

# 一个可验证的秘密共享新个体加入协议

李慧贤<sup>1,2</sup>, 程春田<sup>2</sup>, 庞辽军<sup>3</sup>

(1. 大连理工大学计算机科学与工程系, 116024, 大连; 2. 大连理工大学水利工程信息研究所, 116024, 大连;  
3. 西安电子科技大学综合业务网国家重点实验室, 710071, 西安)

**摘要:** 针对门限秘密共享方案, 提出了一个可验证的新个体加入协议. 应用指数运算来验证新产生份额的真实性, 从而预防系统中可能出现的主动攻击. 该协议具有无需信任中心, 无需改动原有参与者的份额, 仅需  $t$  ( $t$  为门限) 个老成员合作产生新份额, 仅需  $6t$  次广播等优点. 分析与验证表明, 该协议是正确的, 与现有协议相比, 其密钥管理简单, 安全性更高, 具有良好的可靠性和可用性.

**关键词:** 秘密共享; 新个体; 验证; 信任中心

中图分类号: TN98.4 文献标识码: A 文章编号: 0253-987X(2006)02-0207-04

## Verifiable Protocol for Member Expansion in Secret Sharing Schemes

Li Huixian<sup>1,2</sup>, Cheng Chuntian<sup>2</sup>, Pang Liaojun<sup>3</sup>

(1. Department of Computer Science and Engineering, Dalian University of Technology, Dalian 116024, China;  
2. Institute of Hydroinformatics, Dalian University of Technology, Dalian 116024, China; 3. National Key Lab of Integrated Service Networks, Xidian University, Xi'an 710071, China)

**Abstract:** A verifiable protocol for member expansion in the threshold sharing schemes that create  $n$  shares of the secret for  $n$  participants was proposed. The authenticity of the new share can be verified by using exponential computation, which makes the protocol defend against active adversaries. Without a trusted center and modifying the shares of old participants, the protocol needs that  $t$  ( $t$  is the threshold) old participants cooperate to generate and to distribute the new share, and there are only  $6t$  times broadcasting. The validity of the proposed protocol was verified. Compared with the existing protocols, the proposed protocol has a higher security and is easier in key management and better in reliability and usability.

**Keywords:** secret sharing; new member; verify; trusted center

秘密共享是在一组参与者(或成员)中共享秘密的技术, 它主要用于保护重要信息, 以防止信息丢失、被破坏、被篡改等. Shamir<sup>[1]</sup>和Blakley<sup>[2]</sup>最早提出秘密共享的概念, 并分别给出一个  $(t, n)$  门限秘密共享方案. 门限方案是最普遍应用的方案<sup>[3,4]</sup>, 在实际使用中, 参与者的集合可能会经常变动, 为保证安全性, 需要重新分发秘密来更新各参与者的份额, 这不仅给秘密管理带来困难, 而且增加了系统的计算和通讯代价. 考虑参与者集合变动问题, Luo 等人<sup>[5]</sup>和 Wong 等人<sup>[6]</sup>分别提出了一个 Shuffling 协议和

一个非交互式的协议, 这两个协议都需进行  $t^2$  规模的秘密通讯. Dong 等人<sup>[7]</sup>指出, 通讯规模越大, 将使数据传输时间越长, 新份额产生的成功率越低, 密钥管理越困难, 并提出了一个新个体加入协议. 该协议需要  $6t$  次广播通讯, 明显减少了通讯次数, 但存在安全漏洞——不能防御主动攻击<sup>[8]</sup>. 基于上述分析, 本文提出了一个可验证的秘密共享新个体加入协议, 在不改变老成员份额的前提下, 为新加入的成员安全地产生份额, 并允许新成员验证新份额的真实性.

## 1 初始秘密分发过程

针对 Shamir 的门限方案中的新成员加入问题, 本文提出了一个可验证的新个体加入协议, 该协议不需要重新执行秘密分发过程, 即可为新加入的成员安全地分配份额, 实现组成员的扩展. 需要说明的是, 实现本文协议需要对 Shamir 门限方案的初始秘密分发过程(即没有任何新成员加入时的秘密分发过程)进行一些扩充, 即公布一些用于验证的信息. 下面介绍初始秘密分发过程.

