Pure Mathematics 理论数学, 2022, 12(12), 2124-2132
Published Online December 2022 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2022.1212228

Hans汉斯

基于多项式插值的多部门限秘密共享方案

林苇婷，林昌露

福建师范大学数学与统计学院，福建 福州

收稿日期：2022年11月23日；录用日期：2022年12月22日；发布日期：2022年12月29日

摘　要

在门限秘密共享方案中，一个参与者集合是否能恢复主秘密，取决于参与重构的参与者数量。在某种情况下，仅由一组参与者就能恢复主秘密，权限会相对过于集中。为了避免该问题，本文将一个大集合的参与者划分为几个不相交分区，每个分区都有一个独立部分访问结构；只有满足所有部分访问结构的参与者集合，才能恢复主秘密，否则得不到主秘密的任何信息。基于Shamir门限秘密共享方案和自由群中短词排序，本文构造了新的多部门限秘密共享方案，该方案可实现主秘密的动态更新，避免主秘密改变时分发阶段的通信需求，使整个方案在更新主秘密时更加高效。

关键词

门限秘密共享，自由群，信息熵，短词排序，主秘密更新，多项式插值

Multipartie Threshold Secret Sharing Scheme Based on Polynomial Interpolation

Weiting Lin, Changlu Lin

College of Mathematics and Statistics, Fujian Normal University, Fuzhou Fujian

Received: Nov. 23rd, 2022; accepted: Dec. 22nd, 2022; published: Dec. 29th, 2022

Abstract

In the threshold secret sharing scheme, whether a set of participants can recover the secret depends on the number of participants participating in the reconstruction. In some cases, only one group of participants can recover the secret, and the authority will be relatively centralized. To avoid this problem, the participants of a large set are divided into several disjoint partitions, each partition has an independent part access structure; only the set of participants meeting all partial access structures can recover the secret, otherwise no information of the secret can be obtained. Based on Shamir threshold secret sharing scheme and shortlex order in the free group, this paper

文章引用: 林苇婷, 林昌露. 基于多项式插值的多部门限秘密共享方案[J]. 理论数学, 2022, 12(12): 2124-2132.
DOI: 10.12677/pm.2022.1212228

constructs a new multipart threshold secret sharing scheme. This scheme can realize the dynamic update of the secret, avoid the communication requirements of the time transmission phase when the secret changes, and make the whole scheme more efficient when updating the main secret.

Keywords

Threshold Secret Sharing, Free Group, Information Entropy, Shortlex Order, Secret Updating, Polynomial Interpolation

1. 引言

信息技术日新月异，密码学成为网络空间安全的重要技术之一；秘密共享作为密码学领域最重要的内容之一，受到广泛的关注和研究。1979 年，Shamir [1]和 Blakley [2]分别基于有限域上的多项式和超几何平面的射影定理构造了两种门限秘密共享方案，对于现代密码学的研究具有重要作用。一般地，秘密共享方案分为两个算法：分发算法和重构算法。在分发算法中，分发者将主秘密分成若干个份额，并通过安全信道分发给参与者。在重构算法中，若干参与者将各自份额发送给重构者即可恢复主秘密；这些参与者的集合称为授权集，所有授权集的集合称为访问结构。

秘密共享方案可分为多种类型，如门限秘密共享方案[1] [2]，多部秘密共享方案[3] [4] [5] [6]和门限可变秘密共享方案[7] [8]，等等。在多部秘密共享方案中，参与者被划分为几个不相交的分区，每个分区都有一个部分访问结构。若一个参与者集合满足所有的部分访问结构，则该参与者集合就可以恢复主秘密；但只要存在一个或多个分区不满足其相应的部分访问结构，则该参与者集合就不能获得正确的主秘密。多部访问结构在秘密共享方案的研究中备受关注，它是门限秘密共享的自然推广；它并不是对给定子集中的参与者数量设置一个门限条件，而是对每个分区子集中的参与者数量施加一个更小的门限条件[9]。因为参与者众多且分在不同的分区，故多部秘密共享方案在主秘密分发过程需要较大的通信量。分层秘密共享方案是多部秘密共享方案的一种特殊情形。后者的每个访问结构都具备相同的权限和等级；前者的不同分区也是表示不同访问结构，但是它们之间的优先级不相同。

