计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(5):276−281 [doi: 10.15888/j.cnki.csa.007904]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

一种安全的多使用门限多秘密共享方案①

张　剑[1,2], 林昌露[1,2], 丁　健[1,2], 林修慧[1,2], 李朝珍[1,2]

[1](福建师范大学 数学与信息学院, 福州 350117)
[2](福建师范大学 福建省网络安全与密码技术重点实验室, 福州 350007)
通讯作者: 林昌露, E-mail: cllin@fjnu.edu.cn

摘　要: 在多秘密共享方案中, 通常会生成大量公开值来保障多个秘密安全正确地重构, 同时参与者也需要保存大量信息. 为减少公开值的个数以及参与者所需保存的信息量, 本文基于中国剩余定理和 Shamir(t, n)-门限秘密共享方案设计了一个子秘密可多使用的门限存取结构多秘密共享方案. 根据中国剩余定理将多项式产生的子秘密信息进行聚合生成公开值, 减少了公开值的个数; 应用转换值的方法和离散对数对参与者子秘密信息进行保护. 构造了具有以下特点的多秘密共享方案: 可一次共享多个秘密; 不同的秘密可对应不同门限的存取结构; 参与者可验证所恢复秘密值的正确性; 公开值个数更少; 参与者存储一个子秘密且子秘密可以多次使用.

关键词: 秘密共享; 中国剩余定理; 门限存取结构; 可验证性; 多秘密

引用格式: 张剑,林昌露,丁健,林修慧,李朝珍.一种安全的多使用门限多秘密共享方案.计算机系统应用,2021,30(5):276–281. http://www.c-s-a.org.cn/1003-3254/7904.html

Secure Multi-Use Threshold Multi-Secret Sharing Scheme

ZHANG Jian[1,2], LIN Chang-Lu[1,2], DING Jian[1,2], LIN Xiu-Hui[1,2], LI Chao-Zhen[1,2]

[1](College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China)
[2](Fujian Provincial Key Lab of Network Security & Cryptology, Fujian Normal University, Fuzhou 350007, China)

Abstract: In a multi-secret sharing scheme, a large number of public values are generated to ensure the secure and correct reconstruction of multi-secrets, and participants also need to keep a large amount of information. In order to reduce the number of public values and the information that participants should keep, this study designs a multi-secret sharing scheme based on the Chinese Remainder Theorem (CRT) and Shamir (t, n)-threshold secret sharing scheme in which shares can be used more than once. Specifically, the shares generated by polynomials are aggregated to generate public values by CRT, which reduces the number of public values. Transformed value and discrete logarithms are used to protect the shares of participants. In a multi-secret sharing scheme, multiple secrets can be shared at one time; different secrets can be shared in access structures with different thresholds; participants can verify the secrets recovered; the number of public values is fewer; each participant only needs to store one share which can be used repeatedly.

Key words: secret sharing; Chinese Remainder Theorem (CRT); threshold access structure; verifiability; multi-secret

秘密共享是网络通信中保护信息隐私性和安全性的一种非常有效的密码技术, 通过秘密共享技术可以实现将秘密信息共享给多个参与者. 1979 年, Shamir[1] 和 Blakley[2] 最先分别提出了门限秘密共享的概念. Shamir 则是利用有限域上的多项式设计的秘密共享方案, 而 Blakey 利用超几何问题构造了秘密共享方案.

① 基金项目: 国家自然科学基金 (U1705264); 福建省自然科学基金 (2019J01275); 广西可信软件重点实验室研究课题 (KX202039)
Foundation item: National Natural Science Foundation of China (U1705264); Natural Science Foundation of Fujian Province (2019J01275); Research Project of Guangxi Key Laboratory of Trusted Software (KX202039)
收稿时间: 2020-09-18; 修改时间: 2020-10-13; 采用时间: 2020-10-16; csa 在线出版时间: 2021-04-28

