密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2021, 8(3): 537–548

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

基于多变量多项式的门限函数秘密分享方案*

林昌露[1,2,5,6], 罗景龙[1,3], 张胜元[1,2], 王华雄[4]

1. 福建师范大学 数学与统计学院, 福州 350117
2. 福建省网络安全与密码技术重点实验室 (福建师范大学), 福州 350007
3. 鹏城实验室 人工智能研究中心, 深圳 518055
4. 新加坡南洋理工大学 物理与数学学院, 新加坡 308232
5. 网络空间与信息安全重庆市重点实验室, 重庆 400065
6. 桂林电子科技大学 广西可信软件重点实验室, 桂林 541004

通信作者: 林昌露, E-mail: cllin@fjnu.edu.cn

摘 要: 为了提高分布式环境下私密信息存取协议的效率, Boyle 等人在 2015 年欧密会上提出了函数秘密分享 (Function Secret Sharing, FSS) 概念并给出了具体构造. 传统秘密分享方案在参者之间分享的秘密为具体数值, 而 FSS 方案中分享的秘密为函数. Boyle 等人基于伪随机生成器构造了一类 FSS 方案, 它们均为计算意义下安全的, 即只能抵抗计算能力有限的敌手攻击. 本文利用有限域上多变量多项式构造了完善安全的门限 FSS 方案. 其设计技巧是将 FSS 方案中秘密函数在公开点处函数值的计算转换为公开函数在秘密点处函数值的计算. 经过分析发现该方案的通信复杂度与重构门限值 r 和私密门限值 t 之间的比值相关; 当重构门限值与私密门限值之间的比值较大时, 该方案可以实现较低的通信复杂度. 此外, 该方案可以同时满足函数秘密分享的简洁性、压缩性和函数私密性. 这些良好的性能与性质使得该方案可更好地适用于设计各类私密信息存取协议.

关键词: 函数秘密分享; 门限秘密共享; 完善安全性; 私密信息检索

中图分类号: TP309.2 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000456

中文引用格式: 林昌露, 罗景龙, 张胜元, 王华雄. 基于多变量多项式的门限函数秘密分享方案[J]. 密码学报, 2021, 8(3): 537–548. [DOI: 10.13868/j.cnki.jcr.000456]

英文引用格式: LIN C L, LUO J L, ZHANG S Y, WANG H X. A multivariate polynomial based threshold function secret sharing scheme[J]. Journal of Cryptologic Research, 2021, 8(3): 537–548. [DOI: 10.13868/j.cnki.jcr.000456]

A Multivariate Polynomial Based Threshold Function Secret Sharing Scheme

LIN Chang-Lu[1,2,5,6], LUO Jing-Long[1,3], ZHANG Sheng-Yuan[1,2], WANG Hua-Xiong[4]

1. School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China
2. Fujian Provincial Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China

* 基金项目: 国家自然科学基金 (U1705264, 61572132); 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: National Natural Science Foundation of China (U1705264, 61572132); Natural Science Foundation of Fujian Province (2019J01275); Guangxi Key Laboratory of Trusted Software (KX202039)

收稿日期: 2021-02-28 定稿日期: 2021-05-01

3. Pengcheng Laboratory, Artificial Intelligence Research Center, Shenzhen 518055, China
4. School of Physical and Mathematical Sciences, Nanyang Technological University, 308232, Singapore
5. Chongqing Municipal Key Laboratory of Cyberspace and Information Security, Chongqing 400065, China
6. Guangxi Key Laboratory of Trusted Software, Guilin Universityof Electronic Technology, Guilin 541004, China
Corresponding author: LIN Chang-Lu, E-mail: cllin@fjnu.edu.cn

Abstract: Functional Secret Sharing (FSS) is a cryptographic primitive introduced by Boyle et al. at Eurocrypt 2015 and motivated by increasing the efficiency of private information access. Unlike the traditional secret sharing, in which the secret shared among participants is a certain value, the secret shared in FSS is a function. The existing FSS schemes designed by Boyle et al. are constructed based on pseudo-random generators, those schemes are computationally secure and they can only resist the adversaries with limited computing power. In this paper, a threshold FSS scheme with perfect security is constructed by using multi-variable polynomial techniques over finite fields. The core technique is to convert the calculation of the function value of the secret function at the public point in the FSS to the calculation of the function value of the public function at the secret point. It is found that the communication complexity of the proposed scheme is related to the ratio of the reconstruction threshold r and the privacy threshold t. This communication complexity is lower if the ratio is larger. The proposed FSS scheme has the properties such as simplicity, compressibility, and function privacy. The good performance and properties show that the proposed scheme is suitable to the design of some new private information access protocols.

Key words: function secret sharing; threshold secret sharing; perfect security; private information retrieval (PIR)

1 引言

1979 年, Shamir [1] 和 Blakly [2] 分别独立提出秘密分享的概念并给出了具体构造方案, 他们的方案被称为 (t,n)-门限秘密分享方案. 在 (t,n)-门限秘密分享方案中, 通常包括 1 个分发者和 n 个参与者, 在秘密的分发阶段分发者将秘密分为 n 个子秘密发送给相应的参与者; 在重构阶段任意大于 t 个参与者合作可以重构出秘密, 任意 t 个或者少于 t 个参与者则得不到关于秘密的任何信息. 秘密分享在密码学和分布式计算中有许多应用, 如拜占庭协议 [3]、安全多方计算 [4–6]、门限密码学 [7,8] 等.

Chor 等人 [9] 最早考虑了用户私密信息存取问题中的一种场景, 即用户想要从服务器管理的数据库中恢复某一信息, 同时服务器不知道用户恢复信息的内容, 将解决此类问题的模型称之为私密信息检索 (Private information retrieval, PIR) 协议, 并用通信复杂度表示 PIR 协议中用户和服务器之间传输信息的总量, 用于衡量协议的传输效率.

为了降低私密信息存取协议的通信复杂度, Boyle 等人 [10] 在 2015 年欧密会上提出了函数秘密分享 (Function Secret Sharing, FSS) 的概念. 通过设计高效的 FSS 方案, 并将其转换为具有同级别通信复杂度的私密信息存取协议, 从而实现降低私密信息存取协议通信复杂度的目的. 传统的秘密分享方案在参与者之间分享的秘密为某一确定的值, 而 FSS 方案分享的秘密是一般的函数. 通常地, FSS 方案包含三个算法, 即子函数生成算法、子函数函数值计算算法和秘密函数函数值重构算法, 它们可简单地描述如下: 在分发阶段, 分发者通过子函数生成算法将秘密函数分为多个子函数发送给对应的参与者; 在子函数值计算阶段, 参与者确定秘密函数定义域中的点后, 通过子函数函数值计算算法计算子函数在该点处的函数值; 在重构阶段, 所有参与者联合起来用计算得到的子函数函数值重构出秘密函数在该点处的函数值. FSS 方案的安全性要求秘密函数子函数集合的任何真子集不能得到关于被分享函数的任何信息.

实质上, FSS 方案是对 Gilboa 等人 [11] 的分布式点函数 (Distributed Point Function, DPF) 方案的延伸和拓展. 假设点函数的定义域为 $\{0,1\}^l$, 值域为 $\mathbb{G}$, 则对任意的 $x\in\{0,1\}^l$, 该函数 $f_{\alpha,\beta}$ 满足: 若

$x=\alpha$, 有 $f_{\alpha,\beta}(x)=\beta$; 若 $x\neq a$, 有 $f_{\alpha,\beta}(x)=0$. 易知, 此 DPF 方案是参与者个数为 2 且秘密函数为点函数的 FSS 方案. 在文献 [11] 中, Gilboa 等人将秘密函数 $f_{\alpha,\beta}$ 的所有函数值排列为长度为 2^l 长的向量, 应用两方的加法秘密分享方案将该向量分为两个长度为 2^l 的向量作为秘密函数 $f_{\alpha,\beta}$ 的两个子函数. 同时, 利用伪随机生成器生成的伪随机序列来替代子函数中的随机序列的方式, 他们构造了子函数长度为 $O(\lambda l^{\log 3})$ 的 DPF 方案 (其中 λ 为伪随机生成器的种子长度), 并将所设计的 DPF 方案转化得到了通信复杂度为数据库大小对数级别的两服务器计算意义下安全的 PIR 协议. 因为在文献 [11] 中的分布式点函数方案的构造使用了伪随机生成器, 所以其方案的安全性基于密码学中单向函数 [12] 的存在性假设, 它是计算意义下安全, 即仅可以抵抗计算能力有限的敌手.

