一个有效的理想的多秘密共享方案*

李 婧, 李志慧†, 黑 赞
(陕西师范大学 数学与信息科学学院, 西安 710062)

摘 要: 基于单调张成方案,构造了一个有效的理想的多秘密共享方案。在这个方案中,将含有 n 个参与者的集合分割成若干个参与者子集,用来建立多重访问结构。该方案具有防欺诈性,即某个不诚实的参与者在一次密钥重构中即使得到一些参与者的共享也不能恢复其他密钥。整个方案构造过程计算量小,只用到了简单的线性运算。与文献[4,9]相比,有效地避免了模方幂等高复杂度的运算以及解线性方程组的步骤,是一个较为实用的且理想的线性的多秘密共享方案。

关键词: 理想的多秘密共享; 单调张成方案; 多重访问结构; 计算量小
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)06-2211-03
doi:10.3969/j.issn.1001-3695.2012.06.055

Efficient ideal multi-secret sharing scheme

LI Jing, LI Zhi-hui, HEI Zan
(*College of Mathematics & Information Science, Shaanxi Normal University, Xi'an* 710062, *China*)

Abstract: This paper presented an efficient ideal multi-secret sharing scheme based on MSP. This scheme, splitted a set of n participants into several subsets of participants to establish multiple access structures. It was cheat-proof, that was, after a secret was reconstructed by some participants, the dishonest participant could not recover other secrets by using those sharings he obtained. The entire scheme had the advantages of small computational cost, only using simple linear operations. Compared with [4,9], it avoided high complexity operations like exponentiation, which was a practical linear multi-secret sharing scheme.

Key words: ideal multi-secret sharing; monotone span program(MSP); multiple access structures; small computational cost

秘密共享就是在一组参与者中共享秘密,它主要用于防止重要信息丢失、被破坏、窜改或落入坏人手里,是信息安全和密码学中一个重要的研究课题,在密钥管理和电子商务等诸多领域中有着广泛地应用。自 1979 年,Shamir 和 Blakley 分别基于 Lagrange 多项式插值和射影几何理论首次提出了门限秘密共享方案后,学者们相继提出了针对一般访问结构的单秘密共享方案[1,2],针对一个访问结构的多秘密共享方案[3~6],以及针对多个访问结构的多秘密共享方案[7,8]。

Hsu 等人[9]基于单调张成方案提出了一个理想的线性多秘密共享方案(简称 HCT Z 方案)。但该方案存在两个明显的漏洞:a)基于方案访问结构的特点,恶意的参与者可能在恢复秘密时得到其他参与者的子密钥,从而破坏相应的访问结构;b)根据方案在分发阶段的描述,想要找到满足方案所给条件的向量 r 等价于解线性方程组,即 r 的存在性等价于线性方程组的可解性。但是该方案所对应的线性方程组可解与否依赖于分发者选择的密钥。于是,整个方案的可行性受到了限制。

1 HCT Z 方案

1.1 HCT Z 方案中访问结构的定义

设 $P=\{P_1,P_2,\cdots,P_n\}$ 是参与者集合,Ω 是参与者集合 P 的所有非空子集所组成的集合,$|\Omega|=m=2^{|P|}-1$。假设 $\varphi:\{1,2,\cdots,m\}\to\Omega$ 是一个双射,Ω 中每个元素(即参与者子集)分别持有一个不同的目标密钥 $s_1,s_2,\cdots,s_m$。定义 m 重访问结构 $\Gamma=(\Gamma_1,\Gamma_2,\cdots,\Gamma_m)$,其中密钥 s_j 与访问结构 Γ_j 相关,且

$$(\Gamma_j)_{\min}=\{\varphi(j)\}\quad 1\leqslant j\leqslant m \tag{1}$$

其中:$(\Gamma_j)_{\min}$ 表示 Γ_j 的极小访问结构,$(A_j)_{\max}$ 表示极大攻击者结构。很明显,一个参与者子集 $A\subseteq P$ 可能恢复不止一个密钥。例如,若参与者子集 $A\in\Gamma_i$ 且 $A\in\Gamma_j$,则 A 可以恢复密钥 s_i 和 s_j,其中 $1\leqslant i,j\leqslant m$ 且 $i\neq j$。

