一种秘密共享新个体加入协议*

董 攀+, 况晓辉, 卢锡城

(国防科学技术大学 计算机学院,湖南 长沙 410073)

A Non-Interactive Protocol for Member Expansion in a Secret Sharing Scheme

DONG Pan+, KUANG Xiao-Hui, LU Xi-Cheng

(College of Computer Science, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: Phn: +86-731-4573696, E-mail: broadsky@163.com

Received 2003-07-09; Accepted 2003-11-10

Dong P, Kuang XH, Lu XC. A non-interactive protocol for member expansion in a secret sharing scheme. *Journal of Software*, 2005,16(1):116−120. http://www.jos.org.cn/1000-9825/16/116.htm

Abstract: This paper presents a new secret redistribution protocol for threshold sharing schemes that create n shares of the secret for n shareholders. Without having a trusted center, the protocol only requires t (t is the threshold) participants' cooperation and $6t$ times broadcasting to generate and to distribute the new share. At the end, it is demonstrated that the algorithm has a higher security and is better than the Shuffling scheme and Wong's protocol on reliability and secret management.

Key words: secret sharing; new member; trusted center

摘 要: 针对秘密共享方案提出了一种为新个体分配秘密份额的算法.该算法具有无需信任中心、无需改动原有秘密份额、仅需 t 个成员合作(t 为门限)、$6t$ 次广播等优点.最后还证明了该算法具有高安全性,并且在可靠性和密钥管理方面优于 Shuffling 方案和 Wong TM 等人的算法.

关键词: 秘密共享;新个体;信任中心

中图法分类号: TP309 **文献标识码**: A

1 Introduction

Secret sharing system[1] is widely applied in network security. A secret sharing scheme (t,n) is called a threshold scheme if it has following characters: (1) there are n participants in total; (2) any $t(2 \le t \le n)$ or more participants are able to rebuild the key S; (3) any less than $t-1$ participants can't get S. Threshold scheme is

* Supported by the National Natural Science Foundation of China under Grant No.69933030 (国家自然科学基金)

DONG Pan was born in 1978. He a Ph.D. candidate at School of Computer Science, National University of Defense Technology. His current research interests include information security, network security and cryptography. **KUANG Xiao-Hui** was born in 1975. He is a Ph.D. candidate at School of Computer Science, National University of Defense Technology China. His current research interests include computer network, wireless network and information security etc. **LU Xi-Cheng** was born in 1946. He is a professor and doctoral supervisor at School of Computer Science, National University of Defense Technology. His research areas are computer network and super computing, etc.

the most common case in use. A secret sharing system can protect the secret against being lost, destroyed and modified. So it enhances the safeguarding of the secret and secure distributed computation to some extent. In reality, the set of shareholders often updates. Frequent refreshment or redistribution of S between different (possibly disjoint) sets of shareholders and different access structures will bring difficulty to the secret management and lead to a higher computation and communication cost. Reference [2] proposed a shuffling protocol which needs only t members' cooperation to securely distribute shares for new participants. However, the shuffling scheme must commit t^2-1 secret communications. Wong[3] presented a non-interactive protocol with t^2 scale communications. In a wireless network environment, more communications will bring longer time and lower success rate to the generation of new shares, and more difficulty to the key management. This paper proposes a new secret share generation protocol, which satisfies security demand and needs only $6t$ broadcast communications. Like the shuffling scheme or Wong's protocol, no trusted center is required here.

2 Shamir's Secret Sharing Scheme

Among current secret sharing schemes, Shamir scheme[4], proposed in 1979 and based on Lagrange interpolation, is the most efficient and convenient one. It is a (t,n) threshold scheme and can be interpreted as follows:

Select a finite field $GF(q)$, where q is a big enough prime number, and randomly select $a_1,a_2,\ldots,a_{t-1}\in GF(q)$, then we can construct a polynomial

$$f(x)=S+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1}$$

where S is the secret.

Suppose there are n members: $P_1,P_2,\ldots,P_n$. Secret shares $s_i=f(i)$ shall be secretly distributed to P_i. When that is done and t (or more) shareholders want to reconstruct S, let these shareholders be $P_{i1},P_{i2},\ldots,P_{it}$. According to Lagrange interpolation formula, $f(x)$ can be computed by

$$f(x)=\sum_{j=1}^{t}\left\{f(i_j)\prod_{h\neq j}\frac{(x-i_h)}{(i_j-i_h)}\right\}.$$

Let $\omega_j(x)=\prod_{h\neq j}\frac{(x-i_h)}{(i_j-i_h)}$, so $S=f(0)=\sum_{j=1}^{t}s_{i_j}\omega_j(0)$.