1988 年，Simmons 等[10]最先提出了多部访问结构，给出了相应访问结构和分层访问结构的定义，并分析两者定义的异同点。同年，Brickell 等[11]提出了一种构建理想的多部秘密共享方案方法，实现了分层和多部的访问结构；因为需要指数运算得到非奇异矩阵，故该方案效率低下。2007 年，Tassa 等[12]基于 Birkhoff 插值设计了分层门限访问结构，其中插值矩阵必须满足 Polya 条件。然而，Polya 条件只是一个必要条件，而不是一个充分条件；当分配身份和份额给参与者时，分发者必须执行指数级运算验证插值矩阵是否满足 Polya 条件，其效率较低。同年，Farras 等[9]对理想的多部访问结构给出了全面描述，但他们没有设计一个理想的秘密共享方案来实现其多部访问结构。Farras 等提出一个公开问题：是否存在有效的方法从多部拟阵表示中实现理想的多部秘密共享方案。2014 年，Hsu 等[13]基于中国剩余定理设计了一个多部访问结构方案，但是该方案不是理想的多部访问结构，且无法实现主秘密的更新。2016 年，Harsha 等[14]利用背包和问题中的超递增序列实现了可更新主秘密的多部门限秘密共享方案构造，但是由于该方案是基于整数规划求解问题，所以它仅是可计算安全。2019 年，Chen 等[15]构建了理想的

线性多部秘密共享方案，利用文献[9]中提出的基于多拟阵的方法和 Gabidulin 编码实现多部访问结构。2021 年，Chen 等[16]利用线性代数技术提出了一种分区访问结构方案，但该方案需要检查较多矩阵的非奇异性，故其效率也较低。同年，Xu 等[17]提出了具有分层访问结构的多阶段秘密共享方案，但该方案仅是可计算安全。Miao 等[3]基于多项式插值和中国剩余定理提出了多部门限秘密共享方案，其缺点是无法实现主秘密的更新。上述这些方案，有的不满足理想的秘密共享方案特性或子秘密不具有重复使用的性质；有的更新主秘密导致分发算法的通信量较大。

本文基于多项式插值和短词排序技术提出了一类子秘密可重复使用的多部秘密共享方案，主要构造思路是将自由群中的有限表现集分发给对应的每一个层级参与者，利用既约字和短词排序将函数值转换成字集形式，再将字集进行公开；参与重构的参与者们使用持有的份额重构出自由群，并用自由群和短词排序恢复函数值，再用多项式插值公式重构出主秘密的值。

本文方案在不改变部分访问结构的参与者子秘密情况下实现在线更新主秘密，并且具有信息论意义下的安全性。每当分发者改变主秘密时，分发者会根据部分访问结构的份额更新新公开值，然后根据新公开值和部分访问结构重构新主秘密。对于每个主秘密的变化，每个部分访问结构需和当前的公开值一起参与重构秘密，因为之前的公开值不再有效。分发者可在有需要的情况下改变主秘密，避免分发算法的通信复杂度。

本文架构如下：第 1 节介绍本文研究背景以及相关研究工作；第 2 节简要说明一些预备知识；包含本文所需的数学理论基础；第 3 节描述本文方案具体构造；第 4 节给出方案详细分析；第 5 节对本文作出总结。

2. 预备知识

2.1. 秘密共享方案

秘密共享方案主要包括分发者 D，参与者 $P=\{P_1,P_2,\cdots,P_n\}$，重构者 C，共享的主秘密以及秘密分发算法和秘密重构算法。分发者 D 根据分发算法将主秘密值转换为多个份额，并将所对应产生的份额安全地分发给相应的参与者；秘密重构时，重构者 C 根据重构算法将多个参与者的份额转化为主秘密值。

为了方便阐述，本文将秘密共享方案分为 3 个过程：

- **参数选取：**分发者 D 根据方案需要选取合适的参数。
- **秘密分发：**分发者 D 根据方案分发算法将主秘密值分成多个份额，并通过安全信道分发给对应的参与者。
- **秘密重构：**任意的访问结构中的参与者集根据重构算法进行主秘密重构。

2.2. Shamir (t,n) 门限秘密共享方案

在 (t,n) 门限秘密共享方案中，分发者将主秘密分成 n 个份额，使得任意不少于 t 个参与者合作正确地重构出主秘密 s，而小于门限值 t 个的参与者合作无法获得有关主秘密的任何信息。当门限秘密共享方案同时满足以下两个性质，可称该方案是完善的 (t,n) 门限秘密共享方案：1) **正确性**：任意的大于或者等于 t 个参与者合作可以正确地恢复出主秘密；2) **安全性**：任意的少于 t 个参与者合作无法得到主秘密的任何信息。

