第 26 卷第 6 期 电子与信息学报 Vol.26No.6
2004 年 6 月 Journal of Electronics & Information Technology June 2004

基于因子分解和离散对数的动态秘密分享方案 [1]

何业锋 张建中

(陕西师范大学数学与信息科学学院 西安 710062)

摘 要: 该文提出了一个安全性基于离散对数与因子分解的动态秘密分享方案. 它具有如下优点: (1) 系统更新分享的秘密时, 无需更新分享的子秘密, 即子秘密可重复使用; (2) 当系统增删成员时, 无需变更其他成员的子秘密; (3) 当某个成员的子秘密泄露时, 系统只需为该成员重新分配子秘密而不必更改其他成员的子秘密; (4) 防止欺诈; (5) 通信量较少, 工作效率高.

关键词: 离散对数, 因子分解, 动态秘密分享, 欺诈

中图分类号: TN918 **文献标识码**: A **文章编号**: 1009-5896(2004)06-1005-04

A Dynamic Secret Sharing Scheme Based on Factorization and Discrete Logarithms

He Ye-feng Zhang Jian-zhong

(*College of Mathematics and Info. Science, Shanxi Normal Univ., Xi'an* 710062, *China*)

Abstract A dynamic secret sharing scheme based on discrete logarithms and factorization is proposed in this paper. It has the following advanced properties: (1) The dealer can renew system secrets without renewing the shadows of the participants; (2) When the system accepts a new participant or fires a participant, the shadows of other participants would not change; (3) When some participants' shadows are revealed ,they can be renewed without any effect on the others; (4) It can detect the cheater; (5) Comunication is reduced and work efficiency is improved.

Key words Discrete logarithms, Factorization, Dynamic secret sharing, Cheating

1 引言

秘密分享在现代密码学中占有重要的地位, 其应用涉及到密钥管理、安全多方计算、金融网安全、电子商务等诸多领域. 最早的秘密分享方案是在 1979 年由 Shamir[1] 和 Blackley[2] 分别基于 Lagrange 插值多项式和射影几何理论独立提出的. 自此以后, 秘密分享方案得到了广泛的研究, 其中门限秘密分享方案是研究最早、成果最多的一种秘密分享方案. 具体地说, (t,n)-门限方案 [1,2] 是秘密分发者将秘密分拆成若干个子秘密, 分配给 n 个秘密分享者, 使得这 n 个分享者中任何 t 个人就可恢复秘密, 但任何少于 t 个分享者都无法恢复该秘密.

但开始的大多数门限方案 [1,3,4] 不能防止秘密分发者的欺诈行为, 而且分享者的子秘密 (秘密影子 shadow) 只能使用一次. 虽然后来许多研究者对门限方案做了改进, 设计了一些防欺诈的动态秘密分享方案 [5−8] , 但他们的方案构成都比较复杂. 本文根据有限域上离散对数问题及大数分解问题的困难性, 提出了一个简单有效的动态秘密分享方案, 它可以防止恶意参与者的

[1] 2003-01-09 收到, 2003-09-08 改回

国家自然科学基金 (No.10271069)、陕西省自然科学基础研究计划项目 (2002A03)、陕西师重点科研项目资助课题

欺诈. 且子秘密可以无限制地多次使用，减少了秘密分发者与秘密分享者之间的通信量，提高了工作效率. 在实际中将会得到更广泛的应用.

2 方案构成

在给出新方案之前，首先介绍本文用到一些定义及符号.

定义 1 秘密分发者 (dealer) 记为 D，指把秘密分发给 n 个秘密分享者的人或服务器. K 为待分享的秘密. $P_1, P_2, \cdots, P_n$ 是 n 个秘密分享者. I_j 表示 P_j 的身份标识符号 $(j = 1, 2, \cdots, n)$.

定义 2 公告栏 (NB) 指存放公开参数或数据的媒介. 系统各方均可访问公告栏上的内容，但只有秘密分发者 D 才能修改或更新公告栏上的内容.

系统参数 p 为系统选择的大素数，$\mathrm{GF}(p)$ 为相应的有限域，p_1 与 q_1 为 $p-1$ 的两个大素因子，$n = p_1 q_1$. g 为 $\mathrm{GF}(p)$ 上阶为 n 的生成元. 在公告栏上公开 p, g, n，但保密 p_1 与 q_1.