FSS 方案的通信复杂度是用于衡量执行该 FSS 方案所需要传输信息的总长度, 它是决定基于 FSS 方案设计的私密信息存取协议效率高低的关键参数, 它也成为国内外学者关注的焦点. 目前关于 FSS 方案的研究主要是沿着构造通信复杂度更低的计算意义 (computational) 或完善 (perfect) 安全的 FSS 方案的方向进行. 2015 年, Boyle 等人 [10] 运用二叉树的技术将文献 [11] 中方案的通信复杂度从 $O(\lambda l^{\log 3})$ 降低到 $O(\lambda l)$. Boyle 等人 [13] 运用张量运算简化了文献 [10] 中方案的构造, 并将其方案的通信复杂度降低为原来的四分之一. 这些构造的安全性均是基于单向函数的存在性假设, 属于计算意义下安全性; 但是它们均能满足函数秘密分享的简洁性、压缩性以及函数私密性. 近期, Luo 等人 [14] 扩展文献 [10,13] 中的构造, 不仅提出了门限函数秘密分享 (Threshold Function Secret Sharing, TFSS) 概念, 而且还给出了完善安全的 TFSS 方案构造, 该方案的通信复杂度为 $O(l)$. Li 和 Zhang [15] 进一步研究了完善安全的门限函数秘密分享, 给出从完善安全的 PIR 协议构造完善安全的 TFSS 方案的一般构造, 并利用互信息熵的概念讨论了函数隐私性. 罗景龙等人 [16] 基于 Shamir 门限秘密分享构造了一个安全的 TFSS 方案, 该方案的通信复杂度为 $O(l)$; 同时指出 Yuan 等人的函数秘密分享方案 [17] 不满足函数安全性. 但是, 这些完善安全的 TFSS 方案均无法同时满足函数秘密分享的简洁性、压缩性以及函数私密性. 上述这些函数秘密分享方案的效率与性质见表 1.

表 **1** 函数秘密分享方案效率与性质对比

Table 1 Efficiencies and properties of function secret sharing schemes

方案	(t,r,n)	通信复杂度	安全性	简洁性	压缩性	函数私密性
Gilboa 等人 [11]	$(1,2,2)$	$O(\lambda l^{\log 3})$	计算意义	√	√	√
Boyle 等人 [10]	$(1,2,2)$	$O(\lambda l)$	计算意义	√	√	√
Boyle 等人 [13]	$(1,2,2)$	$O(\lambda l)$	计算意义	√	√	√
Boyle 等人 [10]	$(n-1,n,n)$	$O(\lambda 2^{l/2}2^{(n-1)/2})$	计算意义	√	√	√
Luo 等人 [14]	$(r-1,r,n)$	$O(l)$	完善	√	×	×
Li 和 Zhang [15]	$(r-1,r,n)$	与所依赖的 PIR 一样	完善	√	√	×
罗景龙等人 [16]	$(r-1,r,n)$	$O(l)$	完善	√	√	×
本文构造	(t,r,n)	$O(N^{1/\lfloor (r-1)/t\rfloor})$	完善	√	√	√

注: t 为重构门限值, r 为私密门限值, n 为参与者个数, l 为函数定义域的比特规模且 $N=2^l$, λ 为伪随机生成器的种子长度.

Bolye 等人 [10] 在提出了函数秘密分享的概念和构造的同时, 还阐述了它与密码学中的其他概念之间存在着紧密的联系, 如同态秘密分享 [18–20]、全同态加密 [21,22]. FSS 在实际生活中也具有丰富的应用. Wang 等人 [23] 基于 FSS 方案构造了 “Splinter” 系统, 可以支持对公开数据库进行种类丰富的私密信息的查询功能. Boyle 等人 [24] 将 FSS 方案用于安全多方计算的预处理, 提高了安全计算协议的整体效率.

考虑到现有所构造的 (t,r,n)-FSS 方案均无法同时满足函数秘密分享在实际应用中所需要的简洁性、压缩性和函数私密性. 本文利用文献 [9,25] 中的多变量多项式技术, 将 FSS 方案中秘密函数 $f_{\alpha,\beta}:\{0,1\}^l\to\{0,1\}^m$ 在某一公开点 $\alpha'\in\{0,1\}^l$ 处的函数值 $f_{\alpha,\beta}(\alpha')$ 的计算问题转换为某一公开函数 $f(\lambda)$ 在某一秘密点 $H_\beta(\alpha)$ 处的函数值计算问题. 通过这种转换分发者可以将秘密函数 $f_{\alpha,\beta}$ 拆分为 n 个子函数 $f_1,\cdots,f_n$ 发送给相应的参与者, 使得 n 个参与者中的任意 r 个可以重构出秘密函数 $f_{\alpha,\beta}$ 在 $\alpha'\in\{0,1\}^l$

处的函数值 $f_{\alpha,\beta}(\alpha')$, 任意 t 个或少于 t 个参与者则不能得到关于秘密函数 $f_{\alpha,\beta}$ 的任何信息. 本文还采用 $\mathbb{F}_q$ 上的常数项为 "0" 的 $r-1$ 次随机多项式进行掩盖秘密的方法, 构造了可以同时满足简洁性, 压缩性和函数私密性的 (t,r,n)-FSS 方案. 本文方案的效率和性质与现有函数秘密分享方案的比较信息见表 1.

本文的组织结构如下: 第 2 节给出本文所需要的相关概念与知识; 第 3 节简要介绍多变量多项式以及把它用于构造函数秘密分享的思想; 第 4 节对本文方案进行描述与分析; 第 5 节将本文方案与现有的函数秘密分享方案在效率与性质方面作比较分析; 第 6 节对本文工作进行了总结.

2 预备知识

秘密分享由 Shamir [1] 和 Blakly [2] 分别独立提出, 他们所设计的方案被称为 (t,n)-门限秘密分享方案, 其中 n 表示参与者个数, t 表示门限值. 在分发阶段分发者将秘密分为 n 个子秘密, 安全地发送给对应的参与者, 在重构阶段, 任意 $t+1$ 个参与者合作可以正确地重构出秘密, 其安全性要求任意 t 个或少于 t 个参与者不能得到秘密的任何信息. Shamir (t,n)-门限秘密分享方案的形式化定义如下:

定义 1 (Shamir (t,n)-门限方案 [1]) 令 $\mathbb{F}_q$ 为 q 元有限域, 其中 q 为大素数且 $q>n$. 令 $\lambda_1,\cdots,\lambda_n$ 为 $\mathbb{F}_q$ 上两两不同的非零公开值, D 为可信的分发者, $P_1,\cdots,P_n$ 为 n 个参与者, 则称如下定义的秘密分享方案为 Shamir (t,n)-门限方案.

