A Dynamic Secret Sharing Scheme Based on Factorization

Dan Wang
College of Information Engineering
Taishan Medical University, Tai'an 271016, China

Yufei Zhang
College of Information Engineering
Taishan Medical University, Tai'an 271016, China

Abstract

A dynamic (*t, n*)-threshold secret sharing scheme based on factorization is proposed in this paper. It has following properties: (1) the dealer can renew the secret key of the system without renewing the shadows of the participants; (2) when some participants' shadows are revealed, they can be renewed without any effect on the others; (3) a new shadow can be generated for a new participant without any effect on others; (4) the shadows can be reused for many times; (5) the secret key of the system can be recovered in a parallel process.

Keywords: Factorization, Secret sharing scheme, Cryptography, Data safety

1. Introduction

In the modern society, with the popularization of the computer system, the secret communication becomes more and more important. To realize the safety of information, the secret keys are mainly used to encrypt information, and when the cryptographic technology is used to protect information, the core protection is the protection of secret keys, not the protection of the algorithm or the hardware (Wang, 1989), so it is very important to effectively manage the secrete keys in the cryptography. In 1979, Shamir (Shamir, A. 1979, P.612-613) and Backly (Backly, 1979, P.313-317) respectively put forward the concept of secret key decentralized management, and the mechanism to realize this idea was called as the (*t*, *n*)-threshold scheme. In this scheme, one secret key (system secret key) is divided into n parts (*n* shadows) respectively kept by *n* persons, to make the certain integer *t* (*t*<*n*) satisfy: (1) in *n* persons, any *r* ($r \geq t$) persons could recover the system secret key by the cooperation; (2) it is not helpful to recover the system secret key by *r* ($r < t$) persons through the cooperation. This idea makes the secret key management more safe and flexible. At present, except for the secret key management, this idea could also be applied in many aspects of the cryptography such as the group signature and the group authentication.

After the (*t*, *n*)-threshold idea was proposed, many scholars studied this idea, and put forward many schemes (Shamir, 1979, P.612-613 & Backly, 1979, P.313-317 & Liu, 1999, P.612-613 & Harn, 1995, P.262-263 & R. G. E. Piuch, 1999, P.81-84 & Tan, 1999, P.81-84) to realized it. But the early (*t*, *n*)-threshold schemes all had following deficiencies, (1) when the system secret key needs to be renewed (for example, the original secret key has been recovered or the secret key needs to be exchanged because of certain cause), the dealer must redistribute the shadows for each participant (even if these shadows may not be used ever), i.e. each shadow only be used once at most; (2) when the shadow of certain one participant is revealed, the dealer could not redistribute the shadow for this participant without any effect on other participants' shadows; (3) when new participant joins, the dealer must redistribute shadows to each participant. To overcome above disadvantages, scholars proposed many (*t*, *n*)-threshold schemes which could repeatedly use the shadows (Liu, 1999, P.612-613 & Harn, 1995, P.262-263), but these shadows could only save or recover the secret keys in the key set predefined by the dealer, and to save one new secret key (the secret key out of the key set), the dealer must renew the shadows of each participant.

When *t*=*n*, the (*n*, *n*)-threshold scheme which could use the shadow unlimitedly was proposed (R. G. E. Piuch, 1999, P.81-84 & Tan, 1999, P.81-84), but to recover the system secret key, all participants must recover the system secret key according to a compulsory sequence (i.e. a series process) $m_1, m_2, \cdots, m_n$, which needed large time expenditure.

Aiming at above deficiencies, many solutions have been proposed (Liu, 2002, P.1009-1012 & Liu, 2002, P.276-279). Here, a dynamic (*t, n*)-threshold secret key sharing scheme based on factorization is proposed in this paper. It has following properties: (1) the shadows can be used repeatedly without limitation; (2) the dealer can renew the secret key of the system without renewing the shadows of the participants when the shadow of certain participant is revealed; (3) when some participants' shadows are revealed, they can be renewed without any effect on the others; (4) the dealer could confirm the cheaters; (5) the dealer could add or delete one participant conveniently; (6) the secret key of the system can be recovered in a parallel process.