秘密分配 (1) 秘密分发者 D 随机选择 n 个不同的元素 $s_1, s_2, \cdots, s_n \in Z_n$, 并计算 $y_i = g^{s_i} \bmod p$. 将有序数组 $(y_1, y_2, \cdots, y_n)$ 在公告栏上公开，并将 s_i 通过安全信道秘密发送给 P_i 作为他拥有的子秘密 $(i = 1, 2, \cdots, n)$. (2) 秘密分发者 D 随机选择一个元素 $\alpha \in Z_n$ 与一个 $t-1$ 次多项式 $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \in Z_n[x]$, 满足 $f(0) = K$(待分享的秘密), $f(x)$ 保密. 然后计算

$$v_k = g^{a_k} (\bmod\ p), \quad k = 0, 1, \cdots, t-1$$

$$d_i = f(I_i) - (\alpha + s_i)^2 (\bmod\ n), \quad i = 1, 2, \cdots, n$$

D 在公告栏上公开 α 及有序数组 $(v_0, v_1, \cdots, v_{t-1})$ 与 $(d_1, d_2, \cdots, d_n)$.

子秘密的验证 每一个秘密分享者 P_i 在收到秘密分发者 D 发送给他的子秘密 s_i 后，为了验证他所分享的子秘密的有效性，可以查看系统的公告栏，从中找到公开数据 α, d_i 与 $(v_0, v_1, \cdots, v_{t-1})$. 计算 $x_i = (\alpha + s_i)^2 \bmod n$，然后再验证等式：

$$g^{d_i + x_i} = \left(\prod_{k=0}^{t-1} (v_k)^{(I_i)^k} \right) (\bmod\ p)$$

是否成立. 若成立，则认为他所分享的子秘密是有效的. 否则，要求秘密分发者重新公布满足验证等式的 d_i.

秘密恢复 当任意 t 个子秘密的持有者 (不妨设为 $P_1, P_2, \cdots, P_t$) 要恢复系统秘密 K 时，每个成员 P_i 在公告栏上查到 α，然后计算 $x_i = (\alpha + s_i)^2 \bmod n$. 提交屏蔽子秘密 x_i(即子秘密 s_i 的隐藏形式). 其他合作者可以共同验证如下等式：$g^{d_i + x_i} = \left(\prod_{k=0}^{t-1} (v_k)^{(I_i)^k} \right) (\bmod\ p)$ 是否成立. 若成立，则认为 P_i 提供的是有效的屏蔽子秘密 x_i，从而得 $f(I_i) = d_i + x_i \bmod n$ 也是有效的. 再由 $(I_1, f(I_1)), (I_2, f(I_2)), \cdots, (I_t, f(I_t))$ 共 t 个点及 Lagrange 插值公式可求 $f(x)$ 从而恢复系统分享的秘密 $K = f(0)$.

因为 α 可以任意取值，故子秘密 s_i 可以无限制的多次使用.

3 性能分析

定理 若等式 $g^{d_i + x_i} = \prod_{k=0}^{t-1} (v_k)^{(I_i)^k} (\bmod\ p)$ 成立，则认为秘密分享者 P_i 所拥有的子秘密是有效的.

证明　因为

$$g^{d_i+x_i} = g^{d_i+(\alpha+s_i)^2} = g^{f(I_i)} = g^{\sum_{k=0}^{t-1} a_k (I_i)^k}$$
$$= \prod_{k=0}^{t-1} g^{a_k (I_i)^k} = \prod_{k=0}^{t-1} (g^{a_k})^{(I_i)^k} = \prod_{k=0}^{t-1} (v_k)^{(I_i)^k} (\mathrm{mod}\ p)$$

可见当秘密分享者 P_i 拥有的子秘密 s_i 有效时，上面的等式成立。

3.1 安全性　本方案的安全性基于离散对数与大数分解的困难性。在恢复秘密时，分享者 P_i 提供的是屏蔽子秘密 $x_i = (\alpha + s_i)^2 \mathrm{mod}\ n (i = 1, 2, \cdots, t)$ 。攻击者若要从 $x_i = (\alpha + s_i)^2 \mathrm{mod}\ n$ 中求出 s_i ，即为求解合数模的二次剩余问题。而我们知道这是一个困难问题，它的困难性等价于对 n 作因子分解，故是计算不可行的。另一方面，由离散对数问题的困难性可知，攻击者也无法从公开数据 $(y_1, y_2, \cdots, y_n)$ 与 $(v_0, v_1, \cdots, v_{t-1})$ 及验证等式 $g^{d_i+x_i} = \prod_{k=0}^{t-1} (v_k)^{(I_i)^k} (\mathrm{mod}\ p)$ 中求出 s_i ，故攻击者无法恢复系统分享的秘密，方案是安全的。