- **分发阶段**: 给定秘密 $s\in\mathbb{F}_q$, 分发者 D 构造常数项为 s 的 t 次多项式 $f(x)=s+a_1x+\cdots+a_tx^t$, 其中 a_i $(i=1,\cdots,t)$ 是从 $\mathbb{F}_q$ 中随机选取的. D 运用 $f(x)$ 生成参与者 P_i $(i=1,\cdots,n)$ 的子秘密,
$$s_i=f(\lambda_i),$$
并将每个子秘密 s_i 通过安全信道独立地发送给相应的参与者 P_i.
- **重构阶段**: 参与者集合 $\{P_i\}_{i\in[n]}$ 中的任意 $t+1$ 个参与者 P_{i_τ} $(\tau=1,\cdots,t+1)$ 拿出自己的子秘密 s_{i_τ}, 通过多项式插值公式可计算
$$s=\sum_{\tau=1}^{t+1}b_{i_\tau}\cdot s_{i_\tau}.$$
即重构出秘密 s, 其中 $b_{i_\tau}=\prod_{\tau'=1,\tau'\neq\tau}^{t+1}\frac{\lambda_{i_{\tau'}}}{\lambda_{i_{\tau'}}-\lambda_{i_\tau}}$ 为多项式插值系数.

Shamir (t,n)-门限方案在构造的过程中不基于任何密码学中的困难问题假设, 它被公认为是完善安全的密码原语.

现有的 FSS 方案在重构阶段需要全部参与者的参与, 导致其不能灵活运用于一些实际场景. Luo 等人 [14] 给出了参与者人数为 n, 私密门限为 t, 重构门限为 r 的门限函数秘密分享的形式化定义 (简称为 (t,r,n)-FSS 方案). 其定义思想来源于文献 [10,11,13], 并运用基于游戏的安全模型给出了安全性的形式化定义.

定义 2 (门限函数秘密分享方案 [14]) 令 $\mathbb{F}_q(q>n)$ 为有限域, 1^λ 为安全参数, D 为分发者, n 为参与者的个数, t 为私密门限值, r 为重构门限值. 设 $f:D_f\to R_f$ 为可有效的计算并能被简洁描述的函数, 则关于秘密函数 f 的门限函数秘密分享方案包含以下三个概率多项式时间算法 (**Gen, Eval, Dec**):

- **Gen**$(1^\lambda,f)\to(k_1,\cdots,k_n)$: 此算法为子函数生成算法, D 输入安全参数 1^λ, 秘密函数 f, 此算法输出秘密函数 f 的 n 个子函数 $(k_1,\cdots,k_n)$.
- **Eval**$(i,k_i,x)\to y_i$: 此算法为子函数计算算法, 对于给定的 $x\in D_f$, 当参与者 P_i $(i=1,\cdots,n)$ 收到子函数 k_i 后, 输入 (i,k_i,x), 此算法输出子函数 k_i 在 x 点处的函数值 y_i.
- **Dec**$((\lambda_{i_1},y_{i_1}),\cdots,(\lambda_{i_r},y_{i_r}))\to s$: 此算法为输出解码器, 收到任意 r 个子函数在 $x\in D_f$ 处的函数值 $y_{i_1},\cdots,y_{i_r}$ 后, 此算法输出秘密函数 f 在 x 点处的函数值 $f(x)$.

针对上述所定义的 (t,r,n)-FSS 方案, 要求其满足以下正确性和安全性要求:

正确性: (t,r,n)-FSS 的正确性要求当算法 (**Gen**, **Eval**, **Dec**) 正确执行时, 在重构阶段, 任意 r 个参

与者可以利用计算算法 **Eval** 的输出值重构出秘密函数 f 在 x 点处的函数值 $f(x)$. 用数学语言可以描述如下:

$$\begin{aligned}&\Pr[(k_1,\cdots,k_n)\leftarrow\mathbf{Gen}(1^\lambda,f):\mathbf{Dec}\\&((i_1,\mathbf{Eval}(i_1,k_{i_1},x)),\cdots,(i_r,\mathbf{Eval}(i_r,k_{i_r},x)))=f(x)]=1,\end{aligned}\tag{1}$$

即对任意的可以有效计算的且能被简洁地描述的函数 $f:D_f\to R_f$, 任意的 $x\in D_f$, 集合 $\{i_1,\cdots,i_r\}\subseteq[n]$, 当算法 (**Gen**, **Eval**, **Dec**) 均正确执行时, 秘密函数 f 在 x 点处的函数值 $f(x)$ 被正确重构的概率为 "1".

***t*-安全性**: 假设存在受贿参与者集合 $T\subseteq\{P_1,\cdots,P_n\}$ 且 $|T|=t$, 则关于 (t,r,n)-FSS 方案的基于游戏的安全模型具体如下:

- 对任意计算能力无限的敌手 $\mathcal{A}$, 输入安全参数 1^λ, 敌手 $\mathcal{A}$ 生成函数 $(f_0,f_1)\leftarrow\mathcal{A}(1^\lambda)$, 其中 $D_{f_0}=D_{f_1}$, 并将产生的函数 f_0,f_1 发送给挑战者 $\mathcal{C}$.
- 挑战者 $\mathcal{C}$ 收到函数 f_0,f_1 后, 从 $\{0,1\}$ 中随机地选择挑战指数 b, 确定秘密函数 f_b, 执行算法 **Gen** 生成秘密函数 f_b 的子函数 $(k_1,\cdots,k_n)\leftarrow\mathbf{Gen}(1^\lambda,f_b)$.
- 敌手 $\mathcal{A}$ 利用 T 中的受贿参与者所提供的子函数 $\{k_i\}_{i\in T}$, 输出关于挑战指数 b 的猜测 $b'\leftarrow\mathcal{A}(\{k_i\}_{i\in T})$.

令 $\mathrm{Adv}(1^\lambda,\mathcal{A},T):=\Pr[b=b']-\frac{1}{2}$ 为敌手 $\mathcal{A}$ 在上述实验中获得受贿参与者提供的子函数 $\{k_i\}_{i\in T}$ 后对挑战指数 b 进行猜测相对于 $\mathcal{A}$ 随机地对挑战指数 b 进行猜测而言可以猜对 b 的优势. 若对于任意计算能力无限的敌手 $\mathcal{A}$, 参与者个数为 t 的受贿参与者集合 T, 使得在上述不可区分性实验中有 $\mathrm{Adv}(1^\lambda,\mathcal{A},T)=0$ 成立, 则称 (t,r,n)-FSS 方案为完善 t-安全的.

注 1 (完善安全性) 上述安全模型与文献 [10, 11, 13] 中的安全模型定义是一致的. 但这些文献中所设计的 FSS 方案仅为计算意义下安全, 在其安全模型中假设敌手 $\mathcal{A}$ 仅具有有限的计算能力, 并仅限制 $\mathrm{Adv}(1^\lambda,\mathcal{A},T)\le u(\lambda)$, 其中 $u(\lambda)$ 为关于安全参数 1^λ 的可忽略函数 [26]. 不同于文献 [10, 11, 13], 本文专注于考虑完善安全的情形, 即方案的安全性可以抵抗任意具有无限计算能力的敌手, 因此在上述安全模型中假设敌手 $\mathcal{A}$ 具有无限的计算能力, 且要求 $\mathrm{Adv}(1^\lambda,\mathcal{A},T)=0$.

注 2 (鲁棒的解码) 在文献 [10, 11, 13] 中所构造的 FSS 方案的输出解码器 **Dec** 需要收到所有子函数在 x 点的函数值才可以重构出秘密函数 f 在 x 点处的函数值 $f(x)$, 当存在参与者不能参与重构就会导致整个 FSS 方案停止运行. 在定义 2 中给出的 (t,r,n)-FSS 的定义中输出解码器 **Dec** 具有鲁棒性, 只需要收到任意 r 个子函数在 $x\in D_f$ 处的函数值就可以重构处秘密函数 f 在 x 点处的函数值 $f(x)$, 即可以允许 $n-r$ 个参与者不参与重构, 因此可以更加灵活的应用于现实场景中.

