

文章编号:1001-9081(2009)01-0172-03

可验证的多等级门限多秘密共享方案

毛颖颖^{1,2}, 毛 明², 张艳硕^{2,3}

(1. 西安电子科技大学 通信工程学院, 西安 710071; 2. 北京电子科技学院 信息安全系, 北京 100070;

3. 中国科学院 数学机械化重点实验室, 北京 100190)

(maoyy@besti.cn)

摘 要: 目前的多等级门限共享方案中, 高等级用户的作用可以被若干个低等级用户联合取代, 而多秘密门限共享方案中, 所有秘密只能在同一级门限下共享。为克服这两个问题, 利用 Birkhoff 插值法和离散对数的困难性, 提出了一个可认证的多等级门限多秘密共享方案。该方案可以同时划分多个等级, 而每级门限下可以共享多个秘密。每个参与者只需持有一个子秘密, 方便管理与使用。

关键词: 多等级; 多秘密; 门限共享; 可验证; 离散对数

中图分类号: TP309.2; TN918 **文献标志码:** A

Verifiable hierarchical threshold multi-secret sharing scheme

MAO Ying-ying^{1, 2}, MAO Ming², ZHANG Yan-shuo^{2, 3}

(1. Institute of Communication Engineering, Xidian University, Xi'an Shaanxi 710071, China;

2. Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China;

3. Key Laboratory of Mathematics Mechanization, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: In the current multi-level secret sharing scheme, the presence of higher-level participants could be replaced by several lower-level participants. As to the multi-secret sharing scheme, secrets could only be shared under the same level. To eliminate the two limitations, based on Birkhoff Interpolation and the intractability of discrete logarithm, a new verifiable hierarchical threshold multi-secret sharing scheme was proposed. This scheme simultaneously maintained multiple levels and multiple secrets for every threshold level. Every participant kept one sub-secret only, which was convenient to manage and use.

Key words: hierarchical; multi-secret; threshold secret sharing; verifiable; discrete logarithm

0 引言

秘密共享是保密通信中保护密钥的重要手段。文献[1-2]分别提出了 (t, n) 门限秘密共享方案, 在一个共有 n 个参与者的系统中, 参与者以各自拥有不同子秘密的方式来分享秘密, t 个以上的参与者合作可以恢复秘密。

门限共享自诞生后得到了广泛的研究与应用, 近年来, 研究方向主要集中在防欺诈^[3-5]和多秘密^[6-9]共享等方面。而多等级多秘密共享的门限方案却较少被提及。实际上, 多等级多秘密相结合的门限共享具有很强的现实意义。比如在某个银行系统中, 不同等级的业务需要不同的密钥进行管理, 因而需要在多个管理人员中共享多个不同等级的秘密; 而某项重要电子业务的签署又要求至少有若干个高层管理人员的参与, 这就需要对管理人员进行等级划分。

基于这种现实要求, 本文在多等级门限共享方案^[10]的基础上, 提出一种新的可验证的多等级多秘密共享方案。通过一个多项式共享秘密, 该多项式面对不同等级的用户退化成不同的低次多项式。该方案划分了多个等级, 而每级门限下可以共享多个秘密。每个参与者只需拥有一个秘密信息就能共享多个不同等级的秘密。在恢复秘密时, 符合某等级访问结构的参与者集合可以恢复该等级及其以下等级的秘密, 而

符合较低等级访问结构的参与者集合无法恢复较高等级的秘密, 也就是说高等级用户的作用是不可替代的。方案利用离散对数困难性^[8-9]来保证系统安全。

1 多等级门限共享

文献[10]提出了一个基于 Birkhoff 插值法的多等级门限秘密共享方案。确定各级门限值 $\{k_i\}_{i=0}^m$, 构造多项式 $f(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$, a_0 为要分享的秘密。参与者属于不同的等级, 处于第 j 等级的参与者得到下列多项式的一个函数值:

$$f^{(k_{j-1})}(x) = \sum_{i=k_{j-1}}^{k-1} \left(\frac{i!}{(i-k_{j-1})!} (x)^{i-k_{j-1}} \times a_i \right) \quad (1)$$

其中: (k_{j-1}) 表示 $f(x)$ 经过了 k_{j-1} 次求导运算。令 $k_{-1} = 0$ 。最后, 满足如下访问结构的授权子集可使用 Birkhoff 插值法恢复秘密。

$$\Gamma = \{V \subset U \mid \left| V \cap \left(\bigcup_{j=0}^i U_j \right) \right| \geq k_i\} \quad (2)$$