令  $G_F(q)$  为一个有限域,  $q(q > n)$  是一个足够大的素数,  $g$  为  $G_F(q)$  的生成元, 并使得该有限域上的离散对数计算是非常困难的. 系统中有  $n$  个参与者  $P_1, P_2, \dots, P_n$  共享秘密  $k$ . 选择  $t-1$  个随机系数  $a_1, a_2, \dots, a_{t-1} \in G_F(q)$ , 并以  $k$  为常数项构造一个  $t-1$  阶多项式

$$f(x) = k + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \quad (1)$$

然后, 用  $f(x)$  为每个参与者  $P_i$  产生份额  $s_i = f(i)$  ( $i=1, 2, \dots, n$ ), 其中  $i$  为  $P_i$  的公开身份标识信息, 并将  $s_i$  秘密地发送给  $P_i$ . 最后, 广播  $g^k, g^{a_1}, \dots, g^{a_{t-1}}$  作为验证新份额真实性的证据.

## 2 可验证的新份额产生协议

在初始秘密分发的基础上, 以  $t$  个老成员的份额为输入, 新成员的份额为输出. 这里假设在所有成员之间存在可靠的广播信道.

### 2.1 新份额的产生

令新成员为  $P_{n+1}$ , 他的 ElGamal<sup>[9]</sup> 加密算法的私钥和公钥分别为  $d_{n+1}$  和  $g^{d_{n+1}}$ , 令  $(n+1)$  为  $P_{n+1}$  的公开身份标识信息. 为了产生新成员的份额, 需要  $t$  个老成员合作. 不失一般性, 设他们为  $P_1, P_2, \dots, P_t$ , 并将他们构成的集合称为合作组. 新份额产生的实质就是应用 Lagrange 插值公式计算

$$f(n+1) = \sum_{i=1}^t \left( s_i \prod_{j=1, j \neq i}^t \frac{(n+1)-j}{i-j} \right) \quad (2)$$

为了描述简便, 令  $\omega_i(n+1) = \prod_{j=1, j \neq i}^t \frac{(n+1)-j}{i-j}$ . 新份额的产生过程如下.

(1) For  $P_i = P_1$  to  $P_t$ , 执行以下步骤:

(1-1) 随机选择 2 个整数  $e_i$  和  $l_i$ ;

(1-2) 计算  $K_i^0 = s_i \omega_i(n+1) e_i$ ;

(1-3) 广播  $K_i^0$  和  $g^{l_i}$  ( $i=1, 2, \dots, t$ ).

(2) For  $j=1$  to  $t$ , 执行以下步骤:

(2-1) For  $P_i = P_1$  to  $P_t$ , 执行以下步骤:

(2-1-1) 如果  $j \neq i$ , 计算  $K_i^j = K_i^{j-1} \cdot$

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

(2-1-2) 否则, 令  $K_i^j = K_i^{j-1}$ ;

(2-2) 广播  $K_i^j$ , 其中  $i=1, 2, \dots, t$ , 且  $i \neq j$ .

(3) 令  $M_i = K_i^t$  ( $i=1, 2, \dots, t$ ).

(4) For  $j=1$  to  $t$ , 执行以下步骤:

(4-1) For  $P_i = P_1$  to  $P_t$ , 执行以下步骤:

(4-1-1) 如果  $j \neq i$ , 计算  $\omega_i^j = M_i g^{l_j}$ .

$$g^{d_{n+1} l_j} = M_i g^{(k+d_{n+1}) l_j};$$

(4-1-2) 否则, 令  $W_i^j = 0$ ;

(4-2) 广播  $W_i^j$ , 其中  $i=1, 2, \dots, t$ , 且  $i \neq j$ .

(5) For  $P_i = P_1$  to  $P_t$ , 执行以下步骤:

(5-1) 计算  $W_i^e = \sum_{j=1}^t W_i^j$ ;

(5-2) 计算

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

(5-3) 计算

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

(5-4) 广播  $W_i$  和  $Q_i$ .

(6) 计算  $A = \sum_{i=1}^t Q_i$ .

(7) For  $P_i = P_1$  to  $P_t$ , 计算并广播  $A g^{(k+d_{n+1}) l_i}$ .