例 1 令 HCT Z 方案中的 $n=3$,$P=\{P_1,P_2,P_3\}$,$\Omega=\{\{P_1\},\{P_2\},\{P_3\},\{P_1,P_2\},\{P_1,P_3\},\{P_2,P_3\},\{P_1,P_2,P_3\}\}$,$m=7$,$\varphi:\{1,2,\cdots,7\}\to\Omega$,$\Gamma=(\Gamma_1,\Gamma_2,\cdots,\Gamma_7)$,$\Gamma_j$ 对应的密钥为 $s_j(1\leqslant j\leqslant 7)$。

由式(1)的定义可知:$(\Gamma_1)_{\min}=\{\{P_1\}\}$,$(\Gamma_2)_{\min}=\{\{P_2\}\}$,$(\Gamma_3)_{\min}=\{\{P_3\}\}$,$(\Gamma_4)_{\min}=\{\{P_1,P_2\}\}$,$(\Gamma_5)_{\min}=\{\{P_1,P_3\}\}$,$(\Gamma_6)_{\min}=\{\{P_2,P_3\}\}$,$(\Gamma_7)_{\min}=\{\{P_1,P_2,P_3\}\}$。

1.2 单调张成方案的介绍

Karchmer 和 Wigderson 介绍了可计算单调布尔函数的单调张成方案(MSP),记做 $M(\kappa,M,\Psi)$。其中:M 是域 κ 上的 $d\times l$ 矩阵,标号映射 $\Psi:\{1,2,\cdots,d\}\to\{P_1,P_2,\cdots,P_m\}$ 是一个满射,即把 M 的一些行分发给每个参与者。对于任意参与者子集 $A\subseteq P$,相应的特征向量 $\delta_A=(\delta_1,\delta_2,\cdots,\delta_n)\in\{0,1\}^n$,$\delta_i=1$

收稿日期: 2011-11-02; **修回日期**: 2011-12-08 **基金项目**: 国家自然科学基金资助项目(60873119)

作者简介:李婧(1986-),女,河北张家口人,硕士研究生,主要研究方向为有限域、密码学;李志慧(1966-),女(通信作者),教授,博士,主要研究方向为有限域、密码学(snnulzh6@yahoo.com.cn);黑赞(1986-),男,硕士研究生,主要研究方向为有限域、密码学.

当且仅当 $P_i \in A(1 \leqslant i \leqslant n)$。单调布尔函数 $f:\{0,1\}^n \rightarrow \{0,1\}$ 满足对任意 $A \subseteq P$ 且 $B \subseteq A, f(\delta_B)=1$ 可推出 $f(\delta_A)=1$。一个单调张成方案 $M(\kappa, M, \Psi)$ 对于目标向量 v_j 可计算单调布尔函数是指，如果 $v_j \in \text{span}\{M_A\}$ 当且仅当 $f(\delta_A)=1$，其中 M_A 是由矩阵 M 中标号为 P_i 的行所组成（这里 $P_i \subseteq A$），$v_j \in \text{span}\{M_A\}$ 是指存在向量 w 使得 $v_j = w \cdot M_A (1 \leqslant j \leqslant m)$。

1.3 HCT Z 方案回顾

Beimel 证明了设计一个基于多重访问结构 $\Gamma = (\Gamma_1, \Gamma_2, \cdots, \Gamma_m)$ 的线性多秘密共享方案等价于构造一个单调张成方案 $M(\kappa, M, \Psi)$，通过寻找线性空间 $V_i (P_i \in P)$ 使得 $\cap_{A \in (\Gamma_j)_{\min}} \sum_{P_i \in A} V_i - \cup_{B \in (A_j)_{\max}} \sum_{P_i \in B} V_i \neq \varphi (1 \leqslant j \leqslant m)$。基于这一事实，HCT Z 方案的构造有以下三步。