In addition, the scheme in this article only needs one multiplying operation to each user in the system initialization and the secret key recovering process, i.e. $n_i = p_i q_i$, and the power operation only is needed when confirming the cheaters, i.e. $v_i = \alpha^{x_i}$, but in Liu's article (Liu, 2002, P.276-279), the power operations ($x_i = \alpha^{s_i}, v_i = \alpha^{x_i}$) should be implemented in two stages, so from the running speed, the scheme in this article is obviously better than the scheme proposed in Liu's article.

2. New scheme

Supposing that *GF*(*P*) is the finite field, and $P_1, P_2, \cdots, P_n$ are *n* participants in the system.

2.1 System initialization

(1) The system randomly selects different prime pairs p_i, q_i ($i = 1,2,\cdots n$), and $(n_i = p_i q_i) \neq (n_j = p_j q_j)$ $(i \neq j)$, and then p_i, q_i are secretly transferred to P_i($i = 1,2,\cdots n$) by the safety channel. For the safety, the prime numbers p_i, q_i should be binary numbers with 1024 bits at least.

(2) The system randomly selects one element $\alpha \in GF(P)$, one $(t-1)$-order polynomial $h(x)$ to satisfy $h(0) = K$, and K is the secret key of the system which should be saved, then computes

$$y_i = h(\alpha + n_i)$$

(3) The system opens α and the ordered array $(y_1, y_2, \cdots y_n)$ on the bulletin board.

2.2 Secret key recover

When any *t* shadow holders ($P_1, P_2, \cdots, P_t$) want to recover the secret keys of the system, each participant only needs check α and y_i on the bulletin board, and computes $x_i = \alpha + n_i$, and submits x_i (x_i is called as the screening shadow of P_i, and correspondingly, p_i, q_i is called as the secret shadow pair of P_i). For $(x_i, y_i), i = 1,2,\cdots,n$, use the Lagrange interpolation formula

$$h(x) = \sum_{i=1}^{t} y_i \prod_{1 \le j \le t,\, j \neq i} \frac{x - x_j}{x_i - x_j}$$

, to confirm $h(x)$, and then recover the secret key of the system, $K = h(0)$.

3. Analysis of properties

(1) Feasibility

From $x_i = \alpha + n_i$ and $y_i = h(\alpha + n_i)$, (x_i, y_i) is one point on $h(x)$. And because α is the original element and $n_i \neq n_j (i \neq j)$, so $x_i \neq x_j (i \neq j)$. So when recovering the secret key, *t* participants ($P_1, P_2, \cdots, P_t$) could give *t* different points ((x_i, y_i) $(i = 1,2,\cdots t)$) on $h(x)$, and $h(x)$ is $(t-1)$-order polynomial, so these *t* points can be confirmed, so the secret key of the system $K = h(0)$ could be recovered. The above scheme is feasible.

(2) Safety

The safety of this scheme is based on the characteristic that the factorization could not be inverted. First, when recovering the secret key, for each participant, $x_i = \alpha + n_i$, and because of the non-reversibility of factorization, other participants could not recover the shadow pair p_i, q_i of P_i through α and x_i, i.e. each participant's shadow has not been opened because of the recover of the secret key of the system, and they can continue to be used. Second, according to the non-reversibility of factorization, any participant could not obtain other participants' shadows and screening shadows by the opening information α and the ordered array $(y_1, y_2, \cdots y_n)$.

(3) System renewing

(a) The secret key of system *K* has not been recovered, and because of certain cause, the secret key of system needs to be replaced. Here, the dealer only needs to reselect one $(t-1)$-order polynomial $h'(x)$ to satisfy $h'(0) = K'$ which is the new secret key of system, and then the new $h'(x)$ could be used to renew the ordered array $(y_1, y_2, \cdots y_n)$ on the bulletin board.

(b) The secret key of system *K* has been recovered, and the new secret key of system K' needs to be saved. Here, the dealer would select one new original element α' ($\alpha' \neq \alpha$) and $(t-1)$-order polynomial $h'(x)$ to satisfy $h'(0) = K'$ which is the new secret key of system, and then α' and $h'(x)$ are used to renew the ordered array $(y_1, y_2, \cdots y_n)$ on the bulletin board.

