文章编号:1007-5321(2010)06-0072-04

可验证的多策略秘密共享方案

王 锋, 谷利泽, 郑世慧, 杨义先, 胡正名
(1. 北京邮电大学 网络与交换技术国家重点实验室, 北京 100876; 2. 北京邮电大学 网络信息攻防教育部重点实验室, 北京 100876;
3. 北京邮电大学 灾备技术国家工程实验室, 北京 100876)

摘要: 可验证多重秘密共享方案普遍不能区分共享群组密钥的安全等级,即分享群组密钥的门限值相等,为此,提出了一种可验证的多策略秘密共享方案. 在该方案中,密钥分发者能根据分发群组密钥的安全等级选择不同的门限值;在群组密钥分发和重构过程中,能实现参与者对密钥分发者和重构者对参与者的验证,及时检测和识别密钥分发者对参与者以及参与者对密钥重构者的欺骗,从而提高重构群组密钥的成功率;参与者的子密钥能重复使用,可减少密钥分发者的计算负担,提高方案的效率. 该方案具有较高的安全性和实用性.

关 键 词: 秘密共享; 验证性; 多策略; 密钥管理
中图分类号: TP309 **文献标志码**: A

A Verifiable Multi-Policy Secret Sharing Scheme

WANG Feng, GU Li-ze, ZHENG Shi-hui, YANG Yi-xian, HU Zheng-ming
(1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China; 2. Key Laboratory of Network and Information Attack and Defence Technology, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China; 3. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: The secret sharing schemes are important techniques for key management. However, most verifiable multi-secret sharing schemes can not distinguish the security classification because of having the common drawback of sharing secrets with the same value. A verifiable multi-policy secret sharing scheme is proposed. The significant character of the proposed scheme is that each participant has to be kept only one master secret share, the share can be used to reconstruct different group secrets according to the number of threshold values. So it will reduce the calculated amount of the secret distributor. Moreover, the efficient solutions against multiform cheating are proposed, the scheme is therefore with highly security and practicality.

Key words: secret sharing; verifiability; multi-policy; key management

0 引言

秘密共享技术是现代密码学和信息安全的重要研究内容,第 1 个(t,n)门限秘密共享方案[1-2]被提出后,秘密共享技术的理论和应用引起了密码学者的广泛关注,并取得了很多研究成果[3-7]. 目前,秘密共享技术广泛应用于信息安全和数据保密中的数字签名、多方安全计算、银行金库和导弹发射密钥管理等[8-9]. 现有的可验证多重秘密共享方案都有一个共同的缺点,即每个共享密钥对应的门限相等,无

收稿日期: 2009-09-29
基金项目: 国家重点基础研究发展计划项目(2007CB310704); 国家自然科学基金项目(90718001); 国家高技术研究发展计划项目(2009AA01Z439)
作者简介: 王 锋(1982—), 男, 博士生, E-mail: flys99@126.com; 胡正名(1931—), 男, 教授, 博士生导师.

法区别共享密钥的安全等级，这在现实生活中会产生很多问题. 针对这一问题，文献[10]提出了一个多策略秘密共享方案，其中，不同的共享密钥对应的门限值不同. 为提高性能，文献[11]也提出了一个不同共享密钥对应不同门限的多秘密共享方案. 但是，文献[10-11]的方案存在 2 个问题.

1）秘密分发过程中不能防止秘密分发者对参与者的欺骗，即参与者不能验证其子密钥的真实性.

2）群组密钥重构过程中不能防止不诚实的参与者对密钥重构者的欺骗，即密钥重构者不能验证重构信息的真实性.

本文提出了一个可验证的多策略秘密共享方案，不仅解决了文献[10-11]方案存在的问题，还能实现群组密钥分发过程中，密钥分发者能根据分发密钥的安全等级选择不同的门限值；参与者的子密钥能重复使用；重构门限值高的群组密钥后不影响未重构门限值低的群组密钥的安全性.

1　方案构成

本文基于 Rivest-Shamir-Adleman（RSA）公钥密码体制和离散对数难题，提出了一个可验证的多策略秘密共享方案. 密钥分发者需要一个公告牌（NB），只有密钥分发者可以修改、更新 NB 上的内容，其他人只能阅读或下载.