Shamir 方案[1]是基于有限域上多项式插值方法构造的一类 (t,n) 门限秘密共享方案。分发者构造次数不大于 $t-1$ 次多项式 $f(x)$，将主秘密 $s\in\mathbb{F}_p$ (p 为大素数，$p>n$)作为多项式常数项，并且多项式系数为随机生成数值，将多项式在各个点处的函数值 $f(x)$ 安全地分发给 n 个参与者 $P=\{P_1,P_2,\cdots,P_n\}$ 作为各自的份额。该方案参数选取、分发过程和重构过程具体构造如下：

- **参数选取：**

  1) 分发者 D 选取整数 n 和大素数 p，其中 n 为参与者人数且 $p>n$；

  2) 分发者再选取 $x_i \in \mathbb{F}_p$，将所有 x_i 公开，其中 $i=1,\cdots,n$。

- **秘密分发：**

  1) 分发者 D 随机选取 $a_0,a_1,\cdots,a_{t-1} \in \mathbb{F}_p$ 并构造多项式 $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}\pmod p$，其中常数项 $a_0=s$ 为主秘密值；

  2) 分发者 D 计算每个函数值 $f(x_i)(i=1,\cdots,n)$，作为第 i 个参与者 P_i 的份额；

  3) 分发者 D 通过安全信道把这些份额分发给参与者 P_i，其中 $i=1,\cdots,n$。

- **秘密重构：**设有 t 个参与者 $P_1,P_2,\cdots,P_t$ 欲恢复主秘密，他们各自提供其持有的秘密份额，利用 Lagrange 多项式插值公式重构得到主秘密，具体计算方法如下：

$$s=\sum_{i=1}^{t} f(x_i)\prod_{x_j=1,x_j\neq x_i}^{t}\frac{x_j}{x_j-x_i}(\bmod p).$$

2.3. 信息熵

Shannon [18]提出信息熵刻画描述信息的不确定程度，通过随机变量的概率分布函数给出度量信息熵的数学表达式。为了便于本文描述，下文给出信息熵和条件熵的定义。

定义 1 [18] 离散随机变量 V 由有限集合 υ 和定义在 υ 上的概率分布组成，设离散随机变量 V 的概率分布函数为 $p(v)=\Pr\{V=v\}(v\in\upsilon)$，则随机变量 V 的信息熵定义为

$$H(v)=-\sum_{v\in\upsilon}p(v)\log p(v).$$

定义 2 [18] 设随机变量 V,Y 对应的有限集合分别为 υ,γ，则联合分布为 $p(v,y)$ 的离散随机变量对的条件熵为

$$H(Y|V)=\sum_{v\in\upsilon}p(v)H(Y|V=v)=-\sum_{v\in\upsilon}p(v,y)\log(y|v).$$

通过条件熵 $H(V|Y)$，定义信息熵的链式法则为：$H(V|Y)=H(V)+H(Y|V)$。

定义 3 (完善的秘密共享方案[19])当秘密共享方案同时满足如下两个条件，则称该方案为完善的秘密共享方案：

正确性：对于授权集 A，A 中参与者将持有的份额联合起来，可正确恢复主秘密 s，即 $H(s|s_A)=0$，s_A 表示集合 A 中参与者的份额集；

安全性：对于非授权集 B，B 中参与者将持有的份额联合起来，得不到关于主秘密 s 的任何信息，即 $H(s|s_B)=H(s)$，s_B 表示集合 B 中参与者的份额集。

利用信息熵的相关性质将证明了本文方案是完善安全的。

2.4. 自由群

设 X 是群 G 的一个生成元集，对于 X 中的任意元素 $e_1,e_2,\cdots,e_k$，如果 $e_i\neq e_{i+1}(1\le i<k)$，并且 $m_1,m_2,\cdots,m_k$ 全不为 0，则 $e_1^{m_1}e_2^{m_2}\cdots e_k^{m_k}\neq G^1$，其中 G^1 为 G 中的单位元，那么称 X 是群 G 的一个自由生成元集。如果群 G 有一个自由生成元集，则称 G 是自由群。例整数加群 $\mathbb{Z}$ 是自由群。因为 $\mathbb{Z}$ 有一个自由生成元集 $\{1\}$，所以 $\mathbb{Z}$ 是由一个元素生成的自由群。本文把一个非空集合 X 称为字母表。