1.3.1 *初始化阶段*

设 $S_1 \times S_2 \times \cdots \times S_m$ 是主密钥空间（即 $s_j \in S_j, 1 \leqslant j \leqslant m$），$\kappa$ 是一个有限域，令 $S_1 = S_2 = \cdots = S_m = \kappa$，$\bar{v} = \kappa^n$ 是 κ 上的 n 维线性空间。设 $\{e_1, e_2, \cdots, e_n\}$ 是 $\bar{v}$ 的一组基，定义映射 $v: \kappa \rightarrow \bar{v}$ 为 $v(x) = \sum_{i=1}^{n} x^{i-1} e_i$。观察向量 $v(x)$ 的表达式，并由范德蒙行列式的性质可以推出，至多 n 个形如 $v(x)$ 的向量是线性无关的。设 $u_i \in \{v(x): x \in \kappa\}$ 是与参与者 P_i 相伴的一个向量，$V_i = \text{span}\{u_i\} (1 \leqslant i \leqslant n)$，其中 $u_i \neq u_j (i \neq j)$。

设 $v_j = \sum_{x_i \in \kappa}^{P_i \in \varphi(j)} x_i \cdot u_i (1 \leqslant j \leqslant m)$ 是 m 个目标向量，u_i 是分发给 P_i 的行向量。构造一个可计算单调布尔函数 $f_{\Gamma_1}, f_{\Gamma_2}, \cdots, f_{\Gamma_m}$ 的单调张成方案 $M(\kappa, M, \Psi)$，其中 M 是 κ 上的一个 $n \times n$ 的矩阵，第 i 个行向量正是 u_i（即 $\Psi(i) = P_i$），$\Gamma = (\Gamma_1, \Gamma_2, \cdots, \Gamma_m)$ 是式(1)已定义过的。

1.3.2 *分发阶段*

分发者首先随机选取一个向量 $r \in \kappa^n$ 使得内积 $(v_j, r) = s_j (1 \leqslant j \leqslant m)$，并计算 $M \cdot r^{\mathrm{T}}$，将 $M_i \cdot r^{\mathrm{T}}$ 分发给参与者 P_i，其中 r^{T} 表示 r 的转置，M_i 是标号矩阵 M 的第 i 行（即 $M_i = u_i$）。因此，参与者 P_i 得到的共享是 $M_i \cdot r^{\mathrm{T}} (1 \leqslant i \leqslant n)$。

1.3.3 *重构阶段*

对于任意参与者子集 $A \in \Gamma_j (1 \leqslant j \leqslant m)$，由于 $v_j = \sum_{x_i \in \kappa}^{P_i \in \varphi(j)} x_i \cdot u_i$，且 $\varphi(j) \subseteq A$，于是 $v_j = \sum_{P_i \in A} V_i$，故存在一个向量 w 使得 $v_j = w \cdot M_A$。因此，$s_j = (v_j, r) = v_j \cdot r^{\mathrm{T}} = (w \cdot M_A)^{\mathrm{T}} = w \cdot (M_A \cdot v^{\mathrm{T}})$，即 A 中参与者通过计算其共享的线性组合来重构密钥 s_j。

1.4 HCT Z 方案存在的安全隐患

以下所讨论的访问结构特指极小访问结构。利用该方案进行一次密钥重构时，如果在重构过程中所启用的访问结构里出现不诚实的参与者，则参与者的不诚实行为将导致一些尚未启用的访问结构失效（命题 1）。这里失效是指多秘密共享方案中尚未被启用的访问结构所对应的密钥被非授权子集恢复出来，那么这个访问结构已经失去意义。文中不诚实的参与者记做 P_i，R 表示 P_i 参与一次密钥重构之后导致失效的访问结构的数量。

命题 1 HCT Z 方案中如果出现一个不诚实的参与者 P_i，则 $R = 2^d - 1 - k$，。其中：k 是重构密钥时被启用过的且包含参与者 P_i 的访问结构的个数，d 表示遍历这些访问结构的不同参与者的个数。