1.1　系统初始化阶段

在该阶段，密钥分发者（SD）需要公布以下系统参数：p、q 为满足 RSA 密码体制安全性要求的 2 个大素数，且满足 $p=2p'+1$、$q=2q'+1$（p'和 q'也是大素数）；$N=pq$；$R=p'q'$；g 为正整数群$(\mathbb{Z}_N,\cdot)$中指数为 R 的生成元；(e,d)为 SD 的 RSA 算法的公钥和私钥对，满足 $ed=1\bmod(\varphi(N))$，其中 $\varphi(N)$为 N 的欧拉函数值；$G=\{U_1, U_2, \cdots, U_n\}$为参与者的集合，其中 U_j 的身份标识为 $\mathrm{ID}_j(j=1,2,\cdots,n)$；$S=\{S_1,S_2,\cdots,S_k\}(k\leqslant n)$为群组密钥的集合.

SD 将$\{N,g,e\}$公布于 NB 上，$\{R,d\}$自己保密.

1.2　子密钥的分发和验证阶段

SD 在$\mathbb{Z}_R$随机选取 n 个不同的 x_j 作为 U_j 的子密钥，随后随机选择 $a_i\in\mathbb{Z}_R$ 和 $d_i\in\mathbb{Z}_R$，构造 $i-1$ 阶多项式

$$f_i(x)=a_i+d_1x+d_2x^2+\cdots+d_{i-1}x^{i-1}\bmod R$$

并计算

$$\left.\begin{aligned}C_{ij}&=f_i(\mathrm{ID}_j)\bmod R\\Y_{ij}&=g^{C_{ij}}\bmod N\\K_{ij}&=x_j\oplus C_{ij}\end{aligned}\right\}$$

其中，C_{ij}为参与者身份标识对应的多项式值；Y_{ij}为 C_{ij}的公开消息；K_{ij}为参与者的伪秘密份额.

随后 SD 在 NB 上公布 $\{K_{ij}, Y_{ij}, g^{a_i}, g^{d_1}, \cdots, g^{d_{i-1}}\}$，$x_j$ 通过安全的信道发送给 U_j. U_j 收到 x_j 后，从 NB 上得到$\{K_{ij}, g^{a_i}, g^{d_1}, \cdots, g^{d_{i-1}}\}$，计算 $x_{ij}=x_j\oplus K_{ij}$，然后利用

$$g^{x_{ij}}=g^{a_i}\prod_{m=1}^{i-1}(g^{d_m})^{(\mathrm{ID}_i)^m}\bmod N \tag{1}$$

验证 x_j 的真实性. 如果式(1)不成立，则 U_j 收到的子密钥是假的，U_j 可要求 SD 重新为其分发子密钥.

1.3　群组密钥的分发

SD 根据 $S_1,S_2,\cdots,S_k$ 安全等级不同采用不同的门限值. 不失一般性，设 S_i 对应的门限值为 i，分发信息公布在 NB 上.

SD 在$\mathbb{Z}_R$随机选择不同的整数 r_i 计算公开信息为

$$\left.\begin{aligned}T_i&=(g^{r_i})^d\bmod N\\H_i&=g^{a_ir_id}\oplus S_i\end{aligned}\right\}$$

SD 将$\{r_i, T_i, H_i\}$在 NB 上公布.

1.4　群组密钥的重构

假设重构 S_l 和 G 中任意 l 个或多于 l 个的参与者将重构信息发送给密钥重构者，密钥重构者能对参与者进行验证，从而提高了重构密钥的成功率. 设 $W(|W|=l\leqslant k)$是 G 中任意 l 个成员的子集合；不失一般性，设 l 个 $U_j\in W$ 参与重构 $S_l\in S$，各参与者的操作步骤如下：

1）每个 $U_j\in W$ 从 NB 上下载(K_{lj},T_l)后用自己的子密钥 x_j 计算群组密钥的重构信息为

$$\left.\begin{aligned}B_{lj}&=K_{lj}\oplus x_j\\A_{lj}&=(T_l)^{B_{lj}}\bmod N\end{aligned}\right\}$$

$U_j(j=1,2,\cdots,l)$将 A_{lj}通过安全信道发送给密钥重构者.

