cdots, x_n$ $(x_i \in Z_p^*)$ as the member secret shares.

Step 2: For $i = 1,2,\cdots,n$ executes the following steps:

1) Construct a polynomial $P_i(x)$ of degree (t-1) and compute group secrets s_i, $v = P_i(0)$, $s_i = g^v \bmod p$.
2) Compute $Z_{ij} = P_i(ID_j)$, for $j = 1,2,\cdots,n$.
3) Compute, $c_{ij} = h^{i-1}(x_j) \bmod p$, $d_{ij} = Z_{ij} - h^{i-1}(x_j)$ and $q_{ij} = g^{c_{ij}} \bmod p$ as the pseudo shares, for $j = 1,2,\cdots,n$.
4) Compute $r_{ij} = g^{d_{ij}} \bmod p$ for $j=1,2,\cdots,n.$

Step 3: Deliver x_i to each participant secretly and publish all r_{ij} for $i = 1,2,\cdots,k$ and $j = 1,2,\cdots,n$.

5.2. Group Secret Reconstruction

Without losing generality, assume that n different group secrets reconstruction policy exit in the group. For each policy, there is a corresponding group secret and threshold value. s_i

$(i=1,2,\cdots,n)$ are group secrets. Assume to reconstruct the group secret s_l by the co-operation of at least *l* participants . They provide their pseudo shares q_{lj} (for $j=1,2,\cdots,l$) to the group secret combiner. After the group secret combiner receives pseudo shares q_{lj}, he reconstructs the group secret s_l through the following formula:

$$\begin{aligned} s_l &= \prod_{j=1}^{l}(r_{lj}q_{lj})^{\prod_{b=1,b\neq j}^{l}\frac{-ID_b}{ID_j-ID_b}} \\ &= g^{\sum_{j=1}^{l}(Z_{lj}-h^{l-1}(x_j)+h^{l-1}(x_j))\prod_{b=1,b\neq j}^{l}\frac{-ID_b}{ID_j-ID_b}} \\ &= g^{P_l(0)} \bmod p \end{aligned} \qquad (2)$$

The group secrets can be reconstructed in the free order.

6. Analyses of the Improved Scheme's Security

6.1. The Scheme is Multi-time-use

To reconstruct the group secret s_l, at least l participants must provide their pseudo shares q_{lj}. From $q_{lj} = g^{c_{lj}} \bmod p$, attacker can't get $c_{lj} = h^{l-1}(x_j) \bmod p$ because it is a discrete logarithm problem. Though attacker can get c_{lj}, he still can't get x_i because of one-way function's character. On the other hand, to share k secrets in our scheme, each participant only need to keep one secret share x_i.

6.2. The New Scheme is Multi-secret Sharing

It improves the flexibility of the scheme and can meet with different practical application because different group secrets is corresponding to different secret polynomial function in the scheme initialization. The group secret s_i $(i=1,2,\cdots,k)$ can be reconstructed in free order. If s_l is be reconstructed, s_{l-1} and s_{l+1} isn't influenced because attacker can't get member secret sharing according to discrete logarithm problem.

6.3. Less than Threshold Value Members can't Reconstruct Corresponding Group Secret

Attackers can't recover secret polynomial $P_l(ID_j)$ because these problems are based on discrete logarithm problem security and Shamir's secret sharing scheme.

6.4. The Scheme can Resist Conspiring Attack

If some group members want to conspiring attack to generate group secret, the reconstructing formula can't work successfully because attacker can't impersonate right r_{lj}.

7. Analyses of the Improved Scheme's Performance

Shamir's secret sharing, discrete logarithm problem and one way function are used in the multi-secret sharing scheme so that their computation complexity is different. Their difference of performance is listed in the following Table 1. √ represents the security mechanism is used and ×represents the security mechanism isn't used.