证明 设上述条件中包含参与者 P_i 的这些访问结构分别为 $\Gamma_1^*, \Gamma_2^*, \cdots, \Gamma_k^*$，因此不诚实参与者 $P_i \in \bigcap_{j=1}^{k} \{P_{n_j}: P_{n_j} \in \Gamma_j^*, 1 \leqslant n_j \leqslant n\}$。此外，设集合 $F = \bigcup_{j=1}^{k} \{P_{n_j}: P_{n_j} \in \Gamma_j^*, 1 \leqslant n_j \leqslant n\} = \{P_{l_1}, P_{l_2}, \cdots, P_{l_d}\}$，即 $d = |F|$，$P_i \in F$。在 HCTZ 方案中，$\Omega = 2^P / \varphi, m = 2^n - 1, \varphi: \{1, 2, \cdots, m\} \rightarrow \Omega$ 是一个双射。设 $\Omega' = 2^F / \varphi, \Omega' \subseteq \Omega$，则 $|\Omega'| = 2^{|F|} - 1 = 2^d - 1$，因此，$F$ 中的参与者可以生成 $2^d - 1$ 个参与者子集。由 $(\Gamma_j)_{\min} = \{\varphi(j)\}$ 可知，这 $2^d - 1$ 个参与者子集对应着 $2^d - 1$ 个访问结构。于是不诚实的参与者 P_i 在密钥重构之后可获取 F 中其他参与者的共享，从而来恢复 $2^d - 1$ 个密钥。除去已启用过的 k 个访问结构 $\Gamma_1^*, \Gamma_2^*, \cdots, \Gamma_k^*$，$P_i$ 的不诚实行为将导致 $R = 2^d - 1 - k$ 个访问结构失效。

例 2 （接例 1）如果 P_1 是不诚实的参与者，当 P_1 参与了对密钥 s_4, s_5 的重构之后即可获得 P_2, P_3 的子密钥。由命题 1 可知，$k=2, F = \{P_1, P_2, P_3\} = P, d = 3, \Omega' = \Omega$，除去密钥 s_4, s_5 之外，P_1 可恢复密钥 s_1, s_2, s_3, s_6, s_7，即 $R = 2^d - 1 - k = 2^3 - 1 - 2 = 5$。如果除 P_1 外另有不诚实的参与者，$P_i (1 \leqslant i \leqslant 3$ 且 $i \neq 1)$，则 R 的值将继续累加。可以看到 HCTZ 方案中若出现不诚实的参与者，将对方案造成较大的破坏。

1.5 HCT Z 方案的不可行问题

根据本文 1.3.2 节中对 HCT Z 方案分发阶段的描述，分发者随机选取一个 n 维向量 $r \in \kappa^n$ 使得内积 $(v_j, r) = s_j (1 \leqslant j \leqslant m)$。实际上，寻找向量 $r = (r_1, r_2, \cdots, r_n)$ 等价于解一个关于 $r_1, \cdots, r_n$ 的线性方程组：

$$\begin{cases} c_{11} r_1 + c_{12} r_2 + \cdots + c_{1n} r_n = s_1 \\ \cdots \\ c_{n1} r_1 + c_{n2} r_2 + \cdots + c_{nn} r_n = s_n \\ \cdots \\ c_{m1} r_1 + c_{m2} r_2 + \cdots + c_{mn} r_n = s_m \end{cases} \tag{2}$$

其中：$m = 2^n - 1 > n$，$(c_{j1}, c_{j2}, \cdots, c_{jn}) = v_j (1 \leqslant j \leqslant m)$。由于 $v_j = \sum_{x_i \in \kappa}^{P_i \in \varphi(j)} x_i \cdot u_i$，且 $\varphi(j) = \{P_j\} (1 \leqslant j \leqslant n)$，因此，$v_1, \cdots, v_n$ 恰好是 $u_1, \cdots, u_n$ 的数乘。由于 $u_1, \cdots, u_n$ 是线性无关的，则 $v_1, \cdots, v_n$ 也是线性无关的，故方程组式(2)的前 n 个方程有唯一解。观察到 $v_j (n+1 \leqslant j \leqslant m)$ 是 $v_1, \cdots, v_n$ 的线性组合，于是要求分发者事先选择的密钥 $s_j (n+1 \leqslant j \leqslant m)$ 必须是 $s_1, \cdots, s_n$ 的线性组合，整个方程组式(2)才可解。这里 $s_1, s_2, \cdots, s_n$ 分别可以被参与者 $P_1, \cdots, P_n$ 独自恢复。因此，HCT Z 方案的可行性将受到想要共享的 m 个密钥的限制。