Benaloh 和 Leichter[3], Ito 等[4] 分别提出基于授权集和非授权集的秘密共享方案, 实现了一般存取结构上的秘密共享. 为了防止秘密共享中参与者的欺骗行为, Chor 等[5] 提出了可验证的秘密共享方案, 之后 Stadler[6] 提出了公开可验证秘密共享方案. 通常的秘密共享方案中, 秘密分发者将秘密分为多份子秘密, 并按照一定的分发方式发送给参与者, 使得授权集中的参与者联合时可以恢复秘密, 非授权集中的参与者联合时不能恢复秘密. 这些秘密共享方案均为单秘密的共享方案, 执行一次共享算法只能共享一个秘密, 但实际中经常需要共享多个秘密, 若采用这些共享方案则需要多次执行共享算法, 从而使计算、存储和通信等方面的效率降低.

由于单秘密共享方案的局限性, 使得众多学者提出并研究多秘密共享. 1994 年, He 和 Dawson[7] 基于单向函数提出了一个多阶段的(t,n)-门限多秘密共享方案, 执行一次共享算法可共享多个秘密, 但该方案被 Geng 等[8] 证明子秘密不是多次使用的, 恢复全部的秘密后, 参与者所保存的子秘密信息完全泄露, 即子秘密是一次性的. Shao[9] 基于多项式方法提出了共享k个秘密的(k,t,n)-门限多秘密共享方案, 只需少量的公开值即可, 但该方案实现的多秘密共享在秘密恢复阶段所有秘密同时恢复, 若参与者在保护秘密方面有疏漏, 则有可能会造成秘密信息的泄露. Wang 等[10] 提出了一个可验证的门限多秘密共享方案, 该方案在实现 Shao 方案[9] 功能的基础上增加了参与者对分发者的验证以及参与者之间的验证功能, 并且子秘密可重复使用. 很多学者对可验证秘密共享方案进行研究, 曹阳等[11] 提出了一种基于大整数分解可公开验证的秘密共享方案, 彭咏等[12] 研究了一类基于格的可验证秘密共享方案. Harn 和 Hsu[13] 提出了基于双线性多项式的(t,n)-门限多秘密共享方案, Zhang 等[14] 证明了该方案在恢复一个秘密之后, 其余未恢复的秘密可由$t-1$个参与者进行重构得到, 同时对其进行改进, 提出了新的秘密共享方案并解决了 Harn 和 Hsu[13] 方案中的安全隐患. 这些方案实现的多秘密共享对应的存取结构为单一门限的门限存取结构, 事实上在不同的存取结构中共享多个秘密具有更强的实用性, 因此有很多学者研究了关于多存取结构的多秘密共享方案.

2007 年, Geng 等[8] 在 He 和 Dawson 方案[7] 的基础上进行改进, 提出了多存取结构上参与者子秘密可多次使用的门限多秘密共享方案, 使得参与者子秘密在恢复一轮多秘密之后, 子秘密的信息仍是保密的, 从而子秘密具有可多次使用的性质. 为了防止参与者在秘密恢复时的不诚实行为, Chen 等[15] 提出了一个可验证的门限多秘密方案, 该方案可对参与者发送的子秘密进行验证, 防止参与者的欺骗行为, 但子秘密不具有多次使用的性质. Mashhadi[16] 基于线性反馈移位寄存器提出了一个多步的秘密共享方案, 该方案在秘密重构阶段可采用求解范德蒙方程和计算 Lagrange 插值两种方法进行秘密恢复, 但秘密恢复必须按照固定的顺序进行. Zarepour-Ahmadabadi 等[17] 提出一个具有可信第三方的渐进门限秘密共享方案, 多个秘密按照预设的顺序进行重构, 并且每个秘密对应不同的存取结构, 若秘密恢复顺序为$S_1,S_2,\cdots,S_k$, 对应的门限值逐渐变大, 即S_1门限值最小, S_k门限值最大. 该方案与前面几个多秘密方案相比公开值最少, 但该方案需要借助可信第三方实现多秘密共享, 参与者存储的子秘密包含两部分, 且子秘密不具有多次使用的性质. 考虑多秘密方案在公开值个数、多秘密恢复的顺序性、存取结构的多样性以及子秘密的多使用性等方面存在的问题, 本文提出一个更加高效的多秘密共享方案, 具有如下特点:

(1) 参与者存储的子秘密只有一份;

(2) 参与者的子秘密可多次使用;

(3) 不同的秘密对应不同的存取结构;

(4) 秘密重构时可按任意顺序进行恢复;

(5) 实现多秘密的公开值个数少.