定义 4 [20] 设 X 为字母表且 $e_1,e_2,\cdots,e_k\in X$，$m_i\in\mathbb{Z},1\le i\le k$，称 $e_1^{m_1}e_2^{m_2}\cdots e_k^{m_k}$ 为一个字。

定义 5 [20] 如果 $e_i\neq e_{i+1},1\le i<k$，并且所有 $m_i\neq 0,1\le i\le k$，称字 $e_1^{m_1}e_2^{m_2}\cdots e_k^{m_k}$ 是既约的。特别地，把 e_i^0 也称为既约字。

每一个字都可按照下述规则化简成既约字：1) 如果相邻的两个字母相同，则可合并写成一个字母的方幂，将指数的和作为指数；2) 零次幂省略不写。因此字母表 X 形成的所有既约字组成的集合 $F(X)$ 构成一个群。容易看出，X 是群 $F(X)$ 的一个自由生成元集。故 $F(X)$ 是自由群，称它是由 X 生成的自由群。

定义 6 [20] 设 X 是非空集合，R 是自由群 $F(X)$ 的非空子集，用 N 表示 R 生成的正规子群(即为 $F(X)$ 中包含 R 的正规子群的交)，则商群 $F(X)/N$ 称为是由生成元集 X 和定义关系集 R 决定的群。如果群 G 同构于 $F(X)/N$，则 X,R 称为 G 的一个表现，记作 $G\equiv\{X\mid R\}$。特别地，若 $X=\{e_1,e_2,\cdots,e_k\}$，且 $R=\{\omega_1,\cdots,\omega_t\}$，那么就称 G 是有限表现的。

定理 1 [20] 每一个字能化简成唯一的既约字。

定义 7 [21] 设 $X=\{e_1,e_2,\cdots,e_m\}$ 是一个字母表，群 G 由 X 所生成，记为 $G=\langle X\rangle$，那么群 $G=\langle X\rangle$ 的一种短词排序定义如下；给定既约字 $\omega=e_{i_1}\cdots e_{i_p}$ 以及 $l=e_{j_1}\cdots e_{j_k}$，其中 $\omega\neq l$，且 $|\omega|$ 表示的是 ω 的长度，$|l|$ 表示的是 l 的长度，如果满足以下条件之一：

1) $|\omega|<|l|$；

2) 若 $p=k$，且 $e_{i_a}<e_{j_a}$，其中 $a=\min_\alpha\{e_{i_a}\neq e_{j_a}\}$；

则称 ω 和 l 为序关系，记为 $\omega<l$。

例如，若 $X=\{x,y\}$，且给定 $X^{\pm1}$ 的词序为 $x<x^{-1}<y<y^{-1}$，可推断出一些词序为：

$$e<x<x^{-1}<y<y^{-1}<x^2<xy<xy^{-1}<x^{-2}<x^{-1}y<x^{-1}y^{-1}<yx<yx^{-1}<y^2<y^{-1}x<y^{-1}x^{-1}<y^{-2}<x^3<x^3<x^2y<x^2y^{-1}<xyx<xyx^{-1}<\cdots$$

。

根据每一个短词的位置，相应可将词序转化为整数值：x^{-1} 可对应出词序位置为 3；根据词序位置的整数值，可相应的对应出既约短词：词序位置为 10，相应可对应出短词为 $x^{-1}y$。

3. 本文方案

本节基于自由群中的短词排序与 Shamir (t,n) 门限秘密共享方案设计了子秘密可重复使用的多部门限秘密共享方案；其构造思路是：每个部分访问结构门限值是 t_i，通过给每个部分访问结构分发不同自由群的定义关系集，根据定义关系集和函数值生成函数值对应的公开字集，将每个人的身份标识，以及公开字集作为公开信息。具体方案构造如下：

- **参数选取：**

1) 分发者 D 选取 $P=\{P_1,\cdots,P_n\}$ 作为 n 个参与者的集合，然后将 P 又分成 m 个部分访问结构 $P=\{U_1,U_2,\cdots,U_m\}$，每个部分访问结构 U_i 中有 n_i 名参与者，每个参与者只属于其中一个部分访问结构中，即有 $U_i\cap U_j=\varnothing(i\neq j)$ 和 $n=n_1+n_2+\cdots+n_m$。