2 本文方案

2.1 本文方案访问结构的定义

设 $P = \{P_1, P_2, \cdots, P_n\}$ 是参与者集合，m 重访问结构 $\Gamma = (\Gamma_1, \Gamma_2, \cdots, \Gamma_m)$ 的定义如下：

$$(\Gamma_k)_{\min} = \{\{P_{i_{k-1}}, P_{i_{k-1}+1}, \cdots, P_{i_k}\}\} \tag{3}$$

其中：$i_k = t_1 + t_2 + \cdots + t_k - (k-1) (1 \leqslant k \leqslant m)$，规定 $i_0 = 1$，t_k 表示极小访问结构 $(\Gamma_k)_{\min}$ 中所含参与者的个数 $(1 \leqslant t_k \leqslant n)$，且 $t_1 + t_2 + \cdots + t_m - (m-1) = n$，特别地，$i_m = n$。

观察到 $(\Gamma_1)_{\min} = \{\{P_1, P_2, \cdots, P_{t_1}\}\}$，$(\Gamma_2)_{\min} = \{\{P_{t_1}, P_{t_1+1}, \cdots, P_{t_1+t_2-1}\}\}$，$\cdots$，$(\Gamma_m)_{\min} = \{\{P_{t_1+\cdots+t_{m-1}-[(m-1)-1]}, \cdots, P_n\}\}$，将 $(\Gamma_k)_{\min}$ 中所含的唯一的最小授权子集记做 $A_k (1 \leqslant k \leqslant m)$，即 $|A_k| = t_k$。

例 3 设 $n=7$，参与者集合 $P = \{P_1, P_2, \cdots, P_7\}$，令 $m =$

$3, t_1 = 4, t_2 = 2, t_3 = 3$, 则 $(\Gamma_1)_{\min} = \{\{P_1, P_2, P_3, P_4\}\}$, $(\Gamma_2)_{\min} = \{\{P_4, P_5\}\}$, $(\Gamma_3)_{\min} = \{\{P_5, P_6, P_7\}\}$, 其相应的最小授权子集分别是 $A_1 = \{P_1, P_2, P_3, P_4\}$, $A_2 = \{P_4, P_5\}$, $A_3 = \{P_5, P_6, P_7\}$。

2.2　本文方案的构造

设 $S_1 \times S_2 \times \cdots \times S_m$ 是主密钥空间, κ 是一个有限域, 令 $S_1 = S_2 = \cdots = S_m = \kappa$。基于 MSP 对方案的构造有以下三个步骤。

2.2.1　初始化阶段

构造一个 $n \times n$ 的上三角矩阵 M, 用 a_{ij} 表示矩阵 M 的第 i 行第 j 列元素 ($i = 1, \cdots, n; j = 1, \cdots, n$)。当 $i > j$ 时, 令 $a_{ij} = 0$。当 $i \leqslant j$ 时, a_{ij} 的定义如下:

(a) 当 $i = 1, a_{1j} = b_j$, 其中 $b_j \in \kappa$ 且 $b_j \neq 0$;

(b) 当 $i_k + 1 \leqslant i \leqslant i_{k+1} (0 \leqslant k \leqslant m-1)$),

$$a_{ij} = \begin{cases} \dfrac{a_{i_k, j}}{j - j_k} & i_k + 1 \leqslant j \leqslant i_{k+1} \\ \dfrac{a_{i_k, j}}{t_{k+1} - 1} & i_{k+1} + 1 \leqslant j \leqslant n \end{cases}$$

单调张成方案 $M(\kappa, M, \Psi)$ 中的标号映射为 $\Psi(i) = P_i$, M_i 表示矩阵的第 i 个行向量, 定义 $V_i = \text{span}\{M_i\} (1 \leqslant i \leqslant n)$, 目标向量 $v_k = (0, \cdots, 0, 1, 0, \cdots, 0) \in \kappa^n$, 其中第 i_{k-1} 个分量为 1, 其余分量均为 $0 (1 \leqslant k \leqslant m)$。

