An Efficient Secret Sharing Scheme with Multi-dealer

Xin Huang[1], Guohua Xiong[2]
[1]Zhengzhou Information Science and Technology Institute
Zhengzhou
China
[2]Graduate school of Electronic Technology
Beijing
China
huangxin_1010@163.com

JDIM
Journal of Digital Information Management

ABSTRACT: *In order to solve the problem that there is only one dealer in the existing secret sharing scheme, based on large integer factorization and discrete logarithm problems, a new sharing scheme with multi-dealer is proposed, which is combined with Deffie-Hellman key agreement protocol. And then, security and performance analysis is made in this scheme. As the secret can be recovered with the shadows provided by participants and it is computationally difficult to get the sub-keys from the shadows, the sub-keys can be reused to share the multi-secret. The multiple dealers can commonly maintain the shared secret, which can be dynamically renewed by any dealers. The proposed scheme has higher safety and effectiveness over the existing schemes and is more practical.*

Categories and Subject Descriptors
D.4.6 **[Security and Protection]:** Authentication

General Terms:
Security, Secret Sharing

Keywords: Secret Sharing, Multi-dealer, Sub-key

Received: 29 January 2013, Revised 17 March 2013, Accepted 24 March 2013

1. Introduction

Secret sharing is a method of protecting secret among a group of participants. The concept of secret sharing was introduced respectively by Shamir [1] and Blakley [2] in 1979, the first scheme is based on Lagrange interpolation polynomial and the last scheme is based on projective geometry theory. In their schemes, a secret is divided into n shares, any t or more than t shares can restore the original secret, while less than t shares cannot. Since the secret sharing concept was proposed, many secret sharing schemes have been proposed and extensively discussed in the literatures [3-10]. However, few of them [3-5] concentrate on multi-dealer secret sharing, in which the secret is not decided by only one dealer. Multi-dealer secret sharing scheme has many practical applications, such as the secure system in secret database of banks, in which k managers are needed to turn on the secret database.

In 1999, Zhou, L [4] proposed the first multi-dealer secret sharing scheme, but in which the scheme cannot distinguish the cheatings between participants. Deng H [3] proposed a secret sharing scheme without any assumption of pre-fixed trust relationship. It checking mechanism is similar to the mechanism in paper [12], so it needs to publish much authentication information. Guo [5] proposed a threshold multi-secret sharing scheme based on the multi-dealer, each dealer can renew the shared secret. But this scheme's authentication mechanism is based on Wu-Wu cheating detection method [11] which increases computational complexity and communication volume.

In this paper, we propose a threshold secret sharing scheme with multi-dealer based on large integer factorization and discrete logarithm problems. It has the advantage that it can check whether there are cheatings between participants and dealers. In addition, in this scheme each participant only has to keep one shadow,

the number of secrets can be shared.

The rest of this paper is organized as follows. In section 2, we introduce some basic definitions of secret sharing schemes. In section 3, we present a new scheme. The analyses and discussions about the proposed scheme are given in section 4. At last we come to the conclusion in section 5.

2. Preliminaries

For convenience of description, we first introduce definitions and marks.

Definition 1: Participant: Participant is a person or a piece of equipment which has a sub-key, and can obtain secrets with other participants.

Definition 2: Center: Center is a person or a piece of equipment which provide paraments to dealers to help them achieve their purposes.

Definition 3: Dealer: Dealer is a person or a piece of equipment which can distribute the secret shares to participants.

Definition 4: Billboard: Billboard is a media distributor which can help the dealer announce the secret information. Only the dealer can modify and update the contents of the bulletin board, and participants have the permissions to read and download.

As described in clear and concise, we will use the following notation:

$D = \{D_1, D_2, ...D_n\}$: The set of n dealers.

$P = \{P_1, P_2, ...P_n\}$: The set of n participants.

3. New secret sharing scheme

This section specifically describes the new scheme, which includes three stages: initialization parameters, distribution and secret of recovery.

3.1 Parameter Initialization phase

In initialization phase, we complete system parameters selection.

At first, a center chooses two large prime numbers p and q, and calculate the product $N = pq$. Its purpose is to meet the security requirements of RSA cryptosystems: if an attacker knows N, he also cannot calculateand p and q. Subsequently, the dealer randomly selects integer g from $[N^{1/2}, N]$ which must meet the requirements that $g \neq p$ and $g \neq q$; then arbitrarily selects a prime number Q which is greater than N, and transfers the system information (g, N, Q) to the dealers in plaintext. The dealer posts the information on the billboard.

Each participant P_i randomly selects an integer S_i from $[1, N]$ as its sub-key, and calculates $Y_i = g^{S_i} \bmod N$. P_i will keep P_i confidentially, but send its number P_i and Y_i to the dealers in plaintext.