定义 3 (通信复杂度) FSS 方案的通信复杂度定义为该 FSS 方案所需要传输的信息的总长度, 它包含两部分: 发送阶段分发者传输给每位参与者的子函数长度之和与重构阶段参与者为完成对秘密函数函数值的重构所进行传输的信息长度之和. 本文用 $\Theta=\Phi+\Psi$ 表示 (t,r,n)-FSS 方案的通信复杂度, 其中 $\Phi=\sum_{i=1}^n|k_i|$ 表示发送阶段发送者传输给每位参与者的子函数长度之和, $\Psi=\sum_{h=1}^r|y_{i_h}|$ 重构阶段参与重构的参与者为了完成重构进行传输的信息长度之和.

根据上述 (t,r,n)-FSS 方案的定义, Shamir (t,n)-门限方案可以看作参与者人数为 n, 私密门限值为 t, 重构门限值为 $t+1$ 的门限秘密分享方案, 为了方便将该方案记作 Shamir $(t,t+1,n)$-门限方案.

不同于传统的秘密分享方案分享, 分享的秘密为有限域 $\mathbb{F}_q$ 上的确定值, 子秘密的大小等于所分享的秘密的大小等于 q, 因此子秘密的大小为常数级别. 而在 FSS 方案中分享的秘密为某一函数, 且一般在 FSS 方案中子函数的长度与秘密函数的定义域大小成线性关系. 当秘密函数的定义域大小为指数级别时, 则构造的 FSS 方案的子函数长度为指数级别, 进而该 FSS 方案的通信复杂度也为指数级别. 考虑到 FSS 方案设计的最初目的是用于提高私密信息存取协议的通信效率, 因此在文献 [10] 中对 FSS 方案提出了简洁性、压缩性和函数私密性的要求.

简洁性: 在 FSS 方案中通过执行子函数生成算法 **Gen** 产生子函数长度的大小级别要小于秘密函数

定义域大小的级别.

压缩性: 在 FSS 方案中通过子函数计算算法 **Eval** 计算得到的子函数的函数值为秘密函数值域中的元素.

函数私密性: 在 FSS 方案中对任意的秘密函数, 当参与者在重构前确定重构该函数在某一点处的函数值后, 要求在重构阶段参与者仅能重构出秘密函数在该点处的函数值, 而得不到秘密函数在其他点处的函数值.

如果要求在 FSS 方案中, 函数值 $f(x')$ 对于参与者来说是完善安全则需要当算法 **Eval** 收到需要计算的点 x 时, 其输出结果 $\{y_1,\cdots,y_n\}$ 将函数值 $f(x')(x'\neq x)$ 的所有信息全部移除, 只保留重构函数 f 在点 x 处的函数值 $f(x)$ 的信息, 其形式化定义如下:

定义 4 (完善安全的函数私密性) 对于 (t,r,n)-FSS 方案, 若存在概率多项式时间算法 $\mathsf{Sim}:\mathbb{F}_q\to\mathbb{F}_q^n$ 对于其分享的任何秘密函数 $f:D_f\to R_f$ 都有以下等式

$$\{\mathsf{Sim}(f(x)),\nabla\}_{x\in D_f}\equiv\{\mathbf{Eval}(1,k_1,x),\cdots,\mathbf{Eval}(n,k_n,x)\}_{x\in D_f}$$

成立, 则称该 (t,r,n)-FSS 方案满足完善安全的函数私密性. 其中, "$X\equiv Y$" 表示随机变量集 X 与 Y 具有相同的概率分布.

注 3 定义 4 的含义是指若 (t,r,n)-FSS 方案满足完善安全的函数私密性, 则存在概率多项式时间算法 $\mathsf{Sim}:\mathbb{F}_q\to\mathbb{F}_q^n$ 可以仅通过函数值 $f(x)$ 以及一些公开信息 "∇" 就可以模拟出该 (t,r,n)-FSS 方案计算算法 **Eval** 的输出结果 $\{y_1,\cdots,y_n\}$, 因此可以说明算法 **Eval** 的输出结果 $\{y_1,\cdots,y_n\}$ 只包含秘密函数 f 在点 x 处的信息而不包含秘密函数 f 在其他点 $x'\in D_f, x'\neq x$ 的函数值 $f(x')$ 的相关信息.

3 多变量多项式与函数秘密分享

本节将简要介绍有限域上多变量多项式, 并分析它在构造安全点函数秘密分享的基本思想. 对任何正整数 N,d,t,r, 令 $d=\lfloor\frac{r-1}{t}\rfloor$, 若等式

$$\binom{m}{d}\geq N,$$

成立, 则参数 m 需要满足 $m\geq dN^{1/d}=dN^{1/\lfloor\frac{r-1}{t}\rfloor}$. 此时令映射 $E:[N]\to\mathbb{F}_q$ 为单射, 且对任意的 $\alpha\in[N]$, 有 $E(\alpha)$ 为长度为 m、汉明重为 d 的 0-1 向量. 对任意的 $\beta\in\mathbb{F}_q$, 令 β 在 $\mathbb{F}_q$ 上分解为 $\beta=\beta_1\cdots\beta_d$, 其中 $\beta_1,\cdots,\beta_d\in\mathbb{F}_q$. 用 β_h 替换向量 $E(\alpha)$ 的第 h $(h=1,\cdots,d)$ 个 "1" 的分量, 可得向量 $H_\beta(\alpha)\in\mathbb{F}_q^m$. 故存在 m 个变量的多项式,

$$F_{\alpha'}(z_1,\cdots,z_m)=\prod_{l:E(\alpha')[l]=1}z_l.$$

当向量 $E(\alpha')(\alpha'\in[N])$ 的重为 d 时, 多项式 $F_{\alpha'}(z_1,\cdots,z_m)$ 的次数为 d. 此外将长度为 m 重为 d 的向量 $H_\beta(\alpha)$ 代入多项式 $F_{\alpha'}(z_1,\cdots,z_m)$ 中有以下等式成立:

$$F_{\alpha'}(H_\beta(\alpha))=\prod_{l:E(\alpha')[l]=1}H_\beta(\alpha)[l]=\begin{cases}\beta, & x=\alpha,\\ 0, & x\neq\alpha.\end{cases}=f_{\alpha,\beta}(\alpha'). \tag{2}$$

本文将利用式 (2) 把 FSS 方案中计算秘密函数 $f_{\alpha,\beta}(x):\{0,1\}^l\to\mathbb{F}_q$ 在某一公开点 $\alpha'\in\{0,1\}^l$ 处的函数值 $f_{\alpha,\beta}(\alpha')$ 的问题, 转换为计算公开函数 $F_{\alpha'}(\cdot)$ 在秘密点 $H_\beta(\alpha)$ 处函数值的问题. 通过此转换, 任意 $r=dt+1$ 个参与者可以重构出秘密函数 $f_{\alpha,\beta}$ 在点 $\alpha'\in\{0,1\}^l$ 处的函数值 $f_{\alpha,\beta}(\alpha')$ 且任意 t 个或少于 t 个参与者不能得到关于秘密函数 $f_{\alpha,\beta}$ 的任何信息, 具体过程如下:

对任意 t 个向量 $V^1,\cdots,V^t\in\mathbb{F}_q^m$, 令

$$Q(\lambda)=H_\beta(\alpha)+\lambda V^1+\cdots+\lambda^t V^t=(Q(\lambda)_1,\cdots,Q(\lambda)_m).$$

此时 $Q(\lambda)_l$ $(l=1,\cdots,m)$ 为关于 λ 的 t 次随机多项式. 因为 $d=\lfloor\frac{r-1}{t}\rfloor$, 所以

$$F_{\alpha'}(Q(\lambda))=F_{\alpha'}(Q(\lambda)_1,\cdots,Q(\lambda)_m)=\prod_{l:E(\alpha')[l]=1}Q(\lambda)_l. \tag{3}$$

易知, 式(3)是关于 λ 的 $dt=r-1$ 次多项式.