例 4(接例 3)　$n = 7$, 令 $m = 3, t_1 = 4, t_2 = 2, t_3 = 3$, M 是一个 7×7 的上三角矩阵; 目标向量为 $v_1 = (1,0,0,0,0,0,0)$, $v_2 = (0,0,0,1,0,0,0)$, $v_3 = (0,0,0,0,1,0,0) \in \kappa^7$; 矩阵 M 为

$$M = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ 0 & b_2 & \frac{b_3}{2} & \frac{b_4}{3} & \frac{b_5}{3} & \frac{b_6}{3} & \frac{b_7}{3} \\ 0 & 0 & \frac{b_3}{2} & \frac{b_4}{3} & \frac{b_5}{3} & \frac{b_6}{3} & \frac{b_7}{3} \\ 0 & 0 & 0 & \frac{b_4}{3} & \frac{b_5}{3} & \frac{b_6}{3} & \frac{b_7}{3} \\ 0 & 0 & 0 & 0 & \frac{b_5}{3} & \frac{b_6}{3} & \frac{b_7}{3} \\ 0 & 0 & 0 & 0 & 0 & \frac{b_6}{3} & \frac{b_7}{6} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{b_7}{6} \end{pmatrix}$$

显然, $v_1 = b_1^{-1}[M_1 - (M_2 + M_3 + M_4)]$, $v_2 = \left(\frac{b_4}{3}\right)^{-1} \cdot (M_4 - M_5)$, $v_3 = \left(\frac{b_5}{3}\right)^{-1} \cdot [M_5 - (M_6 + M_7)]$。

注记 1　事实上, 由访问结构及 M 的定义可得, $v_k = a_{i_{k-1}, i_{k-1}}^{-1} \cdot [M_{i_{k-1}} - (M_{i_{k-1}+1} + \cdots + M_{i_k})] (1 \leqslant k \leqslant m)$。

2.2.2　分发阶段

分发者在 κ 上秘密地选取 n 个元素, 记做 $r_1, r_2, \cdots, r_n$, 其中 $r_{i_{k-1}} = s_k (1 \leqslant k \leqslant m)$ 是想要共享的密钥。构造一个维 n 向量 $s \in \kappa^n$: $s = (r_1, r_2, \cdots, r_n) = (s_1, r_2, \cdots, r_{i_1 - 1}, s_2, r_{i_1 + 1}, \cdots, r_{i_2 - 1}, s_3, \cdots, s_m, r_{i_{m-1}+1}, \cdots, r_{i_m - 1}, r_n)$, 并计算 $M_i \cdot s^{\mathrm{T}}$, 将其分发给参与者 $P_i (1 \leqslant i \leqslant n)$。

2.2.3　重构阶段

对于任意的参与者子集 $A \in \Gamma_k$, 由访问结构的定义必有 $A_k \subseteq A (1 \leqslant k \leqslant m)$。由注记 1 知, $v_k \in \sum_{P_i \in A_k} V_i$, 容易找到一个 t_k 维向量 w 使得 $v_k = w \cdot M_{A_k}$, 其中 M_{A_k} 是由 $M_i (P_i \in A_k \subseteq A)$ 构成的 $t_k \times n$ 矩阵, 则 $s_k = v_k \cdot s^{\mathrm{T}} = (w \cdot M_{A_k}) \cdot s^{\mathrm{T}} = w \cdot (M_{A_k} \cdot s^{\mathrm{T}})$, 因此, A_k 中参与者通过计算其共享的线性组合来重构密钥 s_k, 从而参与者子集 $A \in \Gamma_k$ 可以恢复密钥 s_k。