2 多等级门限多秘密共享

本文提出一个可验证的多等级门限多秘密共享方案, 下面从系统描述, 参数初始化, 子密钥分配, 秘密恢复几个部分

收稿日期: 2008-07-25; 修回日期: 2008-09-18。

基金项目: 国家 973 计划项目 (G2004CB318000); 北京电子科技学院信息安全与保密重点实验室资助项目 (YZDJ0712)。

作者简介: 毛颖颖 (1983-), 女, 广东韶关人, 硕士研究生, 主要研究方向: 秘密共享、密码分析; 毛明 (1963-), 男, 山西稷山人, 教授, 主要研究方向: 信息安全; 张艳硕 (1979-), 男, 陕西宝鸡人, 讲师, 主要研究方向: 应用密码学、纠错编码理论。

来描述方案。

2.1 系统描述

定义函数 f , 其运算规则为自变量的指数减 1 而系数不变, 常数项则为 0, 表示为:

$$f(m + nx^p) = nx^{p-1} \quad (3)$$

例如: $f(2 + 3x + 6x^5) = 3 + 6x^4$ 。以 f 函数来取代文献[10]的求导运算。

系统中包含一个秘密分发者 D 和 n 个参与者。 n 个参与者构成集合 U , U 被划分为几个不相交的等级集合, $U = \bigcup_{i=0}^m U_i$ 。 $S = \{s_1, s_2, \dots, s_k\}$ 是共享的 k 个秘密, S 也被划分几个不相交的等级集合, $S = \bigcup_{i=0}^m S_i$, 设 $S_0 = \{s_1, s_2, \dots, s_{k_0}\}$, $S_1 = \{s_{k_0+1}, \dots, s_{k_1}\}$, $\dots, S_m = \{s_{k_{m-1}+1}, \dots, s_{k_m}\}$, 其中 $k_m = k$ 。 $T = \{t_i\}_{i=0}^m$ 是一个单调增加的整数序列, 是最高等级秘密 S_0 对应的各级门限值, 当 $0 \leq i \leq m-1$ 时, $t_i = k_i$; 而当 $i = m$ 时, $t_i \geq k_i$ 。要恢复秘密 $S_j (0 \leq j \leq m)$, 参与者集合需满足访问结构:

$$\Gamma_j = \{V \subset U \mid \left| V \cap \left(\bigcup_{l=j}^i U_l \right) \right| \geq t_i - t_{j-1}\} \quad (4)$$

$\forall i \in \{0, 1, \dots, m\}$, 约定 $t_{-1} = 0$ 。恢复秘密集合 S_0 至少需要 t 个参与者。我们将满足 Γ_j 访问结构的参与者子集称为 S_j 的授权子集, S_j 的授权子集可以恢复 S_j 中的秘密; 而任何不满足该访问结构的非授权子集不能得到任何关于秘密的信息。

2.2 参数初始化

D 选择两个满足 RSA 安全性的素数 p_1 和 p_2 , 计算 $N = p_1 p_2$ 。选择 h_0 , 使 $\gcd(h_0, \varphi(N)) = 1$, 求 h' , 使其满足 $h_0 h' = 1 \pmod{\varphi(N)}$, 其中 $\varphi(N)$ 为欧拉函数。选择大整数 $g \in [N^{\frac{1}{2}}, N]$, 计算 $H_0 = g^{h_0} \pmod{N}$ 。公开 $\{g, N, H_0, h'\}$ 。

2.3 子秘密的分配

1) 参与者 u_i 选择随机数 h_i 作为秘密份额, 计算 $H_i = g^{h_i} \pmod{N}$, 将 H_i 发送给 D 。若有 $H_i = H_j (i \neq j)$, D 可要求参与者重新选择 h_i , 直到 $H_i \neq H_j (i \neq j)$ 为止。 $I_i = H_i^{h_0} \pmod{N}$ 就是 u_i 的秘密信息, D 公开 $\{H_1, \dots, H_n\}$ 。

2) D 取大素数 q 和随机数 a_1, \dots, a_{t-k} , 构造多项式:

$$P(x) = s_1 + s_2 x + \dots + s_k x^{k-1} + a_1 x^k + \dots + a_{t-k} x^{t-1} \pmod{q} \quad (5)$$

其中: $t = t_m, t \geq k$ 。根据各参与者 u_i 所处的等级 j , 分发者为各参与者计算 $y_i = P_{k_{j-1}}(I_i)$, 其中 $P_0(x) = P(x), P_1(x) = f(P(x)), P_j(x) = f(P_{j-1}(x))$ 。 D 公开 $\{y_1, \dots, y_n\}$ 。