2) 分发者 D 随机选取 $x_i\in\mathbb{F}_p$，将 x_i 对应地分发给层级 U_i，作为层级 U_i 公开值。

- **秘密分发：**

1) 分发者 D 为层级 U_i，$i=1,2,\cdots,m$ 选取一个有限表现群 $G_i=\langle e_{i1},e_{i2},\cdots,e_{ik}\mid r_{i1},r_{i2},\cdots,r_{iu_i}\rangle$，其中 e_{ij} 为群 G_i 的生成元，r_{ij} 为群 G_i 的定义关系元，$u_i=C_{n_i}^{t_i-1}$。

2) 分发者 D 首先选定 $A_1,\cdots,A_{m_i}$ 为集合 $\{1,2,\cdots,n_i\}$ 中任意 (t_i-1) 个元素的子集，并确定 $\{R_{i1},R_{i2},\cdots,R_{in_i}\}$ 为 $R_i=\{r_{i1},r_{i2},\cdots,r_{iu_i}\}$ 的 n_i 个子集，其中 $r_{ij}\in R_{ij}$ 当且仅当 $i\notin A_j$，$j=1,2,\cdots,u_i;i=1,2,\cdots,n_i$；随后将字集 R_{ij} 作为秘密份额对应地分发给参与者 P_{ij}。

3) 分发者 D 随机选取 $a_0,a_1,\cdots,a_{m-1}\in\mathbb{F}_p$，构造次数不大于 $(m-1)$ 次多项式 $f(x)=a_0+a_1x+\cdots+a_{m-1}x^{m-1}(\mathrm{mod}\ p)$，其中常数项 $a_0=s$ 为主秘密值。

4) 分发者公开短词排序，根据短词与位置整数值的一一对应关系，$f(x_i)$的值可对应短词排序中第$f(x_i)$个位置的短词，利用函数值对应的短词和G_i中的定义关系集，可根据短词既约运算生成公开值ω_i，使得ω_i可以在G_i的定义关系集下既约对应于第$f(x_i)$个词序位置。

- **秘密重构：**

1) 每个层级U_i集合中任意t_i个及以上参与者合作可恢复定义关系集$R_i=\{r_{i1},r_{i2},\cdots,r_{iu_i}\}$，进而可恢复有限表现群$G_i$。

2) 根据群G_i的定义关系集，可将公开字集ω_i既约为短词排序的第$f(x_i)$个词序位置，m个部分访问结构共恢复m个函数值，然后根据利用 Lagrange 多项式插值公式计算得到主秘密：

$$s=\sum_{i=1}^{m} f(x_i)\prod_{x_j=1,x_j\neq x_i}^{m}\frac{x_j}{x_j-x_i}\pmod p。$$

上述方案流程图可如图 1 所示：

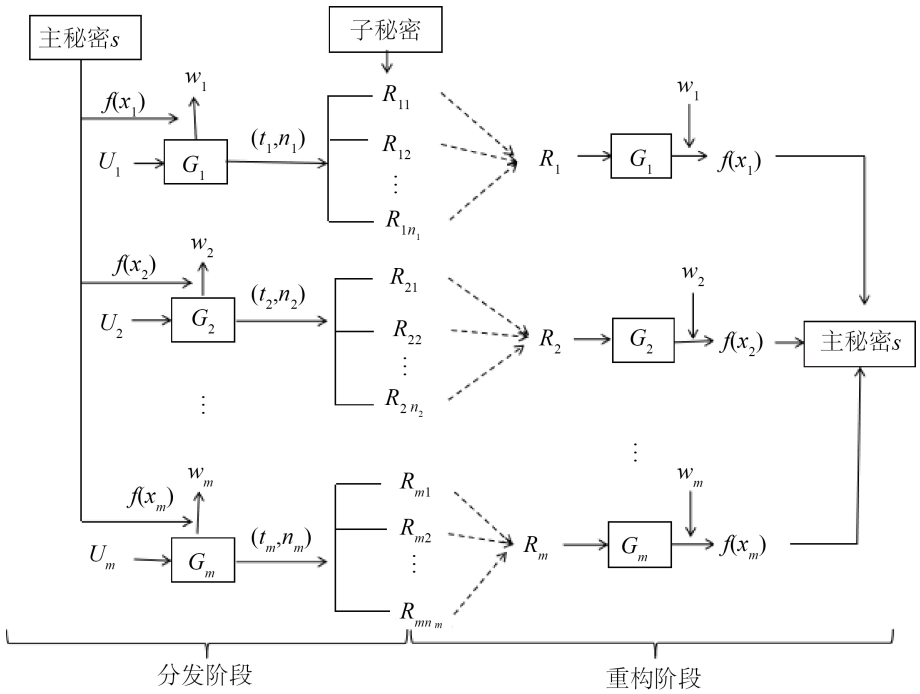

Figure 1. The diagram of scheme
图 1. 方案示意图

4. 方案分析

根据定义 3，本节给出本文方案正确性和安全性分析。正确性分析主要是分析根据方案重构算法是否可以正确地恢复主秘密；安全性证明包括两个部分：一部分是层级U_i内小于门限t_i的参与者合作得不到主秘密的任何信息，另一部分是任意$m-1$个层级合作得不到主秘密的任何信息。