本文应用中国剩余定理, 将其作为公开值聚合的工具来减少公开值的个数, 基于多项式的方法提出了一个子秘密可多次使用的门限多秘密共享方案, 其中参与者只需存储一个子秘密即可, 同时公开值的个数与其他方案相比也是最少的, 并且不同的秘密可对应不同的门限值, 在秘密恢复时可以按照任意的顺序进行秘密的重构, 不需要按照特定的顺序, 具有更好的灵活性.

文中剩余部分按照如下安排: 第 1 节介绍相关的预备知识; 第 2 节介绍方案的具体构造以及方案的安全性分析; 第 3 节对几个多秘密共享方案进行比较分析; 第 4 节是方案的总结.

1 预备知识

这一部分将分别对存取结构, 中国剩余定理, 离散对数问题和 Shamir (t,n)-门限秘密共享方案等内容进行简单的介绍.

1.1 存取结构

设 n 个参与者的集合为$\mathcal{P}=\{P_1,P_2,\cdots,P_n\}$, 存取结构$\Gamma(\subset 2^{\mathcal{P}})$为$\mathcal{P}$的一族可以恢复出秘密 S 的子集的集合, 这些集合称为授权集, $2^{\mathcal{P}}$为$\mathcal{P}$的幂集. 不能恢复出秘密的参与者集合为非授权集, 所有非授权集的集合为非存取结构, 记作$\bar{\Gamma}=2^{\mathcal{P}}-\Gamma$.

存取结构 Γ 具有单调性, 即:

$$A\in\Gamma, A\subset A'\Rightarrow A'\in\Gamma.$$

对于一个(t,n)-门限秘密共享方案而言, 任意大于等于 t 个参与者可恢复秘密 S, 任意小于 t 个参与者不能恢复秘密 S, 即其存取结构为$\Gamma=\{A\subset\mathcal{P}||A|\geq t\}$.

若一个秘密共享方案满足:

(1) 正确性: 对于$\forall A\in\Gamma$, A 中参与者的子秘密联合可正确恢复出秘密 S;

(2) 安全性: 对于$\forall B\in\bar{\Gamma}$, B 中的参与者联合不能得到关于秘密 S 的任何信息.

则称该方案为完备的秘密共享方案[18].

1.2 中国剩余定理

中国剩余定理 (Chinese Reminder Theorem)[19] 又称孙子定理, 简记为 CRT, 是中国古代求解一次同余式的方法. 中国剩余定理基本内容表述如下:

随机选择两两互素的整数$m_1,m_2,\cdots,m_n$, 对于任意的整数$r_1,r_2,\cdots,r_n$, 满足$r_i\in\mathbb{Z}_{m_i}(i=1,2,\cdots,n)$, $\mathbb{Z}_{m_i}$为整数模m_i的剩余类群. 则下列同余方程组:

$$\begin{cases}Y=r_1(\bmod m_1)\\Y=r_2(\bmod m_2)\\\quad\vdots\\Y=r_n(\bmod m_n)\end{cases}$$

在模 M 下有唯一解$Y=\sum_{i=1}^{n}r_i\cdot M_i\cdot b_i\ (\bmod M)$, 其中, $M=\prod_{i=1}^{n}m_i, M_i=M/m_i, b_i=M_i^{-1}\ (\bmod m_i)$, 记为$Y=CRT(r_1,r_2,\cdots,r_n)$.

1.3 离散对数问题

设$\mathbb{F}_q$为有限域, q为一个素数, g为乘法群$\mathbb{F}_q^*$中的生成元, 任取一个整数 k, 则计算$a=g^k\ (\bmod q)$可知$a\in\mathbb{F}_q$. 反之, 已知$a\in\mathbb{F}_q$, 要计算$k=\log_g a\ (\bmod q)$, 称为离散对数问题[20].