The dealers determine whether $Y_i = Y_j$ but $P_i \neq P_j$, if it exists, must inform P_i and P_j of reselecting S_i and calculating, sending a new Y_i.The purpose of this step is to avoid different participants using the same sub-key. After confirming there is no same Y_i, the dealers will publish all participants' (P_i, Y_i) on the bulletin board.

The center randomly selects n positive integers s_0', s_0' ,...s_n' from $[2, n]$ which are relatively prime with $p - 1$ and $q - 1$. Then, it calculates $Y_i' = g^{S_i'} \bmod N$ ($i = 1, 2,...n$), and checks whether $Y_i' = Y_i$, if it exists, reselects s_i'. Next, it finds the smallest positive integer h_i satisfying $s_i' \times h_i = 1 \bmod \phi(N)$, Where $\phi(N)$ is the Euler function. Finally, it sends (s_i', h_i) to D_i secretly and leaves the network.

3.2 Secret Distribution phase

In secret distribution phase, the dealers calculate and publish the information so that participants in the n participants can recover the secret. This stage is done by the dealers alone. The procedure is as follows:

Step 1. Each dealer calculates $Y_i' = g^{S_i'} \bmod N$.

Step 2. Each dealer D_j constructs a polynomial $f_j(x) = \sum_{v=1}^{n} a^i{}_j x^j \bmod Q$, where $a^i{}_j \in Z_Q$ and $a_j^{t-1} \neq 0$, and $a^0{}_j$ is secret.

Step 3. Each dealer D_j calculates and publishes the following information: $(Y_j', h_j, f_j(P_i) \oplus Y_i^{S_i'} \bmod N)$ where $i = 1, ..., n$.

3.3 Secret Recovery Phase

In the secret recovery phase, at least t participants in set P can use their own sub-key and information on the bulletin board to recover the secret. In recovery process, each participant is required not to provide their own sub-key, but to provide the shadow which is calculated from its own sub-key and the information on the bulletin board. Without loss of generality, we select t participants' set $P' = (P_1, ... P_t)$ from P as an example to illustrate the reconstruction process. Secret reconstruction process is as follows:

Step 1. Each participant P_i in P' downloads (Y_j', h_j) ($j = 1, 2, ...n$) and N from bulletin boards.

Step 2. Each participant P_i in P' calculates the shadow $Y_j'' = Y_j'^{S_i'} \bmod N$ ($j = 1, 2, ...n$) by its own sub-key S_i, and sends the results to a designated secret recuperator (SR) P_j.

Step 3. SR P_j first verifies the honest of P_i, that is, $(Y_j'')^{h_i} = Y_i'$. If established, it means there is no cheating; otherwise, P_i does not give his honest shadow, or there is an error

during messages transmission. Then P_j sends a complaint message to P_i, and requests retransmission until validated or other error handling.

Step 4. SR P_j downloads information $f_j(P_i) \oplus Y_i^{S_j'} \bmod N$ from the bulletin board, where $j = 1, 2, ...n$ and $i = 1, 2, ...t$, and calculates $f_j(P_i) \oplus Y_i^{S_j'} \oplus Y_i'^{S_i} \bmod N$. Then, SR can get $n \times t$ points $((p_1, f_1(p_1)), ((p_2, f_1(p_2)), ...,((p_t, f_1(p_t)))$; $((p_1, f_2(p_1)), ((p_2, f_2(p_2)), ...,((p_t, f_2(p_t)))$;..., $((p_1, f_n(p_1)), ((p_2, f_n(p_2)), ...,((p_t, f_n(p_t)))$ afterwards, reconstructs polynomial, expressed as:

$$f(x) = \sum_{j=1}^{n} \sum_{i=1}^{t-1} f_j(p_i) \prod_{j=1, j\neq 1}^{t} \frac{x - p_j}{p_i - p_j} = \sum_{j=1}^{n} \sum_{i=0}^{n} a^i{}_j x^i \bmod Q$$

Step 5. SR recovers secret: $f(0) = a_1{}^0 + a_2{}^0 + ... + a_n{}^0$.

4. Security analysis

1. Assume $t-1$ participants attempt to recover the secret.

By the secret reconstruction algorithm, we can see this scheme is consistent with threshold scheme's basic requirements: t or more than t participants can combine to calculate t different points on polynomial $f_i(x)$, thereby recover $f_i(x)$ by Lagrange interpolation theorems, and then get the secret by calculating $\sum_{i=0}^{n} f_i(0)$. $t-1$ participants have only $t-1$ points on the polynomial $f_i(x)$.This $t-1$ points can be regarded as $t-1$ compatible formulas in t linear equations. But the number of constraint equations is smaller than the number of unknowns, which can't determine the polynomial, therefore, $t-1$ participants can't get the secret.