Table 1. Performance Comparison of Scheme 1 [4], Scheme 2 [10] and Improved Scheme

Security mechanism	Improved scheme	Scheme 1 [4]	Scheme 2 [10]
Shamir's secret sharing	√	√	√
discrete logarithm problem	√	×	√
one way function	√	√	×

The three scheme is emulated in such runtime environment as Celeron 1.4GHz + 1G RAM + Windows XP + VC8.0. The experiment mainly compares member secret shadow distribution and sharing secret reconstruction's efficiency in the three scheme. Sha1 is selected as one way function, modulo p of 512,768,1024 and 1280 bit is selected.The comparison of efficiency in tne three scheme is as following Figure 1.

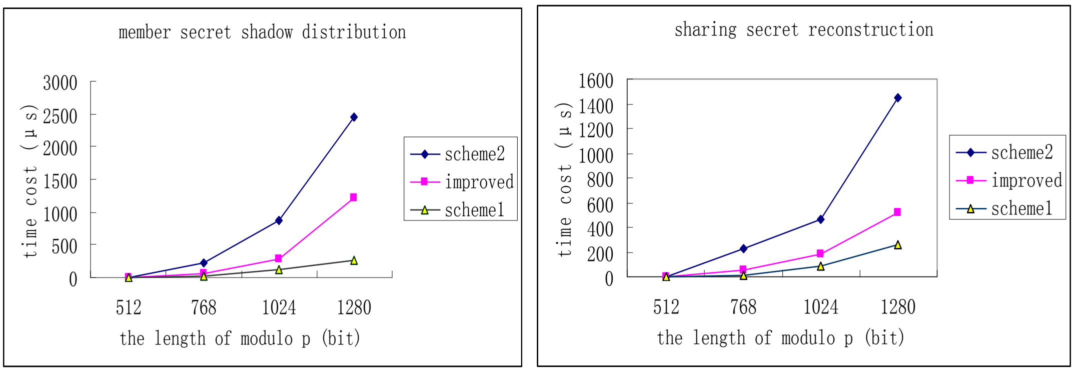

Figure 1. Comparison of Member Secret Shadow Distribution and Sharing Secret Reconstruction's Efficiency in the Three Scheme

8. Conclusion

The shortages of He-Dawson's multi-secret sharing scheme was analyzed and presented in this article, which is one-time-use scheme and can't resist conspiring attack. A improved new multi-secret sharing scheme was proposed by using the one-way function thoughts in the He-Dawson scheme. The improved scheme is multi-time-use of once secret shares distribution and can resist conspiring attack. Furthermore, the new scheme is multi-secret sharing, group secrets can be reconstructed in free order and different group secret is corresponding to different threshold value which can meet with different practical application. At last, the security and efficiency of the new proposed multi-secret sharing scheme are analyzed.

References

[1] GR Blakley. *Safeguarding cryptographic keys*. National Computer Conference. 1979; 48(1): 165-172.

[2] A Shamir. How to share a secret. *Communications of the ACM*. 1979; 22(11): 612-613.

[3] Wen-ai Jackson, Keith M Martin, Christine M O'Keefe. On sharing many secrets. Asiacrypt'94. 1994: 42-54.

[4] J He, E Dawson. Multistage secret sharing based on one-way function. *Electronics Letters.*1994; 30(19): 1591-1592.

[5] L Harn. Multistage secret sharing based on one-way function. *Electronics Letters*. 1995; 31(4): 262.

[6] Ting-Yi Chang, Min-Shiang Hwang, Wei-Pang Yang. A new multi-stage secret sharing scheme using one-way function. *Association for Computing Machinery*. 2005; 39(2): 48-55.

[7] Zhou Yousheng. Dynamic multi-secret sharing scheme based on cellular automata. *Journal of computer research and development.* 2012; 49(9): 1999-2004.

[8] Hou Jianchun. Improved verifiable multi-secret sharing scheme. *Computer Engineering and Applications.* 2012; 48(14): 94-97.

[9] Han Huiying. Variable threshold muti-secret sharing scheme, Natural science journal of harbin normal university. 2012; 28(3): 29-31.

[10] Zhao JJ, Zhang JZ, Zhao R. A practical verifiable multisecret sharing scheme. *Computer Standards & Interfaces*. 2007; 29(1): 138-141.