由于对一般阶数较大的有限域上离散对数问题至今没有一个高效的求解算法, 所以在密码方案的构造过程中, 总是假设在有限域上求解离散对数问题是困难的.

1.4 Shamir (t,n)-门限秘密共享方案

Shamir (t,n)-门限秘密共享方案[1] 根据门限值t构造$t-1$次多项式, 将秘密$p>n$ (p 为大素数, $p>n$) 作为常数项, 计算 n 个点处的函数值作为 n 个参与者的子秘密. 将秘密拆分为 n 份并发送给 n 个参与者$P_1,P_2,\cdots,P_n$, 使得任意大于等于 t 个参与者可以重构出秘密 S, 任意少于 t 个参与者不能得到秘密 S 的任何信息. 具体秘密分发及重构过程如下:

秘密分发阶段:

(1) 分发者 D 选择一个$t-1$次多项式

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1}\quad(\bmod p),$$

其中, $a_0=S$为秘密值, $a_1,a_2,\cdots,a_{t-1}$为随机选择的$\mathbb{F}_p$中的元素;

(2) D 计算$f(i)$作为参与者$P_i(i=1,2,\cdots,n)$的子秘密, 并通过安全信道分别发送给对应的参与者.

秘密重构阶段:

(3) 不妨假设进行秘密重构的参与者为$P_1,P_2,\cdots,P_t$, 分别将子秘密$f(1),f(2),\cdots,f(t)$安全地发送给秘密重构者 C;

(4) 秘密重构者 C 根据 Lagrange 插值公式计算得到秘密:

$$S=\sum_{i=1}^{t}f(i)\prod_{j=1,j\neq i}^{t}\frac{j}{j-i}\quad(\bmod p).$$

Shamir (t,n)-门限秘密共享方案满足:

(1) 任意大于等于 t 个参与者可以根据 Lagrange 插值公式重构出多项式$f(x)$, 从而可正确恢复出秘密 S, 满足正确性;

(2) 任意少于 t 个参与者无法重构出多项式$f(x)$, 因此无法重构得到关于秘密 S 的任何信息, 满足安全性条件.

因此, Shamir (t,n)-门限方案是完备秘密共享方案.

2 方案构造与分析

本节介绍方案的具体构造, 证明了方案的正确性和安全性、子秘密可多次使用性. 设 k 个秘密为$S_1,S_2,\cdots,S_k\in\mathbb{F}_p$, 每个秘密$S_j(j=1,2,\cdots,k)$对应的存取结构为门限值为$t_j$的门限存取结构, 即$\Gamma_j=\{A\subset\mathcal{P}||A|\geq t_j\}$. 本文选择转换值的方法进行秘密隐藏, 同时根据 Shamir (t,n)-门限方案的分发算法为参与者提供伪子秘密, 引

入中国剩余定理将多项式生成的 n 个函数值进行聚合作为公开值, 从而达到最大程度减少公开值个数的目的.

2.1 具体构造

分发者选取素数 p 和两两互素的正整数$m_1,m_2,\cdots,m_n$, 使得$m_i \geq p(i=1,2,\cdots,n)$. 选择满足$p|(q-1)$的素数 q, 取$\mathbb{F}_q$的 p 阶元 g, 以及公开的单向 Hash 函数$h(\cdot)$.

随机选择$x_1,x_2,\cdots,x_n \in \mathbb{F}_p^*$为参与者$P_1,P_2,\cdots,P_n$的公开信息. 对秘密$S_j(j=1,2,\cdots,k)$的共享如下:

(1) 秘密分发阶段

分发者进行如下操作:

① 随机选择元素$a_j,a_{j,1},a_{j,2},\cdots,a_{j,t_j-1} \in \mathbb{F}_p$, 构造多项式:

$$f_j(x)=a_j+a_{j,1}x+a_{j,2}x^2+\cdots+a_{j,t_j-1}x^{t_j-1}\ (\mathrm{mod}\ p);$$

② 计算$f_j(x)$在$x_1,x_2,\cdots,x_n$处的值$f_j(x_1),f_j(x_2),\cdots,f_j(x_n)$, 并根据中国剩余定理计算公开值:

$$PS_j=\mathrm{CRT}(f_j(x_1),f_j(x_2),\cdots,f_j(x_n));$$

③ 根据 g 与随机值a_j, 计算$g^{a_j}\ (\mathrm{mod}\ p)$, 计算并公开转换值$V_j=S_j\oplus g^{a_j}$, 这里$\oplus$为比特的异或运算;

④ 将m_i作为子秘密通过安全信道发送给参与者$P_i,i=1,2,\cdots,n$, 计算并公开秘密S_j的 Hash 值$h_j=h(S_j)$.