At the same time, if the set of shareholders contains less than $t-1$ members, they can't get any useful information of S.

Our protocol will realize the secure generation and distribution of a new secret share for Shamir's secret sharing scheme, and meanwhile expand the group members. The idea partly derives from Refs.[5,6].

3 Expansion Algorithm

3.1 Security requirement

Some goals must be reached in the new share's distribution protocol for security:

a) Any information about S can't be exposed;

b) None but its legal holder can get the new share;

c) The shares of old members are secure.

3.2 Some essential terms

Suppose that all participants have broadcast channels, and ElGamal cryptography[7] is used for secret communication.

$GF(q)$ is the given finite field, g is its generator, and (g,g^d) is the public key, where d is the secret key. M is the message for sending.

Encryption: Select an integer number l randomly, then compute (g^l,Mg^{dl}) as the cipher text;

Decryption: Computer $g^{dl}=(g^d)^l$ and its inverse g^{-dl}, so we can get the message $M=Mg^{dl}g^{-dl}$.

3.3 New share's generation and distribution

Let the new member be P_{n+1}, whose ElGamal encryption secret key and public key are d_{n+1} and g^{dn+1} respectively. Group secret key is S, and group public key is g^S.

3.3.1 New share's generation

Here we need t old members (let them be $P_1,P_2,\ldots,P_t$) to generate the new secret share s_{n+1}. Group public key is g^S. P_i holds the secret share s_i. The lagrange polynomial is $f(x)$.

Generation steps:

Step 1 select two random integers e_i and l_i, and encrypt $s_i\omega_i(n+1)$ by e_i:

$K_i^0=s_i\omega_i(n+1)e_i$, broadcast K_i^0 and g^{l_i}

(t broadcasts with $2t$ data)

Step 2 for j=1 to t do

for i=1 to t do

if ($j\neq i$) do

compute $K_i^j=K_i^{j-1}g^{(S+d_{n+1})l_j}$

else $K_i^j=K_i^{j-1}$

end for i

broadcast K_i^j, $i=1,2,...,t$

end for i

$M_i=K_i^t$

(t broadcasts with $t(t-1)$ data)

Step 3 for j=1 to t do

for i=1 to t do

if ($j\neq i$) do

compute $W_i^j=M_ig^{(S+d_{n+1})l_j}$

else $W_i^j=0$

end for i

broadcast W_i^j, $i=1,2,...,t$

end for j

(t broadcasts with $t(t-1)$ data)

Step 4 for i:=1 to t do

compute $W_i^e=\sum_{j=1}^{t}W_i^j$, then decrypt W_i^e and M_i to get

$$W_i=s_i\omega_i(n+1)g^{(S+d_{n+1})\left(\sum_{j=1}^{t}l_j-l_i\right)}\sum_{j=1,j\neq i}^{t}g^{(S+d_{n+1})l_j}$$

$$Q_i=s_i\omega_i(n+1)g^{(S+d_{n+1})\left(\sum_{j=1}^{t}l_j-l_i\right)}$$

broadcast W_i, Q_i

end for i

compute $A=\sum_{i=1}^{t}Q_i$

(t broadcasts with $2t$ data)

Step 5 for i:=1 to t do

compute and broadcasts $Ag^{(S+d_{n+1})l_i}$

end for i

compute $B=\sum_{i=1}^{t}Ag^{(S+d_{n+1})l_i}-\sum_{i=1}^{t}W_i$

(t broadcasts with t data)

Step 6 $P_1,P_2,...,P_t$ cooperate to decrypt B, and get $C=\sum_{i=1}^{t}s_i\omega_i(n+1)g^{d_{n+1}\sum_{j=1}^{t}l_j}$

(t times broadcasts with t data)

(totally $6t$ broadcasts with $2t(t+2)\ q$ Bit length data)

3.3.2 New share's distribution

P_{n+1} gets $C=\sum_{i=1}^{t}s_i\omega_i(n+1)g^{d_{n+1}\sum_{j=1}^{t}l_j}=f(n+1)g^{d_{n+1}\sum_{j=1}^{t}l_j}$. By $g^{\sum_{j=1}^{t}l_j}$, he can decrypt to get $s_{n+1}=f(n+1)$.