2. An attacker tries to recovery $Y_i'^{S_j} \bmod N$ through Y_i'.

Assume the RSA cryptosystem is secure. If the attacker can get $Y_i'^{S_j} \bmod N$ and know $g^{S_i'} \bmod N$, he must decrypt RSA cryptosystem. Because $Y_i'^{S_j} = (g^{S_i'}) \bmod N$, in which $g^{S_i'} \bmod N$ is the ciphertext, S_j is the private key, $Y_i'^{S_j}$ is plaintext, this indicates that the attacker has the ability to get plaintext through ciphertext in RSA cryptography, which contradicts with the assumption.

3. An attacker tries to disclosure the participant's secret share s_i from the known information.

Assume an attacker can get s_i through Y_i, it means the attacker has the ability to resolve the discrete logarithm problem, but through amount of research for decades, there has not found efficient solutions to solve discrete logarithm. So the assumption does not hold.

4. The dealer D tries to deceive participants by distributing a fake h_i.

Any fake share h_i cannot be verified by calculating $(Y_i')^{h_i} = g$, because the dealer has published the authentication information (Y_i', h_i) on the bulletin board. So the dealer cannot deceive participants by distributing fake shares.

5. A dishonest participant P_l attempts to publish a fake shadow Y_l' to deceive the other participants.

The dishonest participants P_l must modify the information Y_l on the bulletin board before publishing a false shadow Y_l'. Because the shadow Y_l' should pass the verification by other participants. But only the dealer can modify or update the content on the bulletin board, others have the permission to read or download, that is, the dishonest participant cannot modify Y_l on the bulletin board. So a dishonest participant cannot deceive the other participants by releasing a fake shadow Y_l'.

6. A dishonest participant P_j attempts to deceive the dealer D by releasing false information Y_j.

As the dealer has published the test information (P_j, Y_j) on the bulletin board, the secret polynomial $f(x)$ cannot be changed in distribution phase, that is, the fake information Y_j published by dishonest participant has been used. At this time, if the dishonest participant uses the other Y_j^*, he cannot be verified by other participants. So participants cannot deceive the dealer.

7. When we share a number of secrets, participants can reuse their sub-key, which does not affect the system security

In order to share different secrets, the dealers can construct a new polynomial $f_i(x)$ through the information of participants in secret distribution phase. We know only the dealers and legitimate participants can calculate the secret shares from the security of the DH secret security agreement.

5. Conclusion

This paper proposes a threshold secret sharing scheme with multi-dealer based on Deffie-Hellman key agreement protocol. In this program, the participants' sub-keys are determined not by the dealer, but by the number which they own choose. Even the dealers cannot obtain the sub-key of each participant; multiple dealers can commonly maintain the shared secret, which can be dynamically renewed by any dealer. In secret reconstruction process, anyone can immediately test whether participants are cheating. This program can share a number of secrets without modifying the participant's sub-key. Analysis shows that the proposed secret sharing scheme has higher safety and effectiveness, and can better meet the application requirements.

6. Acknowledgment

The authors would like to express their gratitude to all

persons who have provided invaluable guidance and helpful comments and discussions.

References

[1] Shamir, A. (1979). How to share a secrets, *Communications of the ACM*, 22 (11) 612- 613, November.

[2] Blakley, G. R. (1979). Safeguarding cryptographic keys, *In*: Proceedings of National Computer Conference, 48, 313-317, June.

[3] Deng, H., Agrawal, D. P. (2004). Threshold and identity-based security scheme for wireless ad hoc networks, *Ad Hoc Networks*, 2, 291–307.

[4] Zhou, L., Haas, Z. J. (1999). Securing ad hoc networks, *IEEE Network*, 13 (6) 24–30.

[5] Guo, C. Mingchu Li. (2009). A new secret sharing scheme based on the multi-dealer, *Transactions on Fundamentals*, E92-A (5) 1373-1378.

[6] Hwang, R-J, Chang, C-C. (1998). An on-line sharing scheme for multi-secrets, *Computer Communications*, 21, 3, 1170-1176.

[7] Bellare, M., Miner, S. K. (1999). A Forward-Secure Digital Signature Scheme, Advances in Cryptology, Springer-Verlag.

[8] Tan, K. J, Zhu, H. W., Gu, S. J. (1999). Cheaters identification in (t, n) threshold scheme, *Computer Communications*, (22) 762-765.

[9] LIU Mulan, ZHOU Zhanfei, CHEN Xiaoming. (2000). Secret sharing system, *Scientific Aviso*, 45 (9) 897-907.

[10] PANG Liaojun, LI Huixian, WANG Yumin. (2006). A secure and efficient secret sharing scheme with general access structures, FSKD 2006, LNAI 4223, p. 646-649.

[11] Wu, T. C, Wu, T. S. (1995). Cheating Detection and Cheater Identification inSecret Sharing Scheme. *Computer Digit Technology*, 142 (5) 367-369.

[12] Chor, B., Goldwasser, S. (1985). Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults, *In*: Proceedings of the 26th *IEEE Symposium on Foundations of Computer Science*, p.383-395.