2）密钥重构者收到参与者发送的 A_{lj}后从 NB 上下载(Y_{lj}, r_l)，通过

$$(A_{lj})^e=(Y_{lj})^{r_l} \tag{2}$$

验证 A_{lj}的真实性. 若式(2)不成立，说明 A_{lj}是假的，可要求 U_j 重新发送真实的 A_{lj}；若所有 A_{lj}都满足式(2)，密钥重构者进行步骤 3).

3）密钥重构者从 NB 上下载 H_l 后计算

$$S_l' = H_l \oplus \left(\prod_{U_j \in W} (A_{lj})^{\Delta_j} \bmod N \right) = S_l \qquad (3)$$

其中 $\Delta_j = \prod_{U_i \in W, U_i \neq U_j} \frac{-\mathrm{ID}_i}{\mathrm{ID}_j - \mathrm{ID}_i}$.

2 方案分析

可验证多策略门限秘密共享方案能实现不同的共享密钥对应不同的重构门限值;在方案的实现过程中,能及时检测和识别 SD 对参与者以及参与者对密钥重构者的欺骗,从而提高了方案实现的成功率. 本文方案的安全性是基于 RSA 公钥密码体制和离散对数难题,安全性较高.

2.1 方案的验证性分析

定理 1 密钥分发阶段中 U_j 通过式(1)能验证 SD 分发的子密钥 x_j 的真实性.

证明 U_j 收到 x_j 后从 NB 上得$\{K_{ij}, g^{a_i}, g^{d_1}, \cdots, g^{d_{i-1}}\}$,计算 $x_{ij} = x_j \oplus K_{ij}$,由于 $K_{ij} = x_j \oplus C_{ij}$,故 $x_{ij} = C_{ij}$. 由 $C_{ij} = f_i(\mathrm{ID}_j) \bmod R$ 得 $x_{ij} = f_i(\mathrm{ID}_j) \bmod R$,所以

$$g^{x_{ij}} \bmod N = g^{f_i(\mathrm{ID}_j)} = g^{a_i + d_1(\mathrm{ID}_j) + d_2(\mathrm{ID}_j)^2 + \cdots + d_{i-1}(\mathrm{ID}_j)^{i-1}} = g^{a_i} \prod_{m=1}^{i-1} (g^{d_m})^{(\mathrm{ID}_i)^m} \bmod N$$

式(1)成立,即方案能实现参与者对 SD 的验证.

定理 2 密钥重构阶段中密钥重构者能通过式(2)验证 U_j 发送重构信息 A_{lj} 的真实性.

证明 因为 $B_{lj} = K_{lj} \oplus x_j$、$K_{lj} = x_j \oplus C_{lj}$,所以 $B_{lj} = C_{lj}$. 因为 $A_{li} = (T_l)^{B_{li}} \bmod N$、$T_l = (g^{r_l})^d \bmod N$,所以 $A_{lj} = (g^{r_l})^{dC_{lj}} \bmod N$、$(A_{lj})^e = (g^{r_l})^{edC_{lj}} = (g^{C_{lj}})^{r_l ed} \bmod N$. 由于 $ed = 1 \bmod (\varphi(N))$,所以 $(A_{lj})^e = (g^{C_{lj}})^{r_l} \bmod N$. 由于 $Y_{lj} = g^{C_{lj}} \bmod N$,所以

$$(A_{lj})^e = (g^{C_{lj}})^{r_l} \bmod N = Y_{lj}^{r_l} \bmod N$$

式(2)成立,即密钥重构者能实现对参加重构共享密钥参与者的验证.

定理 3 密钥重构者利用真实的重构信息 A_{lj} 能通过式(3)重构群组密钥 $S_l \in S$.