4 New Share's Validity Proof

From Step 4, one can easily see:

$$A=Q_i+\sum_{j=1,j\neq i}^{t}Q_j$$

In Step 5:

$$\begin{aligned}B&=\sum_{i=1}^{t}\left(Q_i+\sum_{j=1,j\neq i}^{t}Q_j\right)g^{(S+d_{n+1})l_i}-\sum_{i=1}^{t}W_i\\&=\sum_{i=1}^{t}s_i\omega_i(n+1)g^{(S+d_{n+1})\left(\sum_{j=1}^{t}l_j-l_i\right)}g^{(S+d_{n+1})l_i}+\sum_{i=1}^{t}\left(\sum_{j=1,j\neq i}^{t}Q_j\right)g^{(S+d_{n+1})l_i}-\sum_{i=1}^{t}W_i\\&=\sum_{i=1}^{t}s_i\omega_i(n+1)g^{(S+d_{n+1})\sum_{j=1}^{t}l_j}+\sum_{j=1,i=1,i\neq j}^{t}\sum^{t}Q_jg^{(S+d_{n+1})l_i}-\sum_{i=1}^{t}W_i\\&=\sum_{i=1}^{t}s_i\omega_i(n+1)g^{(S+d_{n+1})\sum_{j=1}^{t}l_j}+\sum_{j=1}^{t}W_j-\sum_{i=1}^{t}W_i\\&=\sum_{i=1}^{t}s_i\omega_i(n+1)g^{(S+d_{n+1})\sum_{j=1}^{t}l_j}\end{aligned}$$

.

5 Performance Discussion

From the procedure of the new share distribution, one can see that all the results of every step are sent by the broadcasting, while all the data for keeping secret are managed by the generators. So the group key management is simple. Furthermore, our protocol does not need the trusted center and only commits $6t$ broadcasts. In the case of wireless network, especially MANET (the reliability of links is very low), fewer communications lead to a higher probability of success distribution. In the Refs.[2,3], both protocols for new share's distribution need t^2 secret communications, so given a big threshold t, our protocol will perform better in reliability, usability and key

management.

6 Security Discussion

Our algorithm for the new secret share is based on the Shamir secret sharing scheme, so its security depends on Shamir scheme's one. In our protocol, security of the group key S is guaranteed by ElGamal cryptosystem, so every single member can't get S. When computing M_i, we actually perform encryption for s_i three times: its holder's encryption, P_{n+1}'s encryption and group's encryption. In the process of synthesis to the new share, the computation of $s_i\omega_i(n+1)$ is nonlinear, so nobody can acquire any useful information of s_i. The result of every step is encrypted by group key, so P_{n+1} can't get s_i. At last, B, generated by the $P_1,P_2,...,P_t$, is the s_{n+1}'s encryption by P_{n+1}'s secret key, so $P_1,P_2,...,P_t$ can't get s_{n+1}. In sum, the present protocol has a higher security.

Reference:

[1] Desmedt Y. Some recent research aspects of threshold cryptography. In: Okamoto R, Davida G, Mambo M, eds. Information Security. LNCS 1396. Berlin: Springer-Verlag, 1997. 158−173.

[2] Luo H, Lu S. Ubiquitous and robust authentication services for Ad Hoc wireless networks. Technical Report, TR-200030, Department of Computer Science, UCLA, 2000.

[3] Wong TM, Wang CX, Wing JM. Verifiable secret redistribution for archive systems. In: Proc. of the 1st Int'l Security in Storage Workshop. 2002.

[4] Shamir S. How to share a secret. Communications of the ACM, 1979,22(11):612−613.

[5] Pedersen TP. A threshold cryptosystem without a trusted party. In: Proc. of the Eurocrpt 1991. LNCS 547. Berlin: Springer-Verlag, 1991. 522−526.

[6] Takaragi K, Miyazaki K. A threshold digital signature issuing scheme without secret communication. In: Proc. of the IEEE Conf. 1998.

[7] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on IT, 1985,31(4):469–472.

****