因为多项式 $F_{\alpha'}(Q(\lambda))$ 为 $Q(\lambda)_l(l=1,\cdots,m)$ 中的 d 个多项式的乘积, 所以 $F_{\alpha'}(Q(\lambda))$ 为 $\mathbb{F}_q$ 上的可约多项式, 故多项式 $F_{\alpha'}(Q(\lambda))$ 不是 $\mathbb{F}_q$ 上关于变量 λ 的随机多项式. 为了使得本节所构造的 (t,r,n)-FSS 方案满足完善安全的函数私密性, 本文选取 $\mathbb{F}_q$ 上常数项为 "0" 的 $r-1$ 次随机多项式来掩盖多项式 $F_{\alpha'}(Q(\lambda))$ 得到 $\mathbb{F}_q$ 上的随机多项式 $f(\lambda)$. 令多项式 $R(\lambda)=0+a_1\lambda+\cdots+a_{r-1}\lambda^{r-1}$, 为定义在 $\mathbb{F}_q$ 上常数项为 "0" 的 $r-1$ 次随机多项式, 其中 $a_1,\cdots,a_{r-1}$ 是从 $\mathbb{F}_q$ 上随机独立选取的. 令

$$f(\lambda)=F_{\alpha'}(Q(\lambda))+R(\lambda).$$

因为 $R(\lambda)$ 为定义在 $\mathbb{F}_q$ 上关于变量 λ 的 $r-1$ 次随机多项式, 因此 $f(\lambda)$ 也为定义在 $\mathbb{F}_q$ 上的关于变量 λ 的 $r-1$ 次随机多项式且多项式 $f(\lambda)$ 的常数项

$$f(0)=F_{\alpha'}(H_\beta(\alpha))=f_{\alpha,\beta}(\alpha').$$

令 $\lambda_1,\cdots,\lambda_n$ 为 $\mathbb{F}_q$ 上的 n 个两两不同的非零公开值, 因为多项式 $f(\lambda)$ 为关于变量 λ 的 $r-1$ 次随机多项式, 使用 $f(\lambda)$ 的任意 r 个值 $f(\lambda_1),\cdots,f(\lambda_r)$ 可以通过多项式插值得到 $f(\lambda)$ 的常数项 $f(0)=f_{\alpha,\beta}(\alpha')$. 另一方面因为向量 $Q(\lambda)$ 的每一个分量 $Q(\lambda)_l$ $(l=1,\cdots,m)$ 为关于 λ 的 t 次随机多项式, 其中 $Q(0)=H_\beta(\alpha)$. $Q(\lambda_1),\cdots,Q(\lambda_n)\in\mathbb{F}_q^m$, 则 $Q(\lambda_1),\cdots,Q(\lambda_n)$ 中任意 t 个或少于 t 个值不包含 $H_\beta(\alpha)$ 的任何信息.

4 方案构造

在上节分析的基础上构造关于点函数 $f_{\alpha,\beta}(x):\{0,1\}^l\to\mathbb{F}_q$ 完善安全的 (t,r,n)-FSS 方案, 并将分析该方案能同时满足简洁性、压缩性和函数私密性.

4.1 方案描述

假设分享的秘密函数为 $f_{\alpha,\beta}(x):\{0,1\}^l\to\mathbb{F}_q$, 分发者为 D, 参与者人数为 n, 私密门限为 t, 重构门限为 r, 且有 $t<r<n$, 则完善安全的门限函数秘密分享方案由算法 **(Gen, Eval, Dec)** 组成的三元组, 具体描述如下:

- **Gen**$(1^\lambda,f_{\alpha,\beta})\to(k_1,\cdots,k_n)$.
  1) 分发者 D 随机独立地选取 t 个 m 长的向量 $V^1,\cdots,V^t\in\mathbb{F}_q^m$ 和有限域 $\mathbb{F}_q$ 上的值 $a_1,\cdots,a_{r-1}$.
  2) 分发者 D 生成多项式 $Q(\lambda)=H_\beta(\alpha)+\lambda V^1+\cdots+\lambda^tV^t$, $R(\lambda)=0+a_1\lambda+\cdots+a_{r-1}\lambda^{r-1}$.
  3) 分发者 D 计算 $k_i=(Q(\lambda_i),R(\lambda_i))$ $(i=1,\cdots,n)$.
  4) 输出 $(k_1,\cdots,k_n)$.
- **Eval**$(i,k_i,\alpha')\to y_i$.
  1) 对任意的 $\alpha'\in\{0,1\}^l$, 参与者 P_i 计算 $y_i=f(\lambda_i)=F_{\alpha'}(Q(\lambda_i))+R(\lambda_i)$, 其中 $F_{\alpha'}$ 定义在等式 (2) 中.

2) 输出 y_i $(i=1,\cdots,n)$.

- **Dec**$((\lambda_{i_1},y_{i_1}),\cdots,(\lambda_{i_t},y_{i_t}))\to s$.

1) 输出 $s=\Sigma_{h=1}^{r}b_{i_h}\cdot y_{i_h}$, 其中 $b_{i_h}=\prod_{h'=1,h'\neq h}^{r}\frac{\lambda_{i_{h'}}}{\lambda_{i_{h'}}-\lambda_{i_h}}$.

4.2 方案分析

本节将对上述所构造方案进行正确性分析、安全性证明和通信复杂度分析, 并对在实际应用中所需要的简洁性、压缩性、函数私密性也进行详细分析.

定理 1 令 $\mathbb{F}_q$ 为有限域, 1^λ 为安全参数, 则本文所构造的 FSS 方案 **(Gen, Eval, Dec)** 是关于点函数 $f_{\alpha,\beta}:\{0,1\}^l\to\mathbb{F}_q$ 完善安全的门限函数秘密分享方案, 其通信复杂度为 $O(N^{1/\lfloor(r-1)/t\rfloor})$, 其中 $N=2^l$.

证明: 根据定义 2 中所给出的关于函数秘密分享方案的形式化定义, 需要证明本文方案满足正确性和 t-安全性.

正确性: 根据本文 **(Gen, Eval, Dec)** 的构造要证明其正确性只需要证明如下等式成立,

$$\begin{aligned}\Pr[(k_1,\cdots,k_n)\leftarrow\mathbf{Gen}(1^\lambda,\alpha,\beta):\mathbf{Dec}((i_1,\mathbf{Eval}(i_1,k_{i_1},\alpha')),\\ \cdots,(i_r,\mathbf{Eval}(i_r,k_{i_r},\alpha')))=f_{\alpha,\beta}(\alpha')]=1.\end{aligned}$$

即当三个算法 **(Gen, Eval, Dec)** 可以正确且顺利地执行时, 秘密函数 $f_{\alpha,\beta}$ 在 α' 点处的函数值可以被成功重构的概率为 "1".