Because α is the any element in $GF(P)$, so each participant's shadow could be used many times without limitation.

(4) Confirming cheaters

This scheme could be easily modified as a dynamic (t, n)-threshold scheme. Here, the deal only needs opening the checking information to each participant P_i, $v_i = \alpha^{x_i}$, where $x_i = \alpha + n_i$. When recovering the secret key, other participants could confirm whether the participant P_i is the cheater by the checking equation $v_i = \alpha^{x_i}$ (x_i is the screening shadow of P_i). According to the non-reversibility of factorization and discrete logarithm, any participant could not obtain the shadow and screening shadow of the participant P_i by the information α, y_i opened by the system.

(5) Adding or deleting participant

(a) When new participant joins, the dealer only needs randomly generating the shadow pair (p_{n+1}, q_{n+1}) for the new participant P_{n+1}, and adds one element y_{n+1} in the ordered array $(y_1, y_2, \cdots y_n)$ on the bulletin board, and $y_{n+1} = h(\alpha + n_{i+1})$;

(b) When deleting certain one participant P_i, the dealer only needs reselecting one $(t-1)$-threshold polynomial $h'(x)$ to satisfy $h'(0) = K$ which is the secret key of system, and then the $(t-1)$-threshold polynomial $h'(x)$ is used to renew the ordered array $(y_1, y_2, \cdots y_n)$ on the bulletin board, and here, y_i needs not be computed (y_i could be the original value or the item of y_i is empty), so the original shadow pair (p_i, q_i) of P_i is invalid.

(6) Renewing individual secret keys

When the shadow of certain one participant P_i is revealed, the dealer only needs redistribute the shadow (p_i', q_i') for the new participant, and then one $(t-1)$-threshold polynomial $h'(x)$ is selected to satisfy $h'(0) = K$, and new p_i, q_i and $h'(x)$ are used to renew the ordered array $(y_1, y_2, \cdots y_n)$ on the bulletin board, and other participants' shadows need not be changed.

4. Conclusions

The secret sharing problem is studied in this article, and one dynamic secret sharing scheme is proposed based on the factorization.

The research result indicates that the scheme has higher running speed in the system initialization and secret key recovering process. In addition, for the safety, this scheme could better defend participant cheating, but how to prevent the managers' cheating has not been studied in this article, which should be the research direction in the future.

References

Backly, G.R. (1979). Safeguarding cryptographic keys. *In proceedings of the National Computer Conference of AFIPS.* P.313-317.

Harn, L. (1995). Comment: multistage secret sharing based on one-way function. *Electronics Letters.* No. 31(4). P.262-263.

Liu, Huanping, Hu, Mingzeng & Fang, Zhenxing et al. (2002). A Dynamic Secret Sharing Scheme Based on One-Way Function. *Journal of Software.* No. 13(5). P.1009-1012.

Liu, Huanping, Ji, Zhenzhou & Hu, Mingzeng et al. (2002). A Dynamic (k, n)-threshold Secret Sharing Scheme Based on Discrete Logarithm. *Journal of Electronics & Information Technology.* No. 24(2). P.276-279.

Liu, Huanping & Yang, Yixian. (1998). Generalized (*k, n*)-Threshold Scheme. *Journal on Communications.* No. 20(8). P.72-75.

Liu, Huanping, Yang, Yixian & Yang, Fangchun. (1999). A Multiple-Secret-Key Sharing Scheme Based on One-way Function. *Journal of Electronics (China).* No. 21(4). P.612-613.

R. G. E. Piuch. (1999). Online multiple secret sharing. *Electron Letters.* No. 20(7). P.81-84.

Shamir, A. (1979). How to share a secret. *Communications of the ACM.* No. 22(11). P.612-613.

Tan, Kaijun & Zhu, Hongwen. (1999). The Dynamic Private Key Sharing Mechanism Based on the One-way Function. *Journal on Communications.* No. 20(7). P.81-84.

Wang, Yumin & Liu, Jianwei. (1989). *Theory and Technology: the Safety of the Communication Network.* Chengdu: Southwest Jiaotong University Press.