(2) 秘密重构阶段

任意t_j个参与者$P_{j_1},P_{j_2},\cdots,P_{j_{t_j}}$要重构秘密$S_j$, 参与重构的参与者$P_{j,i}(i=1,2,\cdots,t_j)$发送伪子秘密$SH_{j,i}(i=1,2,\cdots,t_j)$给恢复者, 由恢复者进行秘密的计算. 参与者和恢复者分别进行以下操作:

① 参与者: 参与秘密重构的参与者$P_{j,i}(i=1,2,\cdots,t_j)$根据公开值$PS_j$计算$f_j(x_{j,i}) \equiv PS_j \left(\mathrm{mod}\, m_{j,i}\right)$, 之后计算伪子秘密$SH_{j,i} \equiv g^{f_j(x_{j,i})}\ (\mathrm{mod}\ p)$并发送给恢复者.

② 恢复者: 根据参与者发送的伪子秘密, 恢复者计算:

$$g^{a_j} \equiv \prod_{i=1}^{t_j}\left(g^{SH_{j,i}}\right)^{b_i}\ (\mathrm{mod}\ p)$$

其中, $b_i=\prod\limits_{k=1,k\neq i}^{t_j}\dfrac{x_{j,k}}{x_{j,k}-x_{j,i}}$. 再根据转换值$V_j$计算$S_j=V_j\oplus g^{a_j}$恢复秘密$S_j$, 并将秘密$S_j$返回给参与重构的全部参与者.

(3) 秘密验证阶段

参与者收到恢复者发送的秘密S_j时, 可通过验证等式$h(S_j)\stackrel{?}{=}h_j$是否成立来判断所恢复秘密的正确性.

2.2 方案分析

本文方案的安全性与 Shamir (t,n)-门限方案的安全性一致, 同时方案的构造是基于中国剩余定理的性质和有限域上离散对数求解的困难性. 定理 2.1 证明了方案的正确性、安全性, 定理 2.2 分析了子秘密的可多次使用性.

定理 2.1. 在共享秘密S_j时, 本文构造的方案是安全的(t_j,n)-门限秘密共享方案.

证明: 分别从门限方案的正确性和安全性证明本文的方案是一个完备的秘密共享方案:

(1) 正确性: 任意大于等于t_j个参与者可以正确恢复出秘密S_j;

(2) 安全性: 任意少于t_j个参与者无法得到关于秘密S_j的任何信息.

方案正确性: 在进行秘密重构时, 任意至少t_j个参与者参与, 根据公开值PS_j与子秘密分别进行计算$f_j(x_{j,i}) \equiv PS_j(\mathrm{mod}\, m_{j,i})$, $i=1,2,\cdots,t_j$, 再计算伪子秘密$SH_{j,i} \equiv g^{f_j(x_{j,i})}\ (\mathrm{mod}\ p)$发送给恢复者. 恢复者根据参与者发送的信息计算:

$$\begin{aligned}\prod_{i=1}^{t_j}(SH_{j,i})^{b_i}(\mathrm{mod}\ p)&=\prod_{i=1}^{t_j}\left(g^{f_j(x_{j,i})}\right)^{b_i}(\mathrm{mod}\ p)\\&=g^{\sum_{i=1}^{t_j}f_j(x_{j,i})b_i}(\mathrm{mod}\ p)\\&=g^{a_j}(\mathrm{mod}\ p)\end{aligned}$$

再根据公开信息中S_j对应的转换值V_j, 恢复者可进行比特的异或运算$S_j=V_j\oplus g^{a_j}$从而恢复秘密S_j.