若算法 **(Gen, Eval, Dec)** 正确且顺利地执行, 则子函数生成算法可以正确地生成子函数 $k_i=(Q(\lambda_i),R(\lambda_i))$ $(i=1,\cdots,n)$. 因为 $f(\lambda)$ 为定义在 $\mathbb{F}_q$ 上的关于变量 λ 的 $r-1$ 次随机多项式且其常数项为 $f(0)=F_{\alpha'}(H_\beta(\alpha))=f_{\alpha,\beta}(\alpha')$. 对 $\mathbb{F}_q$ 上两两不同的非零公开值 $\lambda_1,\cdots,\lambda_n$, 每个参与者 P_i $(i=1,\cdots,n)$ 执行子函数计算算法 **Eval** 输出 $y_i=\mathsf{Eval}(i,k_i,\alpha')=f(\lambda_i)$, 它们是多项式 $f(\lambda)$ 的 n 个值. 当输出解码器 **Dec** 收到任意 r 个值 $y_{i_h}=f(\lambda_{i_h})$ $(h=1,\cdots,r)$ 后可以通过多项式插值计算出多项式 $f(\lambda)$ 的常数项 $f(0)=\mathsf{Dec}((i_1,y_{i_1}),\cdots,(i_r,y_{i_r}))=\sum_{h=1}^{r}b_{i_h}\cdot y_{i_h}=F_{\alpha'}(H_\beta(\alpha))=f_{\alpha,\beta}(\alpha')$, 进而重构出秘密函数 $f_{\alpha,\beta}$ 在 α' 点处的函数值. 综上, 正确性得证.

t-安全性: 通过考虑以下存在受贿参与者集合 $T\subset\{P_1,\cdots,P_n\},|T|=t$, 具有无限计算能力敌手 $\mathcal{A}$ 的基于游戏的安全模型来证明本文方案的 t-安全性. 不失一般性假设 $T=\{P_1,\cdots,P_t\}$.

- 具有无限计算能力的敌手 $\mathcal{A}$ 输入安全参数 1^λ 生成 $(f_{\alpha^0,\beta^0},f_{\alpha^1,\beta^1})\leftarrow\mathcal{A}(1^\lambda)$, 其中 $D_{f_{\alpha^0,\beta^0}}=D_{f_{\alpha^1,\beta^1}}$, $\alpha^0,\alpha^1\in[N]$, $\beta^0,\beta^1\in\mathbb{F}_q$, 并将产生的函数 $(f_{\alpha^0,\beta^0},f_{\alpha^1,\beta^1})$ 发送给挑战者 $\mathcal{C}$.
- 挑战者 $\mathcal{C}$ 从 $\{0,1\}$ 中随机地选择一个挑战值 b, 确定秘密函数 f_{α^b,β^b} 并按如下过程执行子函数生成算法 **Gen** 输入秘密函数 f_{α^b,β^b}.

  1) 分发者 D 随机独立地选取 t 个 m 长的向量 $V^1,\cdots,V^t\in\mathbb{F}_q^m$ 和 $a_1,\cdots,a_{r-1}\in\mathbb{F}_q$.

  2) 分发者 D 生成多项式 $Q(\lambda)=H_{\beta^b}(\alpha^b)+\lambda V^1+\cdots+\lambda^tV^t$, $R(\lambda)=0+a_1\lambda+\cdots+a_{r-1}\lambda^{r-1}$.

  3) 分发者 D 计算 $k_i=(Q(\lambda_i),R(\lambda_i))(i=1,\cdots,n)$.

  4) 输出 $(k_1,\cdots,k_n)$.
- 敌手 $\mathcal{A}$ 利用受贿参与者集合 T 中的受贿参与者所提供的子函数 $\{k_i\}_{i\in T}$, 给出关于挑战指数 b 的猜测 $b'\leftarrow\mathcal{A}(\{k_i\}_{i\in T})$.

根据本文方案的构造可知秘密子函数 $k_i=(Q(\lambda_i),R(\lambda_i))$, 可以对 $Q(\lambda_i)$ 和 $R(\lambda_i)$ 分别进行如下分析:

首先, 在方案中 $Q(\lambda)=H_{\beta^b}(\alpha^b)+\lambda V^1+\cdots+\lambda^tV^t$, $\lambda_1,\cdots,\lambda_n$ 为 $\mathbb{F}_q$ 上的两两不同的非零公开值,

因此 $\{Q(\lambda_i)\}_{i\in T}$ 满足以下等式:

$$\underbrace{\begin{pmatrix} Q(\lambda_1) \\ Q(\lambda_2) \\ \vdots \\ Q(\lambda_t) \end{pmatrix}}_{Q} = \underbrace{\begin{pmatrix} \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^t \\ \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^t \\ \vdots & \vdots & & \vdots \\ \lambda_t & \lambda_t^2 & \cdots & \lambda_t^t \end{pmatrix}}_{\Lambda} \underbrace{\begin{pmatrix} V^1 \\ V^2 \\ \vdots \\ V^t \end{pmatrix}}_{V} + \underbrace{\begin{pmatrix} H_{\beta^b}(\alpha^b) \\ H_{\beta^b}(\alpha^b) \\ \vdots \\ H_{\beta^b}(\alpha^b) \end{pmatrix}}_{H}. \tag{4}$$

在式 (4) 中因为 V 为 $t\times m$ 的随机矩阵, Λ 为 t 阶非退化矩阵, 又 $Q=\Lambda V+H$ 且 H 是 $t\times m$ 的未知常矩阵, 则矩阵 Q 为 $t\times m$ 的随机矩阵. 因此, 敌手通过矩阵 Q 得不到关于矩阵 H 的任何信息, 即敌手无法获知关于挑战指数 b 的任何信息.

其次, $R(\lambda_i)$ 为多项式 $R(\lambda)=0+a_1\lambda+\cdots+a_{r-1}\lambda^{r-1}$ 在 λ_i 点处的取值, 因为多项式 $R(\lambda)$ 不包含挑战指数 b 的信息, 故 $R(\lambda_i)$ 中不包含关于挑战指数 b 的任何信息. 因此, $\{k_i\}_{i\in T}$ 中不包含关于挑战指数 b 的任何信息. 综上, 敌手猜对挑战指数 b 的概率为 $\Pr[b'=b]=1/2$, 即可证得本文所构造的方案具有完善的 t-安全性. □

通信复杂度: 本文构造的 FSS 方案中, 子函数 $k_i=(Q(\lambda_i),R(\lambda_i))$ 其中 $Q(\lambda_i)\in\mathbb{F}_q^m, R(\lambda_i)\in\mathbb{F}_q$, 则 $|Q(\lambda_i)|=m\log q, |R(\lambda_i)|=\log q$, 因此 $\Phi=n(m+1)\log q$. 子函数计算算法的输出值 $y_i=\mathsf{Eval}(i,k_i,\alpha')=F_{\alpha'}(k_i)=f(\lambda_i)$ $(i=1,\cdots,n)$, 因为 $f(\lambda)$ 是 $\mathbb{F}_q$ 上的多项式, 则 $y_i\in\mathbb{F}_q$, 因此有 $\Psi=r\log q$, 又 $m=dN^{1/\lfloor(r-1)/t\rfloor}$, 所以本文方案的通信复杂度为 $\Theta=\Phi+\Psi=n(m+2)\log q=O(N^{1/\lfloor(r-1)/t\rfloor})$.

最后, 本文构造的函数秘密分享方案能同时满足简洁性、压缩性和函数私密性, 具体分析如下:

简洁性: 本文构造的 FSS 方案中, $k_i=(Q(\lambda_i),R(\lambda_i))$ $(i=1,\cdots,n)$, 其长度 $|k|=(m+1)\log q=(N^{1/\lfloor(r-1)/t\rfloor}+1)\log q=O(N^{1/\lfloor(r-1)/t\rfloor})$; 当 $r-1>t$ 时, 该子函数的长度小于秘密函数 $f_{\alpha,\beta}$ 的定义域 D_f 大小的级别, 因此本文方案满足简洁性.

压缩性: 本文构造的 FSS 分享方案中子函数计算算法 $\mathbf{Eval}$ 的输出值 $y_i=\mathsf{Eval}(i,k_i,\alpha')=F_{\alpha'}(k_i)=f(\lambda_i)$. 因为 $f(\lambda)$ 为有限域 $\mathbb{F}_q$ 上的多项式, 因此 y_i 为 $f_{\alpha,\beta}$ 值域 $\mathbb{F}_q$ 中的值, 且参与者可以通过 y_i 的线性组合 $s=\sum_{h=1}^r b_{i_h}\cdot y_{i_h}$, 其中 $b_{i_h}=\prod_{h'=1,h'\neq h}^r\frac{\lambda_{i_{h'}}}{\lambda_{i_{h'}}-\lambda_{i_h}}$, 重构秘密函数 $f_{\alpha,\beta}$ 在 α' 点处的函数值 $f_{\alpha,\beta}(\alpha')$. 因此本文方案满足压缩性.