(8) 计算  $B = \sum_{i=1}^t A g^{(k+d_{n+1}) l_i} - \sum_{i=1}^t W_i$ .

(9) 由  $P_1, P_2, \dots, P_t$  合作, 即每个  $P_i$  提供信息

$$g^{-k l_i}, \text{ 再利用 } B \text{ 来计算 } C = \sum_{i=1}^t s_i \omega_i(n+1) g^{d_{n+1} \sum_{j=1}^t l_j}.$$

上述新份额产生过程总共进行了  $6t$  次广播, 共广播了  $2t(t+2)$  个数据.

### 2.2 新份额的分配

新成员  $P_{n+1}$  可以得到  $C = \sum_{i=1}^t s_i \omega_i(n+1) g^{d_{n+1} \sum_{j=1}^t l_j} = f(n+1) g^{d_{n+1} \sum_{j=1}^t l_j}$ . 由  $g^{\sum_{j=1}^t l_j}$  和  $P_{n+1}$  计算  $g^{d_{n+1} \sum_{j=1}^t l_j} = (g^{\sum_{j=1}^t l_j})^{d_{n+1}}$  和  $g^{-d_{n+1} \sum_{j=1}^t l_j}$ , 从而能够解密并得到  $s_{n+1} = f(n+1) g^{d_{n+1} \sum_{j=1}^t l_j} g^{-d_{n+1} \sum_{j=1}^t l_j} = f(n+1)$ .

### 2.3 新份额的验证

由公共信息  $g^k, g^{a_1}, g^{a_2}, \dots, g^{a_{t-1}}$ , 新成员  $P_{n+1}$  可以通过下式是否成立来验证份额  $s_{n+1}$  的真实性

$$g^{s_{n+1}} \equiv g^k \prod_{l=1}^{t-1} (g^{a_l})^{(n+1)^l} \quad (3)$$

下面来证明应用式(3)验证的正确性

$$\begin{aligned} g^{s_{n+1}} &= g^{f(n+1)} = g^{(k+a_1(n+1)+a_2(n+1)^2+\dots+a_{t-1}(n+1)^{t-1})} = \\ &= g^k g^{a_1(n+1)} g^{a_2(n+1)^2} \dots g^{a_{t-1}(n+1)^{t-1}} = \\ &= g^k \prod_{l=1}^{t-1} (g^{a_l})^{(n+1)^l} \end{aligned}$$

## 3 分析与讨论

### 3.1 协议的验证

本文提出的协议针对门限秘密共享方案,其中每个参与者  $P_i (1 \leq i \leq n)$  的公开身份标识信息  $i$  和份额  $s_i$  为满足式(1)中多项式  $f(x)$  的一个点  $(i, s_i)$ , 因此验证协议的正确性也就是验证新加入的参与者  $P_{n+1}$  的公开身份标识信息  $n+1$  和新产生的份额  $s_{n+1}$  为满足多项式  $f(x)$  的一个点  $((n+1), s_{n+1})$ . 下面,验证本文协议产生新份额的正确性.

由 2.1 节中的第(6)步,容易得出  $A = Q_i +$

$$\begin{aligned} &\sum_{j=1, j \neq i}^t Q_j, \text{ 因此在第(8)步中, } B \text{ 可以化简为} \\ B &= \sum_{i=1}^t (Q_i + \sum_{j=1, j \neq i}^t Q_j) g^{(k+d_{n+1})l_i} - \sum_{i=1}^t W_i = \\ &= \sum_{i=1}^t s_i \omega_i (n+1) g^{(k+d_{n+1})(\sum_{j=1}^t l_j - l_i)} g^{(k+d_{n+1})l_i} + \\ &= \sum_{i=1}^t (\sum_{j=1, j \neq i}^t Q_j) g^{(k+d_{n+1})l_i} - \sum_{i=1}^t W_i = \\ &= \sum_{i=1}^t s_i \omega_i (n+1) g^{(k+d_{n+1})\sum_{j=1}^t l_j} + \\ &= \sum_{i=1}^t (\sum_{j=1, j \neq i}^t Q_j) g^{(k+d_{n+1})l_i} - \sum_{i=1}^t W_i = \\ &= \sum_{i=1}^t s_i \omega_i (n+1) g^{(k+d_{n+1})\sum_{j=1}^t l_j} + \sum_{j=1}^t W_j - \\ &= \sum_{i=1}^t W_i = \sum_{i=1}^t s_i \omega_i (n+1) g^{(k+d_{n+1})\sum_{j=1}^t l_j} \end{aligned}$$