2.4 秘密恢复

1) 参与者 u_i 读取 (g, H_0) , 计算并出示 $I_i = H_i^{h_0} = g^{h_0 h_i} = H_0^{h_i} \pmod{N}$ 。

2) 任何人都能通过下式验证 u_i 的秘密信息是否真实。

$$I_i^{h'} = H_i \pmod{N}; i \in [1, n] \quad (6)$$

3) 现在以 S_0 的授权子集为例, 看如何恢复秘密。 V 中的参与者联合解如式(7)的方程, 即可重构多项式 $P(x)$, 恢复系统中的所有秘密。

用同样的方法, 符合访问结构 $\Gamma_j (0 \leq j \leq m)$ 的参与者集合可以重构多项式 $P_{k_{j-1}}(x)$, 从而可以恢复秘密 $S_i (j \leq i \leq m)$ 。

$$\begin{cases} s_1 + s_2 I_1 + \dots + s_k I_1^{k-1} + a_1 I_1^k + \dots + a_{t-k} I_1^{t-1} = y_1 \\ \vdots \\ s_1 + s_2 I_{i_0} + \dots + s_k I_{i_0}^{k-1} + a_1 I_{i_0}^k + \dots + a_{t-k} I_{i_0}^{t-1} = y_{i_0} \\ s_{k_0+1} + s_{k_0+2} I_{i_0+1} + \dots + s_k I_{i_0+1}^{k-k_0} + a_1 I_{i_0+1}^{k-k_0} + \dots + a_{t-k} I_{i_0+1}^{t-1-k_0} = y_{i_0+1} \\ \vdots \\ s_{k_0+1} + s_{k_0+2} I_{i_1} + \dots + s_k I_{i_1}^{k-k_0} + a_1 I_{i_1}^{k-k_0} + \dots + a_{t-k} I_{i_1}^{t-1-k_0} = y_{i_1} \\ \vdots \\ s_{k_{m-1}+1} + \dots + s_k I_{i_{m-1}+1}^{k-k_{m-1}} + a_1 I_{i_{m-1}+1}^{k-k_{m-1}} + \dots + a_{t-k} I_{i_{m-1}+1}^{t-1-k_{m-1}} = y_{i_{m-1}+1} \\ \vdots \\ s_{k_{m-1}+1} + \dots + s_k I_{i_m}^{k-k_{m-1}} + a_1 I_{i_m}^{k-k_{m-1}} + \dots + a_{t-k} I_{i_m}^{t-1-k_{m-1}} = y_{i_m} \end{cases} \quad (7)$$

3 方案分析

3.1 方案正确性证明

命题 1 若 V 是 S_j 的授权子集, V 可以恢复秘密 S_j 。

证明 设 V 是一个 S_0 的最小授权子集, 若上述方程组的系数矩阵行列式不为 0, 则方程组有且只有唯一解。如果 V 是授权子集, 但不是最小授权子集, V 中必定包含一个最小授权子集 V_0 可解出 S_0 。以 s_i, a_i 为未知数, 记上述方程组的系数矩阵为 M_V , 即:

$$M_V = \begin{bmatrix} 1 & I_1 & \dots & I_1^{k-1} & I_1^k \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & I_{i_0} & \dots & I_{i_0}^{k-1} & I_{i_0}^k \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 1 & \dots & I_{i_{m-1}+1}^{k-k_{m-1}} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 1 & \dots & I_{i_m}^{k-k_{m-1}} \end{bmatrix} \quad (8)$$

U_{k-1} 表示 M_V 去掉最后一行最后一列后得到的矩阵行列式, 显然:

$$\det(M_V) = \sum_{i=0}^{k-2-k_{m-1}} b_i I_{i_m}^i + U_{k-1} I_{i_m}^{t-1-k_{m-1}} \quad (9)$$

其中 b_i 为某个常数。 M_V 行列式为 0 的概率为:

$$\text{Prob}(\det(M_V) = 0) =$$

$$\sum \text{Prob}(\det(M_V) = 0 \mid U_{k-1} = 0) \text{Prob}(U_{k-1} = 0) + \sum \text{Prob}(\det(M_V) = 0 \mid U_{k-1} \neq 0) \text{Prob}(U_{k-1} \neq 0) \quad (10)$$