完善安全的函数私密性: 本文构造的 FSS 方案中, 因为 $R(\lambda)$ 为有限域 $\mathbb{F}_q$ 上的随机多项式, $f(\lambda)=F_{\alpha'}(Q(\lambda))+R(\lambda)$, 所以 $f(\lambda)$ 也为有限域 $\mathbb{F}_q$ 上的随机多项式, 且 $f(0)=F_{\alpha'}(H_\beta(\alpha))$. 因为 $y_i=f(\lambda_i)$, 所以 $f(0)=\sum_{h=1}^r b_{i_h}\cdot y_{i_h}=f_{\alpha,\beta}(\alpha')$, 其中 $b_{i_h}=\prod_{h'=1,h'\neq h}^r\frac{\lambda_{i'_h}}{\lambda_{i'_h}-\lambda_{i_h}}$ 为多项式插值系数, 进而 $\{y_1,\cdots,y_n\}=\{\mathsf{Eval}(1,k_1,x),\cdots,\mathsf{Eval}(n,k_n,x)\}_{x\in D_f}$ 在 $\mathbb{F}_q$ 上是关于条件 $f_{\alpha,\beta}(\alpha')=\sum_{h=1}^r b_{i_h}\cdot y_{i_h}$ 的随机均匀分布. 此时存在概率多项式时间的算法 Sim 从 $\mathbb{F}_q$ 上随机均匀地选取 $b_1,\cdots,b_{r-1}$ 产生多项式 $H(x)=f_{\alpha,\beta}(\alpha')+b_1x+\cdots+b_{r-1}x^{r-1}$. 利用多项式 $H(x)$ 以及公开值 $\nabla=(\lambda_1,\cdots,\lambda_n)$, 算法 Sim 可以模拟出概率分布 $\{\mathsf{Sim}(f_{\alpha,\beta}(\alpha')),\nabla\}_{x\in D_f}=\{y'_1,\cdots,y'_n\}, y'_i=g(\lambda_i)$ $(i=1,\cdots,n)$ 为 $\mathbb{F}_q$ 上关于条件 $f_{\alpha,\beta}(\alpha')=\sum_{h=1}^r b_{i_h}\cdot y'_{i_h}$ 的随机均匀分布. 因此 $\{y'_1,\cdots,y'_n\}\equiv\{y_1,\cdots,y_n\}$, 所以

$$\{\mathsf{Sim}(f_{\alpha,\beta}(\alpha')),\nabla\}_{x\in D_f}\equiv\{\mathbf{Eval}(1,k_1,x),\cdots,\mathbf{Eval}(n,k_n,x)\}_{x\in D_f}.$$

综上由定义4可知本文方案满足完善安全的函数私密性.

5 方案比较

本节将基于多变量多项式的 (t,r,n)-FSS 方案与现有的 FSS 方案在效率和性质方面进行比较. 将它与现有的文献 [10,11,13–16] 在安全性、有无门限值及方案的通信复杂度进行比较; 对其是否满足简洁性、

压缩性和函数私密性进行比对. 假设所有 FSS 方案分享的秘密函数均为点函数 $f_{\alpha,\beta}:\{0,1\}^l\to\mathbb{F}_q$, t 表示私密门限值, n 为参与者个数, λ 为伪随机生成器的种子长度. 具体比较结果见表 1.

经过比较发现本文方案相对于文献 [10, 11, 13] 中的 FSS 方案具有额外的门限特性, 在重构的过程中可以容忍 $n-r$ 参与者不参与, 因此可以更加灵活地应用于现实场景; 该方案还是完善安全的. 当分享的秘密函数为 $f_{\alpha,\beta}:\{0,1\}^l\to\mathbb{F}_q$ 时, 本文方案的通信复杂为 $O(N^{1/\lfloor(r-1)/t\rfloor})$(其中 $N=2^l$), 它与方案的重构门限值 r 和私密门限值 t 相关. 本文方案为了实现具有完善的函数私密性牺牲了方案的通信效率, 但是当 r 与 t 的比值较大时本文方案可以实现较低的通信复杂度. 与文献 [14–16] 相比, 从表 1 可看出本文方案可以同时满足 FSS 在实际应用中所需要的简洁性, 压缩性以及函数私密性, 因此可以更好地适用于设计各类私密信息存取, 如私密信息检索协议等.

6 总结

本文基于多变量多项式技术构造了新的 (t,r,n)-FSS 方案, 按照函数秘密分享形式化的安全定义对其进行了相应的安全证明与分析. 将本文方案与现有相关工作作对比, 经过分析发现本文方案的通信复杂度与方案重构门限值 r 和私密门限值 t 之间的比值相关, 当重构门限值与私密门限值之间的比值较大时, 该方案可以实现较低的通信复杂度. 此外, 本文方案可以同时满足函数秘密分享的简洁性、压缩性及函数私密性.

参考文献

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

[2] BLAKEY G R. Safeguarding cryptographic keys[C]. In: Proceedings of 1979 International Workshop on Managing Requirements Knowledge (MARK). IEEE, 1979: 313–318. [DOI: 10.1109/MARK.1979.8817296]

[3] SIU H S, CHIN Y H, YANG W P. Byzantine agreement in the presence of mixed faults on processors and links[J]. IEEE Transactions on Parallel and Distributed Systems, 1998, 9(4): 335–345. [DOI: 10.1109/71.667895]

[4] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game[C]. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing. ACM, 1987: 218–229. [DOI: 10.1145/28395.28420]

[5] LIU J, TIAN Y, ZHOU Y, et al. Privacy preserving distributed data mining based on secure multi-party computation[J]. Computer Communications, 2020, 153: 208–216. [DOI: 10.1016/j.comcom.2020.02.014]

[6] YAO A. C. How to generate and exchange secrets[C]. In: Proceedings of the 27th Annual Symposium on Foundations of Computer Science. IEEE, 1986: 162–167. [DOI: 10.1109/SFCS.1986.25]

[7] DESMEDT Y, FRANKEL Y. Threshold cryptosystems[C]. In: Advances in cryptology—CRYPTO '89. Springer Berlin Heidelberg, 1989: 307–315. [DOI: 10.1007/0-387-34805-0_28]

[8] HARN L, LIN C L. Asynchronous secret reconstruction and its application to the threshold cryptography[J]. International Journal of Communications, Network and System Sciences, 2014, 1: 22–29. [DOI: 10.4236/ijcns.2014.71003]

[9] CHOR B, GOLDREICH O, KUSHILEVITZ E, et al. Private information retrieval[C]. In: Proceedings of the 36th Annual Symposium on Foundations of Computer Science. IEEE, 1995: 965–982. [DOI: 10.1109/SFCS.1995.492461]

[10] BOYLE E, GILBOA N, ISHAI Y. Function secret sharing[C]. In: Advances in Cryptology—EUROCRYPT 2015, Part II. Springer Berlin Heidelberg, 2015: 337–367. [DOI: 10.1007/978-3-662-46803-6_12]

[11] GILBOA N, ISHAI Y. Distributed point functions and their applications[C]. In: Advances in Cryptology—EUROCRYPT 2014. Springer Berlin Heidelberg, 2014: 640–658. [DOI: 10.1007/978-3-642-55220-5_35]

[12] HÅSTAD J, IMPAGLIAZZO R, LEVIN L A. A pseudorandom generator from any one-way function[J]. SIAM Journal on Computing, 1999, 28(4): 1364–1396. [DOI: 10.1137/S0097539793244708]