由  $P_1, \dots, P_t$  合作去解密  $B$ , 即每个  $P_i (i=1, 2, \dots, t)$  广播  $g^{-kl_i}$ . 然后,对  $B$  解密得到

$$\begin{aligned} C &= \sum_{i=1}^t s_i \omega_i (n+1) g^{(k+d_{n+1})\sum_{j=1}^t l_j} g^{\sum_{i=1}^t (-kl_i)} = \\ &= \sum_{i=1}^t s_i \omega_i (n+1) g^{d_{n+1}\sum_{j=1}^t l_j} = f(n+1) g^{d_{n+1}\sum_{j=1}^t l_j} \end{aligned}$$

由  $g^{\sum_{j=1}^t l_j}$ , 新成员  $P_{n+1}$  对  $C$  解密得到  $s_{n+1} = f(n+1) g^{d_{n+1}\sum_{j=1}^t l_j} g^{-d_{n+1}\sum_{j=1}^t l_j} = f(n+1)$ , 显然  $((n+1), s_{n+1})$  满足式(1)中的多项式  $f(x)$ , 即本文协议产生的新份额是正确的.

1),  $s_{n+1}$ ) 满足式(1)中的多项式  $f(x)$ , 即本文协议产生的新份额是正确的.

### 3.2 安全性分析

一个新份额产生协议应该达到 3 个安全目标<sup>[7]</sup>: ①关于秘密的任何信息都不能被披露; ②除了合法秘密持有者,任何人都不能得到新的份额; ③老成员的份额是安全的.

(1)在本文提出的协议中,尽管将  $g^k$  公布作为验证信息,但由于求解离散对数在计算上是不可行的,所以任何人从  $g^k$  都得不到关于秘密  $k$  的任何信息.

(2)在产生新份额时,  $C$  虽然由老成员  $P_1, P_2, \dots, P_t$  合作产生,却以新成员  $P_{n+1}$  的密钥  $d_{n+1}$  进行 ElGamal 加密,即  $C = f(n+1) g^{d_{n+1}\sum_{j=1}^t l_j}$ . 由 ElGamal 加密算法可知,在不知道  $d_{n+1}$  的情况下,要获得  $s_{n+1}$  将面临破解 ElGamal 加密算法(或离散对数问题)的困难.因此,除了合法秘密持有者,任何人都得不到新份额  $s_{n+1}$ .

(3)在计算  $M_i (i=1, 2, \dots, t)$  时,每个老成员  $P_i$  的份额  $s_i$  被加密了 3 次,即由持有者  $P_i$  以  $e_i$  加密,新成员以  $g^{d_{n+1}}$  加密和合作组以  $g^k$  加密.因此,系统外的攻击者想要获得  $s_i$  将面临一次破解乘数加密和两次破解 ElGamal 算法(或离散对数问题)的困难.另外,在产生新份额的过程中,  $s_i \omega_i (n+1)$  的计算是非线性的,而且每一步计算结果都以  $g^k$  进行加密,因此任何人(包括  $P_{n+1}$ )都无法获得关于  $s_i (i=1, 2, \dots, t)$  的有用信息,即老成员的秘密份额是安全的.

本文协议产生的新份额是可以验证的,由 2.3

节可知,新成员可以利用式  $g^{s_{n+1}} = g^k \prod_{l=1}^{t-1} (g^{a_l})^{(n+1)^l}$  来验证新份额的真实性,这可以防御系统中可能出现的主动攻击,而在 Dong 等人的协议中不具备新份额验证的能力,新成员无法验证所分配份额的真实性,很可能接收假的份额,从而无法达到新个体加入的目的.

综上所述,可以得出本文提出的协议满足新份额产生的安全目标,且可验证新份额的真实性,具有更高的安全性.