定理 2 本文方案是完善的多部秘密共享方案。

证明：正确性：假设U_i中的t_i个参与者$P_{i1},P_{i2},\cdots,P_{it_i}$需要恢复出份额$f(x_i)$，这时参与者们利用持有的字集可以恢复出自由群$G_i$，那么根据自由群$G_i$的定义关系集，将公开字集$\omega_i$既约为词序中的第$f(x_i)$个位置，得出$f(x_i)$的函数值. 那么$m$个部分访问结构一共有$m$个$f(x_i)$的值，因此可以根据 Lagrange

多项式插值公式求解出主秘密 s。

安全性：1) 以下证明任意的 t_i-1 个参与者得不到第 t_i 个 R_{it_i} 的信息。根据信息熵相关定义证明，因为分发者分发给部分访问结构中的每个参与者的字集不同，所以

$$
\begin{aligned}
&H\left(R_{it_i}\mid R_{i1}R_{i2}\cdots R_{it_i-1}\right)=-\sum_{b_{it_i}\in R_{it_i}}\sum_{y\in Y}p(y)\,p\left(b_{it_i}\mid y\right)\log p\left(b_{it_i}\mid y\right)\\
&=-\sum_{b_{1_i}\in R_{1_i}}\sum_{b_{1_i}b_{2_i}\cdots b_{t_i-1}\in R_{1_i}R_{2_i}\cdots R_{t_i-1}}p\left(b_{i1}b_{i2}\cdots b_{it_i-1}\right)p\left(b_{it_i}\mid b_{i1}b_{i2}\cdots b_{it_i-1}\right)\log p\left(b_{it_i}\mid b_{i1}b_{i2}\cdots b_{it_i-1}\right)\\
&=-\sum_{b_{it_i}\in R_{it_i}}\sum_{b_{i1}b_{2i}\cdots b_{it_i-1}\in R_{i1}R_{i2}\cdots R_{it_i-1}}p\left(b_{i1}b_{i2}\cdots b_{it_i-1}\right)p\left(\frac{b_{i1}b_{i2}\cdots b_{it_i-1}b_{it_i}}{b_{i1}b_{i2}\cdots b_{it_i-1}}\right)\log p\left(\frac{b_{i1}b_{i2}\cdots b_{it_i-1}b_{it_i}}{b_{i1}b_{i2}\cdots b_{it_i-1}}\right)\\
&=-\sum_{b_{it_i}\in R_{it_i}}p\left(b_{it_i}\right)\log p\left(b_{it_i}\right)\\
&=H\left(R_{it_i}\right)
\end{aligned}
$$

其中 $y=b_{i1}b_{i2}\cdots b_{it_i-1}$ 为 $Y=R_{i1}R_{i2}\cdots R_{it_i-1}$ 的一个子集，故 t_i-1 个参与者得不到第 t_i 个参与者的信息。

以上证明式子第三步至第四步是因为分发者分发给每个参与者的字集 $R_{i1},R_{i2},\cdots,R_{it_i-1}$ 不同，因此对于 $R_{i1},R_{i2},\cdots,R_{it_i-1}$ 的任意子集，有 $p\left(b_i\right)=p\left(b_j\right)$，其中 $i,j\in i1,i2,\cdots,it_i$。最后可以得到

$p\left(\frac{b_{i1}b_{i2}\cdots b_{it_i-1}b_{it_i}}{b_{i1}b_{i2}\cdots b_{it_i-1}}\right)=p\left(b_{i1}\right)p\left(b_{i2}\right)\cdots p\left(b_{it_i-1}\right)p\left(b_{it_i}\right)\Big/\left(p\left(b_{i1}\right)p\left(b_{i2}\right)\cdots p\left(b_{it_i-1}\right)\right)=p\left(b_{it_i}\right)$。