方案安全性: 对于不同的秘密$S_u,S_v(u\neq v)$, 分别对应不同的公开转换值$V_u=S_u\oplus g^{a_u},V_v=S_v\oplus g^{a_v}$, 这里$a_u,a_v$均为分发者构造多项式选取的随机值. 因此, 不同的秘密重构时是相互独立的, 当参与者恢复秘密S_u时, 不能得到关于秘密S_v的任何信息.

假设$P_1,P_2,\cdots,P_{t_j-1}$想重构秘密S_j, 包含秘密S_j部分信息的只有参与者提供的伪子秘密$g^{f_j(1)},g^{f_j(2)},\cdots,g^{f_j(t_j-1)}$. 由于$f_j(x)$为$t_j-1$次多项式, 故只有$t_j-1$个参与者时, 只能构造$t_j-1$个方程, 无法计算多项式$f_j(x)$, 从而不能计算得到$g^{a_j}$. 又因为$S_j=V_j\oplus g^{a_j}$, 所以任意$t_j-1$个参与者不能得到秘密$S_j$的任何信息.

设参与者P_{i1}的子秘密为m_{i1}, 参与者P_{i2}的子秘密为m_{i2}, 根据中国剩余定理的性质, 由于参与者P_{i1}无法得到参与者P_{i2}的子秘密m_{i2}, 因此不能由秘密S_j的公开值PS_j得到$f_j(x_{i2})$, 即不能得到对应的伪子秘密SH_{ji2}. 从而只有当参与者个数达到门限值t_j才能得到至少t_j个伪子秘密进行秘密重构, 从而恢复秘密S_j.

定理 2.2. 本文构造的方案中, 参与者的子秘密具有安全性; 在秘密重构阶段不会泄露参与者保存的子秘密信息, 子秘密具有重复使用性.

证明: 在重构秘密S_j时, 参与者P_i根据公开值计算$f_j(x_i) \equiv PS_j \pmod{m_i}$, 若攻击者能够得到参与者$P_i$的多个信息$f_{j1}(x_i),\cdots,f_{jl}(x_i)$, 即有同余方程组:

$$\begin{cases} f_{j1}(x_i) = PS_{j1} \pmod{m_i} \\ f_{j2}(x_i) = PS_{j2} \pmod{m_i} \\ \quad\vdots \\ f_{jl}(x_i) = PS_{jl} \pmod{m_i} \end{cases}$$

可以得到关于参与者P_i的子秘密m_i的部分信息, 甚至得到子秘密m_i. 但本方案中参与者发送给秘密恢复者的伪子秘密为$SH_{j,i} \equiv g^{f_j(x_i)} \pmod{p}$, 由于求解有限域上离散对数问题是困难问题, 根据伪子秘密$SH_{j,i}$无法求解$f_j(x_i)$, 因此攻击者无法得到与参与者P_i在秘密重构阶段产生的$f_j(x_i)$任何信息, 进而无法获取上述同余方程组, 保证了参与者的子秘密m_i在秘密重构阶段的私密性. 因此参与者的子秘密具有可重复使用性, 若再次执行秘密共享方案, 可不改变参与者的子秘密, 仍能进行安全的多秘密共享. 从而减少子秘密分发时产生的通信量, 并且参与者无需增加信息的存储量.

3 方案比较

本文构造的方案中应用中国剩余定理作为聚合生成公开值的工具, 将根据 Shamir(t,n)-门限方案生成的 n 个伪子秘密进行聚合产生一个公开值. 因此 k 个秘密对应产生 k 个聚合的公开值以及 k 个转换值, 只需要 $2k$ 个公开值即可共享多个秘密, 在分发多秘密时, 每个参与者只需存储一个子秘密即可, 并且参与者所存储的子秘密可多次使用. 同时每个秘密可对应不同的存取结构, 实现了多存取结构的秘密共享. 在秘密恢复阶段, 本文的方案不需要按照固定顺序进行秘密重构, 在需要恢复哪个秘密时, 根据对应的公开值进行重构即可. 因此可以减少一次性重构全部秘密和固定顺序重构秘密带来的安全隐患.