### 3.3 性能分析

下面从密钥管理、是否需要可信任中心和广播规模这 3 个方面来分析本文协议的性能.

(1)在本文的协议中,每个参与者的计算结果是

通过广播来传送的,而且所有需要保密的数据均由该数据的产生者来管理.因此,本文协议的密钥管理非常简单.

(2)与 Shuffling 协议、Wong 等人的协议和 Dong 等人的协议一样,本文提出的协议不需要可信中心参与新份额的产生.

(3)本文的协议仅需  $6t$  次广播,与 Dong 等人的协议中的一样多,而 Shuffling 协议和 Wong 等人的协议中都需要  $t^2$  规模的秘密通讯,显然本文协议的通讯规模是比较小的.

从上面的分析可以看出,本文提出的协议具有明显的优势,尤其在无线网络环境中,由于网络连接的可靠性很低,容易受到攻击者的主动和被动攻击,通讯次数越少,新份额产生成功的概率就越大.因此,本文协议可靠性高,可用性强.

## 4 结 论

本文提出了一个可验证的新份额产生协议,该协议允许秘密共享方案中新成员动态加入,而不需要更新原有成员的份额.该协议能够验证新产生份额的真实性,预防系统中可能出现的主动攻击.在产生新份额时,原有成员的份额不需要更新,而且新份额的产生不影响原有份额的安全性.另外,本文协议的通讯量仅为  $6t$  规模,与现有方案相比是比较低的,而且密钥管理简单,特别适合应用在连接不可靠的无线网络中.分析结果表明,本文提出的协议符合秘密共享的安全性要求和目标,是一个安全有效的新份额产生协议.

## 参考文献:

- [1] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.
- [2] Blakley G. Safeguarding cryptographic key [A]. AFIPS 1979 Natl Conf, New York, USA, 1979.
- [3] Yang C C, Chang T Y, Hwang M S. A  $(t, n)$  multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2004, 151(2): 483-490.
- [4] Pang L J, Wang Y M. A new  $(t, n)$  multi-secret sharing scheme based on Shamir's secret sharing [J]. Applied Mathematics and Computation, 2005, 167(2): 840-848.
- [5] Luo H, Lu S. Ubiquitous and robust authentication services for Ad Hoc wireless networks [R]. Technical Report, TR-200030. Los Angeles, USA: Department of Computer Science, University of California, Los Angeles, 2000. 28-33.
- [6] Wong T M, Wang C X, Wing J M. Verifiable secret redistribution for archive systems [A]. The 1st Int'l Security in Storage Workshop, Greenbelt, USA, 2002.
- [7] Dong P, Kuang X H, Lu X C. A non-interactive protocol for member expansion in a secret sharing scheme [J]. Journal of Software, 2004, 16(1): 116-120.
- [8] Lamport L, Shostak R, Pease M. The Byzantine general problems [J]. ACM Trans Prog Lang Syst, 1982, 4(3): 382-401.
- [9] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Trans on IT, 1985, 31(4): 469-472.

(编辑 刘 杨 苗 凌)

[文摘预登]

## 基于离散余弦变换直流分量的盲视频水印方案

刘连山<sup>1,2</sup>, 李人厚<sup>1</sup>

(1. 西安交通大学系统工程研究所, 710049, 西安; 2. 山东科技大学信息科学与工程学院, 266510, 青岛)

利用离散余弦变换(DCT)直流系数稳定的特点,提出了一种通过调整视频图像的分块 DCT 直流系数来隐藏水印的方法.将选取的视频帧以  $8 \times 8$  像素进行分块,根据掩蔽矩阵来选取需要嵌入的水印块.把选中的图像块再以  $4 \times 4$  像素细分为 4 个互不重叠的小图像块,调整它们的 DCT 直流系数的值并将其嵌入水印.实验结果证明,该视频算法具有很强的鲁棒性且计算简单,能抵抗缩放、帧删除、多次视频压缩、转换压缩编码格式、共谋攻击、删除行或列等有意和无意的攻击,特别是当 MPEG-2 压缩比特率为 4 Mb/s 时,从 3 幅图像中提取的水印相关值分别达到了 0.996 1, 0.996 1 和 0.986 3.