3.2 防欺诈　(a) 防秘密分发者的欺诈：每个秘密分享者 P_i 在收到他所分享的子秘密 s_i 后，可以通过验证等式 $g^{d_i+x_i} = \prod_{k=0}^{t-1} (v_k)^{(I_i)^k} (\mathrm{mod}\ p)$ 是否成立，来验证他所分享的子秘密 s_i 的有效性，从而可以防止秘密分发者 D 的欺诈行为。(b) 防秘密分享者的欺诈：在恢复秘密时，每个分享者 P_i 提供的是屏蔽子秘密 x_i 。合作者可以根据验证等式 $g^{d_i+x_i} = \prod_{k=0}^{t-1} (v_k)^{(I_i)^k} (\mathrm{mod}\ p)$ 成立与否来判断 P_i 提供的屏蔽子秘密 x_i 是否有效。因此，本方案可以防止恶意参与者提供虚假的子秘密。

3.3 秘密更新　当需要重新分配一个新秘密时，秘密分发者 D 只需重新选择一个 $\alpha' (\alpha' \neq \alpha)$ 及一个新的 $(t-1)$ 次多项式 $f'(x) (f'(x) \neq f(x))$ ，满足 $f'(0) = K'$ 为新秘密。然后利用新的 α' 及 $f'(x)$ 更新公告栏上的 α 及有序数组 $(d_1, d_2, \cdots, d_n)$ 和 $(v_0, v_1, \cdots, v_{t-1})$ 而无需更改每个分享者 P_i 的子秘密 s_i ，当然有序数组 $(y_1, y_2, \cdots, y_n)$ 也无需变动。

由于 a 是 Z_n 上的任意元素，故每个成员的子秘密 s_i 可以无限制地多次使用。

3.4 增删成员　当系统需增加新成员 P_{n+1} 时，D 只需为 P_{n+1} 随机生成一个子秘密 s_{n+1} ，并在公告栏上的有序数组 $(y_1, y_2, \cdots, y_n)$ 和 $(d_1, d_2, \cdots, d_n)$ 中分别增加 $y_{n+1} = g^{s_{n+1}} \mathrm{mod}\ p$ 与 $d_{n+1} = f(I_{n+1}) - (\alpha + s_{n+1})^2 \mathrm{mod}\ p$ 即可。

当要删除某个成员 P_j 时，只需重新选择一个 $t-1$ 次多项式 $f'(x)$ ，满足 $f'(0) = K$ 为分享的秘密。然后利用新的 $t-1$ 次多项式 $f'(x)$ 更新公告栏上的有序数 $(v_0, v_1, \cdots, v_{t-1})$ 与 $(d_1, d_2, \cdots, d_n)$ ，此时无需计算 d_j(可令 d_j 仍为原值或置 d_j 项为空)，则 P_j 的子秘密即无效。

3.5 子秘密维护　当某个成员 P_j 的子秘密泄露时，D 只需为该成员重新分配 s_j' 之后选择一个 $t-1$ 次多项式 $f'(x)$ ，满足 $f'(0) = K$ 。并利用新的 s_j' 和 $f'(x)$ 更新公告栏上的有序数组 $(y_1, y_2, \cdots, y_n)$, $(d_0, d_1, \cdots, d_n)$ 和 $(v_0, v_1, \cdots, v_{t-1})$ ，而不必更改其他成员的子秘密。

4 结束语

本文基于离散对数与大数分解的困难性，提出了一个防欺诈的动态秘密分享方案，在这个方案中，当秘密更新时，分享者的子秘密无需变更，即子秘密可以重复使用。故而减少了秘密分发者与秘密分享者之间的通信量。从而提高了工作效率，更宜于实际使用。

参　考　文　献

[1] Shamir A. How to share a secret. *Communications of the ACM*, 1979, 22(11): 612–613.

[2] Blackley G R. Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference of AFIPS, Montvale, 1979, 48: 313–317.

[3] Fouque P A, Poupard G, Sten J. Sharing decryption in the context of voting or lotteries. Proceedings of Financial Cryptography 2000. Berlin: Springer-Verlag, 2000: 90–104.

[4] Brickell E F, Daveport D M. On the classification of idea secret sharing scheme. *J. Cryptology*, 1991, 4(2): 123–134.

[5] Tompa M, Woll H. How to share a secret with cheaters. *J. Cryptology*, 1988, 1(2): 133–138.

[6] Chor B, Goldwasser S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. Proceedings of the 26th Annual IEEE Symposium on the Foundations of Computer Science, 1985: 383–395.

[7] Stadler M. Publicly verifiable secret sharing. Advances in Cryptology-Eurocrypt'96, Berlin: Springer-Verlag, 1996: 190–199.

[8] Gennaro R, Micali S. Verifiable secret sharing as secure computation. Advances in Cryptology-Crypto'94. Berlin: Springer-Verlag, 1995: 168–182.

何业锋： 女， 1979 年生，硕士生，感兴趣的领域包括网络安全与保密、秘密共享、数字签名等.

张建中： 男， 1960 年生，工学博士，教授，硕士生导师，目前主要从事信息安全、信息认证、网络安全与保密、密码协议等领域的研究工作.