假设 t_i-1 个参与者 $P_{i1},P_{i2},\cdots,P_{it_i-1}$ 尝试直接恢复主秘密，那么每个参与者对应地拿出自己手中拥有的定义关系集的子集 R_{ij} 去恢复自由群 G_i。因为分发者给每个部分访问结构中的参与者分发自由群 G_i 中的定义关系集不一致，所以 t_i-1 个参与者只能得到部分但不是全部的 $r_1,r_2,\cdots,r_{u_i}$，这时参与重构的参与者们会就此生成一个自由群 $G'=\left\langle x_1,x_2,\cdots,x_k\mid r_1',r_2',\cdots,r_g'\right\rangle$，其中 $g<u_i$。那么参与者们并没有恢复完整的群 G_i 的定义关系集合，所以 G_i 和 G_i' 的单位元会有所不同，有 $G_i\neq G_i'$，根据 G_i' 去既约公开字集 ω_i 会得到错误的 $f\left(x_i\right)$，错误的 $f\left(x_i\right)$ 不能恢复正确的主秘密 s。

2) 任意两个部分访问结构 U_i 和 U_j 的参与者互相得不到对方的子秘密值，这是因为分发给每个部分访问结构的参与者们是不同的自由群，即有 $G_i\neq G_j$，自由群不同，通过自由群的定义关系集求解出的短词也是不同的，只有对应的访问结构的自由群才能正确求解出既约的短词，进而对应的求解出函数值。因此 $m-1$ 个层级合作只能获取 $m-1$ 个函数值，只能列出 $m-1$ 个线性方程组，求解不出 m 个未知数，所以基于 Shamir 方案易知 $m-1$ 个层级合作得不到主秘密的任何信息。 □

本文方案可以实现主秘密更新功能。分发者需要更新主秘密时，只需要更新多项式的函数值对应的公开字集 ω_i。当公开字集改变，部分访问结构中的参与者利用同一个自由群既约公开字集，既约出的短词对应不同的词序位置，即新的函数值位置，最后根据 Lagrange 多项式插值公式求解出更新之后的主秘密。

5. 方案比较

本文的多部门限秘密共享方案能够通过参与者子秘密的动态使用，进行主秘密的更新，避免更改主秘密时分发阶段中的通信需求。对于多部秘密共享方案中，因为访问结构较多，分发算法尤其繁杂，所以若主秘密能够实现动态更新，效率会得到了较大的提升。本文方案可动态实现主秘密更新，于分发算法效率上要优于文献[3] [13]。与文献[14]相比较：因为文献[14]是基于整数规划的 NP 问题，所以该方案是可计算安全的；本文方案不基于任何困难问题假设，所以本文方案具有较高的安全性。本文方案与其

他多部门限秘密共享方案的对比如表 1 所示。

Table 1. Performance comparison of multipartie threshold secret sharing schemes
表 1. 多部门限秘密共享方案性能比较

方案	构造方式	主秘密更新	信息率	计算复杂度	困难问题
Miao 等方案[3]	CRT	×	>1	$O(1)$	无条件安全
Harn 等方案[13]	CRT	×	≈1	$O(m)$	可计算安全
Harsha 等方案[14]	超递增序列	√	1	$O(m\log t)$	可计算安全
本文方案	多项式	√	1	$O(t\log t)$	无条件安全

注：信息率是指主秘密大小与子秘密大小的比值。

6. 总结

本文基于 Shamir(t,n)门限秘密共享方案，以自由群的短词排序为工具构造了一个主秘密可以多次更新的多部门限秘密共享方案。该方案通过分发自由群中定义关系集的子集作为参与者的份额；参与者们通过恢复自由群的定义关系集，利用短词排序方法恢复函数值，Lagrange 多项式插值公式重构主秘密。本文方案具有动态更新主秘密的优点，避免了主秘密更新时分发阶段的再次通信。未来的研究工作可经过扩展到构造子秘密可重复使用门限多秘密共享方案以及门限可变的多部秘密共享方案等。

参考文献

[1] Shamir, A. (1979) How to Share a Secret. *Communications of the ACM*, **22**, 612-613. https://doi.org/10.1145/359168.359176

[2] Blakley, G.R. (1979) Safeguarding Cryptographic Keys. *International Workshop on Managing Requirements Knowledge*, New York, 4-7 June 1979, 313-313. https://doi.org/10.1109/MARK.1979.8817296

[3] Miao, F., Yu, Y., Meng, K., *et al*. (2021) Grouped Secret Sharing Schemes Based on Lagrange Interpolation Polynomials and Chinese Remainder Theorem. *Security and Communication Networks*, **2021**, Article ID: 6678345. https://doi.org/10.1155/2021/6678345