例 5(接例 4)　$n = 7$, 令 $m = 3, t_1 = 4, t_2 = 2, t_3 = 3$, 分发者秘密选取 $r_1, r_2, r_3, r_4, r_5, r_6, r_7$, 其中 $r_1 = s_1, r_4 = s_2, r_5 = s_3$ 分别是 Γ_1、Γ_2、Γ_3 的密钥。根据本文 2.2.2 节的描述, $s = (s_1, r_2, r_3, s_2, s_3, r_6, r_7) \in \kappa^7$, P_i 得到的共享是 $M_i \cdot s^{\mathrm{T}} (1 \leqslant i \leqslant 7)$。当 $A \in \Gamma_1$ 时, $A_1 \subseteq A$, 由 $v_1 = b_1^{-1}[M_1 - (M_2 + M_3 + M_4)] = b_1^{-1} M_1 - b_1^{-1} M_2 - b_1^{-1} M_3 - b_1^{-1} M_4$ 得 $v_1 \in \sum_{P_i \in A_1} V_i$, 即存在一个向量 w 使得 $v_1 = w \cdot M_{A_1}$。于是 $s_1 = v_1 \cdot s^{\mathrm{T}} = (w \cdot M_{A_1}) \cdot s^{\mathrm{T}} = w \cdot (M_{A_1} \cdot s^{\mathrm{T}})$, 这里 $w = (b_1^{-1}, -b_1^{-1}, -b_1^{-1}, -b_1^{-1})$。当 $A \in \Gamma_2$ 或 $A \in \Gamma_3$ 时, 情况可类似分析。

3　分析与讨论

3.1　本文方案的安全性分析

本文方案的安全性是指针对访问结构 Γ_k, 任意的非授权子集都不能恢复密钥 S_k。根据本文 2.2.2 和 2.2.3 节的描述, 该方案的安全性等价于 $v_k \notin \cup_{B \in (A_k)_{\max}} \sum_{P_i \in B} V_i$, 其中 $1 \leqslant k \leqslant m$, $(A_k)_{\max}$ 是相对访问结构 Γ_k 的极大访问结构, B 表示非授权子集。

命题 2　假设 $\Gamma = (\Gamma_1, \Gamma_2, \cdots, \Gamma_m)$, $\kappa, M_i, V_i (1 \leqslant i \leqslant n)$ 如本文 2.2 节所定义, 且 $B \in (A_k)_{\max}$, 则 $v_k \notin \cup_{B \in (A_k)_{\max}} \sum_{P_i \in B} V_i$ $(1 \leqslant k \leqslant m)$。

证明　由于本文方案中所构造的上三角矩阵 M 所对应的行列式 $|M| \neq 0$, 因此矩阵 M 的行向量 $M_1, M_2, \cdots, M_n$ 是线性无关的。进一步, 由 $V_i = \text{span}\{M_i\} (1 \leqslant i \leqslant n)$ 和 $A_k \notin (A_k)_{\max} (1 \leqslant k \leqslant m)$ 可得, 线性空间 $\sum_{P_i \in B} V_i$ 中不存在 v_k 的线性组合。否则, $v_k = \sum_{\substack{P_i \in B \\ x_i \in \kappa}}^{P_i \in B} x_i \cdot M_i$, 且 $v_k = a_{i_{k-1}, i_{k-1}}^{-1} \cdot [M_{i_{k-1}} - (M_{i_{k-1}+1} + \cdots + M_{i_k}]$, 由此可得 $M_1, M_2, \cdots, M_n$ 线性相关, 于是推出矛盾, 故 $v_k \notin \sum_{P_i \in B} V_i$, $v_k \notin \cup_{B \in (A_k)_{\max}} \sum_{P_i \in B} V_i (1 \leqslant k \leqslant m)$。

3.2　本文方案的防欺诈性分析

以下所讨论的访问结构特指极小访问结构。由本文方案访问结构的定义可知, $(\Gamma_k)_{\min}$ 中只有一个授权子集 $A_k (1 \leqslant k \leqslant m)$, 且 $A_{k-1} \cap A_k = \{P_{i_{k-1}}\}$, 本文方案不存在 HCTZ 方案中的安全隐患。事实上, 若新方案中出现不诚实的参与者 $P_i (1 \leqslant i \leqslant n)$, 他至多属于两个相邻的访问结构。因此, p_i 在参与密钥重构之后, 至多得到两个相邻的访问结构中所含参与者的共享。设这两个相邻的访问结构分别为 $(\Gamma_{k-1})_{\min}$ 和 $(\Gamma_k)_{\min}$, A^* 是这两个相邻的访问结构中所有参与者组成的集合, 由于 A^* 不包含 A_j, 即 $A^* \notin \Gamma_J (1 \leqslant j \leqslant m$ 且 $j \neq k-1, k)$, 故 P_i 无法恢复除 s_{k-1} 和 s_k 以外的其他密钥。因此, 该方案不存在由某个参与者不诚实的行为而造成访问结构失效的问题。