证明 由于 $H_l = g^{a_l r_l d} \oplus S_l$,

$$A_{lj} = g^{r_l d C_{lj}} \bmod N \ (j = 1, 2, \cdots, l)$$

由式(3)得

$$S_l' = H_l \oplus \prod_{U_j \in W} (A_{lj})^{\Delta_j} \bmod N = g^{a_l r_l d} \oplus S_l \oplus \prod_{U_j \in W} (g^{r_l d C_{lj}})^{\Delta_j} \bmod N$$

由 $\Delta_j = \prod_{U_i \in W, U_i \neq U_j} \frac{-\mathrm{ID}_i}{\mathrm{ID}_j - \mathrm{ID}_i}$ 和 Lagrange 插值定理得

$$\prod_{U_j \in W} (g^{r_l d C_{lj}})^{\Delta_j} \bmod N = g^{f_l(0) r_l d} = g^{a_l r_l d} \bmod N$$

所以

$$S_l' = H_l \oplus \prod_{U_j \in W} (A_{lj})^{\Delta_j} \bmod N = g^{a_l r_l d} \oplus S_l \oplus g^{a_l r_l d} \bmod N = S_l$$

式(3)成立,即密钥重构者利用真实的重构信息 A_{lj} 能通过式(3)重构群组密钥 $S_l \in S$.

2.2 方案的安全性分析

1) 参与者的子密钥是安全的. 在密钥分发过程中,SD 通过安全信道将参与者的子密钥发送给指定参与者,且参与者能通过式(1)验证子密钥的真实性. 在密钥重构过程中,U_j 不是将子密钥 x_j 发送给密钥重构者,而是发送给 A_{ij},从而防止子密钥的暴露,保证了子密钥的安全. 攻击者可能会利用 NB 上公布的(K_{ij}, Y_{ij}),从 Y_{ij} 得到 C_{ij},再利用 K_{ij} 得到 x_j,这是不能成功的. 因为从 Y_{ij} 得到 C_{ij} 就要解决离散对数难题(DLMC),现有的计算能力还无法有效解决 DLMC.

2) 群组密钥是安全的. 攻击者利用 NB 中公布的群组密钥的信息无法恢复出群组密钥. 例如,攻击者可能会利用等式 $H_i = g^{a_i r_i d} \oplus S_i$ 和 NB 上的 H_i、r_i、g^{a_i}、e 通过计算 $g^{a_i r_i d}$ 得到 S_i,这样攻击者要从$\{N, e\}$得到 d,但是其难度相当于破译 RSA 公钥密码体制. 另外,1 次密码重构不会影响其他未重构群组密码的安全性. 例如,密钥重构者可能会在重构了门限为 l 的群组密钥 S_l 后,利用现有的重构信息重构门限为 $l-1$ 的共享密钥 S_{l-1}. 从群组密钥重构过程中可以看出,不同的群组密钥 S_i 需要不同的 $g^{a_i r_i d}$. 密钥重构者在重构 S_l 后,得到的是 $g^{a_l r_l d}$,而 $S_{l-1} = g^{a_{l-1} r_{l-1} d} \oplus H_{l-1} \bmod N$,另外,密钥重构者从重构信息 A_{lj} 不能得到 $A_{(l-1)j}$,因为这同样要解决 DLMC 和破译 RSA 公钥密码体制. 所以,利用 l 个成员的重构信息不能重构出门限为 $l-1$ 的群组密钥 S_{l-1}.

3) 在群组密钥重构过程中,能有效阻止不诚实参与者 U_j' 伪造满足式(2)的 A_{ij}'. U_j' 要想伪造满足式(2)的 A_{ij}',首先要有 SD 的 RSA 私钥 d,然后改变 NB 上的 Y_{ij} 或 r_i. 但是,U_j' 从$\{N, e\}$得到 d 的难度相当于破译 RSA 密码体制;另外,只有 SD 才能更改 NB 上的内容,其他人只能阅读或下载,所以 U_j' 不能伪造满足式(2)的 A_{ij}'.

2.3 方案的性能分析

文献[11]指出,其方案的性能要优于文献[10]方案,但是文献[10-11]方案都不具备可验证的功

能，表 1 给出了本文方案与文献[10-11]方案在计算　　复杂度和功能上的比较.