[4] Subrahmanyam, R., Rukma Rekha, N. and Subba Rao, Y.V. (2022) Multipartite Verifiable Secret Sharing Based on CRT. In: Smys, S., *et al*., Eds., *Computer Networks and Inventive Communication Technologies*, Springer, Singapore, 233-245. https://doi.org/10.1007/978-981-16-3728-5_17

[5] Shima, K. and Doi, H. (2018) A Hierarchical Secret Sharing Scheme Based on Information Dispersal Techniques. In: Lee, K., Ed., *International Conference on Information Security and Cryptology-ICISC* 2018, Springer, Cham, 217-232. https://doi.org/10.1007/978-3-030-12146-4_14

[6] Tochikubo, K. (2019) General Secret Sharing Schemes Using Hierarchical Threshold Scheme. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **102**, 1037-1047. https://doi.org/10.1587/transfun.E102.A.1037

[7] Ding, J., Lin, C. and Lin, F. (2020) Optimal Threshold Changeable Secret Sharing with New Threshold Change Range. In: Nguyen, K., *et al*., Eds., *International Conference on Provable Security* 2020, Springer, Cham, 361-378. https://doi.org/10.1007/978-3-030-62576-4_18

[8] Harn, L., Hsu, C. and Xia, Z. (2022) A Novel Threshold Changeable Secret Sharing Scheme. *Frontiers of Computer Science*, **16**, Article ID: 161807. https://doi.org/10.1007/s11704-020-0300-x

[9] Farràs, O., Martí-Farré, J. and Padró, C. (2012) Ideal Multipartite Secret Sharing Schemes. *Journal of Cryptology*, **25**, 434-463. https://doi.org/10.1007/s00145-011-9101-6

[10] Simmons, G.J. (1988) How to (Really) Share a Secret. In: Goldwasser, S., Ed., *Advances in Cryptology—CRYPTO*'88, Springer, Cham, 390-448. https://doi.org/10.1007/0-387-34799-2_30

[11] Brickell, E.F. (1989) Some Ideal Secret Sharing Schemes. In: Quisquater, J.-J. and Vandewalle, J., Eds., *Advances in Cryptology—EUROCRYPT* '89, Springer, Cham , 468-475. https://doi.org/10.1007/3-540-46885-4_45

[12] Tassa, T. (2007) Hierarchical Threshold Secret Sharing. *Journal of Cryptology*, **20**, 237-264. https://doi.org/10.1007/s00145-006-0334-8

[13] Hsu, C.F. and Harn, L. (2014) Multipartite Secret Sharing Based on CRT. *Wireless Personal Communications*, **78**, 271-282. https://doi.org/10.1007/s11277-014-1751-x

[14] Harsha, P., Chanakya, P. and Vadlamudi, C.V. (2018) A Reusable Multipartite Secret Sharing Scheme Based on Super Increasing Sequence. *International Journal of Network Security*, **20**, 527-535.

[15] Chen, Q., Tang, C. and Lin, Z. (2019) Efficient Explicit Constructions of Compartmented Secret Sharing Schemes. *Designs, Codes and Cryptography*, **87**, 2913-2940. https://doi.org/10.1007/s10623-019-00657-2

[16] Chen, Q., Tang, C. and Lin, Z. (2021) Efficient Explicit Constructions of Multipartite Secret Sharing Schemes. *IEEE Transactions on Information Theory*, **68**, 601-631. https://doi.org/10.1109/TIT.2021.3123102

[17] Xu, G., Yuan, J., Xu, G., *et al*. (2021) A New Multi-Stage Secret Sharing Scheme for Hierarchical Access Structure with Existential Quantifier. *Information Technology and Control*, **50**, 236-246. https://doi.org/10.5755/j01.itc.50.2.27789

[18] Shannon, C.E. (1948) A Mathematical Theory of Communication. *The Bell System Technical Journal*, **27**, 379-423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

[19] Cohen, H. (1993) A Course in Computational Algebraic Number Theory. Springer, Berlin. https://doi.org/10.1007/978-3-662-02945-9

[20] 丘维声. 抽象代数基础[M]. 第 2 版. 北京: 高等教育出版社, 2015: 75-81.

[21] Cavallo, B. and Kahrobaei, D. (2015) Secret Sharing Using Non-Commutative Groups and the Shortlex Order. *Contemporary Mathematics*, **633**, 1-8. https://doi.org/10.1090/conm/633/12646