例 6(接例 5)　若参与者集合中 P_1 是不诚实的参与者, 则 P_1 参与了对密钥 s_1 的重构之后, 即可得到 P_2, P_3, P_4 的共享, $A^* = \{P_1, P_2, P_3\}$, 而 A^* 不包含 A_2 和 A_3, 即 $A^* \notin \Gamma_2$ 且 $A^* \notin \Gamma_3$, 所以 P_1 无法恢复密钥 s_2, s_3; 如果 P_4 是不诚实的参与者, 他参与了对密钥 s_1 和 s_2 的重构之后, 即可得到 P_1, P_2, P_3, P_5 的共享, $A^* = \{P_1, P_2, P_3, P_4, P_5\}$, 而 A^* 不包含 A_3, 即 $A^* \notin \Gamma_3$, 故 P_4 仍无法恢复密钥 s_3。

注记 2　针对本文的方案, 可以进一步利用离散对数的困难问题为方案增加可验证性, 从而防止不诚实的参与者出示假共享。

(下转第 2231 页)

(上接第 2213 页)

3.3 本文方案的可行性分析

本文方案在分发阶段将 $M_i \cdot s^T$ 发送给参与者 $P_i(1 \leqslant i \leqslant n)$,其中 s 是由分发者事先秘密选定的,无须解方程组。因此,该方案可有效地避免解线性方程组的运算,尤其避免了因方程组无解而导致方案不可行的问题。

4 结束语

本文基于单调张成方案设计了一个有效的理想的多秘密共享方案,其中参与者集合是 $P = \{P_1, P_2, \cdots, P_n\}$。方案的 m 重访问结构中的参与者按顺序具有首尾相接的特点,有效地防止了欺诈行为。整个方案构造过程简单,计算量小,是一个理想的线性的多秘密共享方案。

参考文献:

[1] DING Yang, HUANG Rong-sheng. A new secret sharing scheme from linear code [J]. Machine Learning and Cybernetics, 2009, 6: 3204-3208.

[2] QIN Hua-wang, DAI Yue-wei, WANG Zhi-quan. A secret sharing based on (t,n) threshold and adversary structure [J]. International Journal of Information Security, 2009, 8(5): 379-385.

[3] ZHAO Jian-jie, ZHANG Jian-zhong, ZHAO Rong. A practical verifiable multi-secret sharing scheme[J]. Computer Standards & Interfaces, 2007, 29(1): 138-141.

[4] DEHKORDI M H, MASHHADI S. An efficient threshold verifiable multisecret sharing [J]. Computer Standards & Interfaces, 2008, 30(3): 187-190.

[5] DEHKORDI M H, MASHHADI S. New efficient and practical verifiable multi-secret sharing schemes[J]. Information Sciences, 2008, 178(9): 2262-2274.

[6] ALVAREZ G, ENCINAS L H, REY A M. A multisecret sharing scheme for color images based on cellular automata[J]. Information Sciences, 2008, 178 (22): 4382-4395.

[7] DAS A, ADHIKARI A. An efficient multi-use multi-secret sharing scheme based on hash function [J]. Applied Mathematics Letters, 2010, 23(9): 993-996.

[8] XIAO Liang-liang, LIU Mu-lan. Linear multi-secret sharing schemes [J]. Science in China Series F, 2005, 48(1): 125-136.

[9] HSU C F, CHANG Qi, TANG Xue-ming, *et al*. An ideal multi-secret sharing scheme based on MSP[J]. Information Sciences, 2011, 181 (7): 1403-1409.