表 1 中对比的 3 个方案均为子秘密可多使用的多秘密共享方案. 其中 Geng 等的方案[8] 应用单向函数以及离散对数问题, 保护子秘密的安全性, 但所产生的公开值个数为n^2, 同时该方案中的秘密值是根据构造的多项式常数项求模指数运算得到的, 不具有一般性. Wang 等的方案[10] 利用 RAS 算法实现, 参与者参与重构秘密时, 根据子秘密计算一个伪子秘密发送给重构者, 通过伪子秘密无法计算子秘密信息, 实现了子秘密的保护, 但在秘密重构阶段该方案一次恢复全部秘密. Mashhadi 方案[16] 在秘密恢复时限制了秘密的重构顺序, 恢复某个秘密必须先恢复前面所有的秘密. 本方案共享的秘密可以为任意信息, 每个秘密可选择不同的存取结构进行共享, 可灵活地根据需要在秘密分发阶段选择合适的门限存取结构. 在共享秘密时, 根据不同的门限值构造随机多项式生成秘密的掩盖值, 对秘密进行隐藏生成的公开值个数为$2k$, 远小于其他几个方案产生的公开值个数, 并且不同秘密在共享时为相互独立的, 因此在秘密重构时可根据需要恢复对应的秘密值.

表 1 子秘密可多使用秘密共享方案对比

方案	公开值个数	秘密恢复顺序	存取结构
Geng等[8]	n^2	任意顺序	多存取结构
Wang等[10]	$2n+m-t+1$	一次恢复	单一存取结构
Mashhadi[16]	$\le k(n-t_1+2)$	固定顺序	多存取结构
本文方案	$2k$	任意顺序	多存取结构

Shao 的方案[9] 构造两个不同的多项式, 产生的公开值为$2(k-t)$个, 但 Shao 的方案子秘密不具有多使用性, 并且所有秘密为一次性全部恢复的; Chen 等的方案[15] 虽然在秘密恢复时可以按任意顺序恢复, 但其公开值个数为$\sum_{i=1}^{k}(n-t_i+1)$, 大于本方案的$2k$; Zarepour-Ahmadabadi 等的方案[17] 公开值个数为 k 个, 但需要可信第三方参加秘密重构, 并且参与者的子秘密不具有多使用性. 表 2 中通过 3 个方案的比较, 说明了本方案与其他几种公开值个数较少的多秘密共享方案在秘密恢复、存取结构、参与者保存的子秘密个数以及子秘密的安全性等方面进行对比具有更好的性质.

表 2 多秘密共享方案性能对比

方案	秘密恢复顺序	存取结构	参与者子秘密个数	子秘密多使用性
Shao [9]	一次性恢复	单一存取结构	1	不可多使用
Chen等[15]	任意顺序	多存取结构	1	不可多使用
Zarepour-Ahmadabadi等[17]	固定顺序	多存取结构	2	不可多使用
本文方案	任意顺序	多存取结构	1	可多使用

4 结论

本文基于 Shamir(t,n)-门限秘密共享方案, 应用中国剩余定理作为聚合的工具生成公开值, 提出了一个

子秘密可多次使用的多秘密共享方案. 该方案一次分发多个秘密, 每个秘密可以对应不同的门限结构, 同时参与者只存储一个子秘密. 在秘密重构阶段可根据需要恢复对应的秘密, 参与者根据不同秘密的公开值信息进行计算, 生成伪子秘密参与秘密重构, 最后根据对应的转换值计算得到秘密. 同时参与者可以根据公开的 Hash 函数对恢复的秘密进行计算, 通过与分发者的公开承诺值进行比较对所恢复的秘密进行验证. 分析表明, 与现有的部分多秘密共享方案相比, 本文的方案在公开值个数以及子秘密的多使用性等方面有更好的性能.