1) 如果 $U_{k-1} \neq 0$, I_{i_m} 最多有 $t-1-k_{m-1}$ 个不同的取值可使 $\det(M_V) = 0$, 则有:

$$\text{Prob}(\det(M_V) = 0 \mid U_{k-1} \neq 0) \leq \frac{t-1-k_{m-1}}{(q-1)-(k-1)} \quad (11)$$

当 $k_{m-1} = 0$ 时, 此数值最大, 但此时 M_V 为范德蒙矩阵, 行列式必不为 0。所以情况最糟时为 $\frac{t-2}{q-t-2}$;

2) 如果 $U_{k-1} = 0$, 那么 $\det(M_V)$ 是个 I_{i_m} 次数小于 $t-1-k_{m-1}$ 的多项式, 用归纳法可得:

$$\text{Prob}(U_{k-1} = 0) \leq \frac{(t-3)(t-2)}{2(q-t-1)} \quad (12)$$

综上所述, 有:

$$\text{Prob}(\det(M_V) = 0) \leq \frac{(t-3)(t-2)}{2(q-t-1)} + \frac{t-2}{q-t-3} \leq \frac{(t-2)(t-1)}{2(q-t)} \quad (13)$$

在实际应用中,通常 t 很小而 q 很大(例如 q 是一个128位的大素数),所以系数矩阵行列式为0的概率很小,方案是可行的。同理可证,满足访问结构 Γ_j 的用户集合 V 可以重构多项式 $P_{k_{j-1}}(x)$,从而恢复 $S_i (j \leq i \leq m)$ 中的秘密。

3.2 安全性分析

3.2.1 完善安全性证明

命题2 若参与者集合 V 人数不足, V 无法恢复秘密。

证明 不失一般性,设参与者集合 V 还差一个参与者才能成为 S_j 的授权子集。为求解秘密集合 S_j ,参与者集合 V 必须通过 $t-k_{j-1}-1$ 个方程求解 $t-k_{j-1}$ 个未知数,其中至少有1个自由变量,则 V 能得到一组正确秘密的概率最多为 $1/q$,与穷举无异,所以 V 无法恢复秘密。

命题3 若参与者集合 V 因较高等级参与者数量不足而不满足访问结构 Γ_j , V 无法恢复秘密 S_j 。

证明 现在以 S_0 的恢复为例,证明较高等级参与者数量不够时,即使参与者数量再多,也不能恢复秘密。设 $|V| \geq t$, V 中缺少等级 j 上的一个用户。也就是有 $v_1, \dots, v_{l_0} \in U_0, v_{l_0+1}, \dots, v_{l_1} \in U_1, \dots, v_{l_{m-1}+1}, \dots, v_{l_m} \in U_m$,其中 $l_i \geq t_i (0 \leq i \leq j-1), l_j = t_j - 1, l_i \geq t_i - 1 (j+1 \leq i \leq m)$ 。因为 $|V| = l_m > t-1$,有 $l_m - l_j > t - t_j$ 。低于等级 j 的用户在 M_V 的行向量中至少有 k_j 个0,所以其中 $l_m - l_j$ 行的实际维数至多为 $t - k_j$,有 $|V_0| = l_m - [(l_m - l_j) - (t - k_j)] = t - 1$,即 V 还缺少一个参与者才能恢复子秘密。同理可证,在恢复秘密 S_j 的时候,如果较高等级的参与者人数不足,哪怕参与者总数再多,也不能恢复秘密。

由命题2、3可知,任意非授权子集无法恢复秘密,方案是完善安全的。

3.2.2 方案基于离散对数困难性

1) 安全防欺诈。本方案的欺诈检测是基于离散对数问题的困难性。任何人都能通过式(4)验证自己或他人的秘密信息是否正确。

2) 防窃取秘密信息。a) 如果攻击者想通过公开信息 H_i 得到参与者 u_i 的秘密信息 I_i ,则必须解离散对数问题 $H_i = g^{h_i} \bmod N$,所以攻击者无法窃取 I_i 。b) 在恢复秘密后,攻击者想通过 u_i 出示的 I_j 得到子秘密 h_j 。那么攻击者必须解离散对数问题 $I_j = H_j^{h_0}$ 。所以攻击者无法得到 u_i 的子秘密 h_j 。c) 如果攻击者想从公开信息 H_0 和 h' 推出保密信息 h_0 ,就必须解 $H_0 = g^{h_0} \bmod N$,或者 $h'h_0 = 1 \bmod N$,这分别是基于离散对数和RSA大数分解的困难性。所以攻击者无法从公开信息 H_0 和 h' 推出保密信息 h_0 。