表 1　本文方案与文献[10-11]方案在计算复杂度和功能上的比较

性能	文献[10]方案	文献[11]方案	本文方案
系统初始化复杂度	0	0	0
密钥分发复杂度	$k(2n+1)T_e + knT_h$	knT_h	$2knT_e + knT_m$
群组密钥重组复杂度	$2kT_e + (2k^2-k)T_m$	$(2k^2-2k)T_m$	$2kT_e + (k^2-k)T_m$
方案的总复杂度	$(2nk+3k)T_e + (2k^2+kn-k)T_m$	$(2k^2+kn-2k)T_m$	$2k(n+1)T_e + (k^2+kn-k)T_m$
对 SD 的验证	否	否	是
对参与者的验证	否	否	是
参与者子密钥重复使用	是	是	是

注：T_e 表示执行 1 次模指数运算所需的时间；T_m 表示执行 1 次模乘运算所需的时间；T_h 表示执行 1 次单向 Hash 函数所用的时间. 其中，$T_m = T_h$，$T_e = 240T_m$.

从表 1 可见，本文方案在计算复杂度方面要优于文献[10]方案，而比文献[11]方案要稍微复杂. 但是，本文方案能实现参与者对 SD 及密钥重构者对参与者的验证，这样不仅提高了方案的安全性，也提高了密钥重构的成功率，从而提高了方案实现的效率. 因此，本文方案比文献[10-11]方案具有更好的性能和更高的安全性，更适于实际应用.

3　结束语

本文提出的可验证(t,n)多策略秘密共享方案，在保持现有多策略秘密共享方案特性的同时，很好地解决了现有多策略秘密共享方案存在的欺骗问题；在方案实现的过程中，不需要交互式协议就能实现参与者对 SD 及密钥重构者对参与者的验证，有效阻止了 SD 对参与者及参与者对密钥重构者的欺骗，从而提高了群组密钥重构的成功率和方案的效率，具有较高的安全性和应用性.

参考文献：

[1] Shamir A. How to share a secret[J]. Communication of the ACM, 1979, 22(11): 612-613.

[2] Blakley G. Safeguarding cryptographic keys[C]// Proc AFIPS 1979 NCC. New York: AFIPS Press, 1979: 313-317.

[3] 张勐, 刘振华, 温巧燕. 严格 k-欺骗免疫秘密共享[J]. 北京邮电大学学报, 2007, 30(2): 24-27.
Zhang Jie, Liu Zhenhua, Wen Qiaoyan. Strictly k-cheating immune secret sharing[J]. Journal of Beijing University of Posts and Telecommunications, 2007, 30(2): 24-27.

[4] Dong Y, Go H W, Sui A F, et al. Providing distributed certificate authority service in mobile ad hoc networks[C]// SecureComm 2005. Athens: [s. n.], 2005: 149-156.

[5] 于佳, 郝容, 孔凡玉, 等. 先动的可公开验证服务器辅助秘密共享[J]. 北京邮电大学学报, 2008, 31(5): 13-17.
Yu Ja, Hao Rong, Kong Fanyu, et al. Proactive and publicly verifiable server-assisted secret sharing[J]. Journal of Beijing University of Posts and Telecommunications, 2008, 31(5): 13-17.

[6] Chang T Y, Hwang M S, Yang W P. A new multi-stage secret sharing scheme using one-way function[J]. Association for Computing Machinery, 2005, 39(1): 48-55.

[7] Chang T Y, Hwang M S, Yang W P. An improvement on the Lin-Wu (t, n)-threshold verifiable multi-secret sharing scheme[J]. Applied Mathematics and Computation, 2005, 163(1): 169-178.

[8] Fouque P A, Poupard G, Stern J. Sharing decryption in the context of voting or lotteries[C]// FC 2000. Berlin: Springer Verlag, 2000: 90-94.

[9] Ray I, Narasimhamurthi N. An anonymous electronic voting protocol for voting over the Internet[C]// WECWIS'01. Los Alamitos: IEEE Computer Society, 2001: 188-190.

[10] Geng Yongjun, Fan Xiahong, Hong Fan. A new multi-secret sharing scheme with multi-policy[C]// ICACT'07. Phoenix Park: National Computerization Agency, 2007: 1515-1517.

[11] Lin Hanyu, Yeh Y S. Dynamic multi-secret sharing scheme[J]. International Journal of Contemporary Mathematical Sciences, 2008, 3(1): 37-42.