参考文献

1 Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612–613. [doi: 10.1145/359168.359176]

2 Blakley GR. Safeguarding cryptographic keys. Proceedings of the AFIPS 1979 National Computer Conference. New York, NY, USA. 1979.313–317. [doi: 10.1109/AFIPS.1979.98]

3 Benaloh J, Leichter J. Generalized secret sharing and monotone functions. Advances in Cryptology. New York, NY, USA. 1988. 27–35. [doi: 10.1007/0-387-34799-2_3]

4 Ito M, Saito A, Nishizeki T. Secret sharing scheme realizing general access structure. Electronics and Communications in Japan (Part Ⅲ-Fundamental Electronic Science), 1989, 72(9): 56–64. [doi: 10.1002/ecjc.4430720906]

5 Chor B, Goldwasser S, Micali S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults. 26th Annual Symposium on Foundations of Computer Science. Portland, OR, USA. 1985. 383–395. [doi: 10.1109/SFCS.1985.64]

6 Stadler M. Publicly verifiable secret sharing. International Conference on Advances in Cryptology Saragossa, Spain. 1996. 190-199. [doi: 10.1007/3-540-68339-9_17]

7 He J, Dawson E. Multistage secret sharing based on one-way function. Electronics Letters, 1994, 30(19): 1591–1592. [doi: 10.1049/el:19941076]

8 Geng YJ, Fan XH, Fan H. A new multi-secret sharing scheme with multi-policy. The 9th International Conference on Advanced Communication Technology. Okamoto, Kobe, Japan. 2007.1515–1517. [doi: 10.1109/ICACT.2007.358655]

9 Shao J. Efficient verifiable multi-secret sharing scheme based on hash function. Information Sciences, 2014, 278: 104–109. [doi: 10.1016/j.ins.2014.03.025]

10 Wang N, Cai YY, Fu JS, *et al*. Information privacy protection based on verifiable (*t*, *n*)-threshold multi-secret sharing scheme. IEEE Access, 2020, 8: 20799–20804. [doi: 10.1109/ACCESS.2020.2968728]

11 曹阳. 基于大整数分解可公开验证的秘密共享方案. 计算机系统应用, 2016, 25(3): 271–273.

12 彭咏, 邵培南, 李翔, 等. 基于格的可验证秘密共享方案. 计算机系统应用, 2020, 29(1): 225–230. [doi: 10.15888/j.cnki.csa.007208]

13 Harn L, Hsu CF. (*t*, *n*) multi-secret sharing scheme based on bivariate polynomial. Wireless Personal Communications, 2017, 95(2): 1495–1504. [doi: 10.1007/s11277-016-3862-z]

14 Zhang T, Ke XZ, Liu YX. (*t*, *n*) multi-secret sharing scheme extended from Harn-Hsu ’s scheme. Eurasip Journal on Wireless Communications and Networking, 2018, 2018(1): 71. [doi: 10.1186/s13638-018-1086-5]

15 Chen D, Lu W, Xing WW, *et al*. An efficient verifiable threshold multi-secret sharing scheme with different stages. IEEE Access, 2019, 7: 107104 –107110. [doi: 10.1109/ACCESS.2019.2929090]

16 Mashhadi S. How to fairly share multiple secrets stage by stage. Wireless Personal Communications, 2016, 90(1): 93–107. [doi: 10.1007/s11277-016-3332-7]

17 Zarepour-Ahmadabadi J, Shiri-Ahmadabadi M, Miri A, *et al*. A new gradual secret sharing scheme with diverse access structure. Wireless Personal Communications, 2018, 99(3): 1329–1344. [doi: 10.1007/s11277-017-5187-y]

18 Tassa T. Hierarchical threshold secret sharing. Journal of Cryptology, 2007, 20(2): 237 –264. [doi: 10.1007/s00145-006-0334-8]

19 Odlyzko AM. Discrete logarithms in finite fields and their cryptographic significance. Proceedings of EUROCRYPT 84 A Workshop on Advances in Cryptology. Paris, France. 1985. 224–314. [doi: 10.1007/3-540-39757-4_20]

20 Trotter H. Book Review: A course in computational algebraic number theory. Bulletin of the American Mathematical Society, 1994, 31(2): 312–318. [doi: 10.1090/S0273-0979-1994-00542-7]