综上所述,可以认为只要大整数分解问题和离散对数问题是难解的,本方案就是安全的。

4 方案优点

本方案与多秘密共享方案^[7-9]共有的优点如下:

- 1) 秘密份额与共享密钥长度一致。
- 2) 每个用户只需持有一个秘密份额就能共享多个秘密。
- 3) 一次运算能同时恢复多个秘密。
- 4) 秘密更新或增删参与者时,秘密份额可复用。
- 5) 可验证秘密分发者 D 与参与者是否可信。

本文方案独具的优势如下:

- 1) 对参与者划分等级,且高等级参与者不可替代。现有

的多级门限方案中,参与者等级虽有上下之分,但一个高等级用户的作用可被若干个低等级用户合作取代。而在本文方案中,高等级参与者的作用不可或缺、不可替代。比如参与者集合 V 符合访问结构 Γ_1 但不符合 Γ_0 ,可以恢复多项式:

$$P_{k_0}(x) = \sum_{i=k_0}^k s_{i+1} x^{i-k_0} + \sum_{j=0}^{t-1-k_0} a_{j+1} x^{j+k-k_0} \quad (14)$$

显然,其中不包含 S_0 中的秘密信息。

2) 对秘密划分等级。现有的多秘密共享只能在同一门限下共享秘密。而本文划分秘密等级,每级门限下可共享多个秘密,例如符合访问结构 Γ_j 的参与者集合可以重构多项式 $P_{k_{j-1}}(x)$,恢复 $S_i (j \leq i \leq m)$ 中的所有秘密。

3) 文献[10]方案中,处于 j 等级的参与者 u_i 得到 $P(x)$ 进行 k_{j-1} 次求导运算后的函数值,如式(1)所示。而本方案各参与者得到的秘密份额形如:

$$P_{k_{j-1}}(x) = \sum_{i=k_{j-1}}^{t-1} (x)^{i-k_{j-1}} \times c_i \quad (15)$$

其中:当 $k_{j-1} \leq i \leq k$ 时, $c_i = s_i$,当 $k+1 \leq i \leq t-1$ 时, $c_i = a_{i-k}$ 。显然,对于每一个处于第 j 等级的用户 u_i ,本论文方案比文献[10]节省了系数部分的 $(k-k_{j-1}+1) \times k_{j-1}$ 次模乘运算。同时,本方案将多项式中的一部分系数作为共享秘密,在没有添加额外存储空间和计算量的情况下,既保证高等级参与者的权威地位,又实现了多个秘密的共享。

5 结语

基于Birkhoff插值法和离散对数问题,提出了一个新的可验证的多等级多秘密共享方案。方案对参与者和共享秘密分别进行了等级划分,高等级参与者的作用不可替代,每级门限下可共享多个秘密,且每个参与者只需持有一个秘密信息,就能共享多个不同等级的秘密。方案可验证,子秘密可复用,具有重要的现实意义和应用价值。

参考文献:

- [1] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612.
- [2] BLAKLEY G R. Safeguarding cryptographic keys[C]// Proceeding of National Computer Conference '79. Montvale, USA: AFIPS Press, 1979: 313-317.
- [3] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C]// Proceedings of the 28th IEEE Symposium on Foundations of Computer Science. Washington, DC: IEEE Press, 1987: 427-437.
- [4] FUJISAKI E, OKAMOTO T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications[C]// EUROCRYPT '98: Advances in Cryptology. Berlin: Springer-Verlag, 1998: 32-47.
- [5] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]// CRYPTO '91: Advances in Cryptology. Berlin: Springer, 1991: 129-140.
- [6] SHAO JUN, CAO ZHEN-FU. A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme[J]. Applied Mathematics and Computation, 2005, 168(1): 135-140.
- [7] 黄东平,刘铎,王道顺,等.一种安全的门限多秘密共享方案[J].电子学报,2006,34(11),1937-1940.
- [8] ZHAO JIAN-JIE, ZHANG JIAN-ZHONG, ZHAO RONG. A practical verifiable multi-secret sharing scheme[J]. Computer Standards & Interfaces, 2007, 1(29): 138.
- [9] DEHKORDI M H, MASHHADI S. New efficient and practical verifiable multi-secret sharing schemes[J]. Information Science, 2008, 9(178): 2262-2274.
- [10] TASSA T. Hierarchical threshold secret sharing[J]. Journal of Cryptology, 2007, 20(2): 237-264.