[13] BOYLE E, GILBOA N, ISHAI Y. Function secret sharing: Improvements and extensions[C]. In: Proceedings of the ACM Conference on Computer and Communications Security. ACM, 2016: 1292–1303. [DOI: 10.1145/2976749.2978429]

[14] LUO J L, ZHANG L F, LIN F C, et al. Efficient threshold function secret sharing with information-theoretic security[J]. IEEE Access, 2020, 8: 6523–6532. [DOI: 10.1109/ACCESS.2019.2963677]

[15] LI W M, ZHANG L F. Towards efficient information-theoretic function secret sharing[J]. IEEE Access, 2020, 8: 28512–28523. [DOI: 10.1109/ACCESS.2020.2971722]

[16] LUO J L, LIN C L, LI C Z, et al. Threshold function secret sharing scheme based on polynomial interpolation[J]. Computer Systems and Applications, 2020, 29(5): 29–35. [DOI: 10.3969/j.issn.1003-3254.2020.05.005]
罗景龙, 林昌露, 李朝珍, 等. 基于多项式插值的门限函数秘密分享方案 [J]. 计算机系统应用, 2020, 29(5): 29–35. [DOI: 10.3969/j.issn.1003-3254.2020.05.005]
[17] YUAN D Z, HE M X, ZENG S K, et al. (t, p)-Threshold point function secret sharing scheme based on polynomial interpolation and its application[C]. In: Proceedings of 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing. ACM, 2016: 269–275. [DOI: 10.1145/2996890.3007871]
[18] BOYLE E, COUTEAU G, GILBOA N, et al. Homomorphic secret sharing: Optimizations and applications[C]. In: Proceedings of the ACM Conference on Computer and Communications Security. ACM, 2017: 2105–2122. [DOI: 10.1145/3133956.3134107]
[19] BOYLE E, KOHL L, SCHOLL P. Homomorphic secret sharing from lattices without FHE[C]. In: Advances in Cryptology—EUROCRYPT 2019, Part II. Springer Cham, 2019: 3–33. [DOI: 10.1007/978-3-030-17656-3_1]
[20] BOYLE E, GILBOA N, ISHAI Y, et al. Foundations of homomorphic secret sharing[C]. In: Proceedings of 9th Innovations in Theoretical Computer Science Conference (ITCS 2018). Cambridge, MA, USA, 2018: 1–21. [DOI: 10.4230/LIPIcs.ITCS.2018.21]
[21] GENTRY C. Fully homomorphic encryption using ideal lattices[C]. In: Proceedings of the 41th Annual ACM Symposium on Theory of Computing. ACM, 2009: 169–178. [DOI: 10.1145/1536414.1536440]
[22] PLANTARD T, SUSILO W, ZHANG Z F. Fully homomorphic encryption using hidden ideal lattice[J]. IEEE Transactions on Information Forensics and Security, 2013, 12(8): 2127–2137. [DOI: 10.1109/TIFS.2013.2287732]
[23] WANG F, YUN C, GOLDWASSER S, et al. Splinter: Practical private queries on public data[C]. In: Proceeding of the 14th USENIX Symposium Networked System Design Implement (NSDI 2017). USENIX, 2017: 299–314.
[24] BOYLE E, GILBOA N, ISHAI Y. Secure computation with preprocessing via function secret sharing[C]. In: Theory of Cryptography—TCC '19, Part I. Springer Cham, 2019: 341–371. [DOI: 10.1007/978-3-030-36030-6_14]
[25] WOODRUFF P D, YEKHANIN S. A geometric approach to information-theoretic private information retrieval[J]. SIAM Journal on Computing, 2007, 37(4): 1046–1056. [DOI: 10.1109/CCC.2005.2]
[26] BELLARE M. A note on negligible functions[J]. Journal of Cryptology, 2002, 15(4): 271–284. [DOI: 10.1007/s00145-002-0116-x]

作者信息

林昌露 (1978–), 福建大田人, 副教授. 主要研究领域为秘密分享与安全多方计算及其以相关应用.
cllin@fjnu.edu.cn

罗景龙 (1996–), 安徽亳州人. 主要研究领域为安全与人工智能.
jinglongluo1@163.com

张胜元 (1966–), 福建连城人, 教授. 主要研究领域为编码与密码.
syzhang@fjnu.edu.cn

王华雄 (1965–), 福建安溪人, 副教授 (终身教职). 主要研究领域为理论计算机科学、编码理论、密码学.
hxwang@ntu.edu.sg

附录: 实例

为辅助读者理解本文所构造的门限函数秘密分享方案, 在此给出一个具体的实例. 令 $N = 4, q = 5, m = 4, d = 2, \alpha = 2, \beta = 3$, 则有

$$E(1) = (0, 0, 1, 1), E(2) = (0, 1, 0, 1), E(3) = (1, 0, 0, 1), E(4) = (1, 0, 1, 0).$$

因为 $d=2$, 则 β 可以拆分为 $\beta=3=2\times 4 \pmod 5$. 故 $H_\beta(\alpha)=H_3(2)=(0,2,0,4)$, 则对任意的 $\alpha'\in[4]$, 存在 $m=4$ 变量的多项式

$$F_{\alpha'}(z_1,z_2,z_3,z_4)=\prod_{l:E(\alpha')[l]=1} z_l, l=1,2,3,4. \tag{5}$$

基于上述条件我们可以构造如下参与者个数为 $n=4$, 重构门限为 $r=3$, 私密门限 $t=1$, 秘密函数为 $f_{2,3}:[4]\to\mathbb{F}_5$ 的 $(1,3,4)$-FSS 方案. 其中 $\lambda_i=i, i=1,2,3,4$ 为 $\mathbb{F}_5$ 上 4 个两两不同的非零公开值.

- **Gen**$(1^\lambda, f_{2,3})\to(k_1,k_2,k_3,k_4)$.
  1) 发送者 D 随机独立地选取向量 $V^1=(2,1,3,2)\in\mathbb{F}_5^4$ 和 $2,3\in\mathbb{F}_5$.
  2) 发送者 D 生成多项式 $Q(\lambda)=H_3(2)+\lambda V^1=(0,2,0,4)+\lambda(2,1,3,2)=(2\lambda,2+\lambda,3\lambda,4+2\lambda)$, $R(\lambda)=0+2\lambda+3\lambda^2$.
  3) 发送者 D 计算 $k_i=(Q(\lambda_i),R(\lambda_i)), i=1,\cdots,n$ 如下:

$$\begin{cases} k_1=(Q(1),R(1))=((2,3,3,1),0),\\ k_2=(Q(2),R(2))=((4,4,1,3),1),\\ k_3=(Q(3),R(3))=((1,0,4,0),3),\\ k_4=(Q(4),R(4))=((3,1,2,2),1). \end{cases}$$

  4) 输出 (k_1,k_2,k_3,k_4).
- **Eval**$(i,k_i,\alpha')\to(y_i)$.
  1) 对任意的 $\alpha'=2\in[4]$, 参与者 P_i 计算 $y_i=f(\lambda_i)=F_{\alpha'}(Q_{\lambda_i})+R(\lambda_i)$, 其中 $F_{\alpha'}$ 定义见等式(5), 具体如下:

$$\begin{cases} y_1=F_{\alpha'}(Q_1)+R(1)=3\times 1+0=3,\\ y_2=F_{\alpha'}(Q_2)+R(2)=4\times 3+1=3,\\ y_3=F_{\alpha'}(Q_3)+R(3)=0\times 0+3=3,\\ y_4=F_{\alpha'}(Q_4)+R(4)=1\times 2+1=3. \end{cases}$$

  2) 输出 y_1,y_2,y_3,y_4.
- **Dec**$((\lambda_{i_1},y_{i_1}),(\lambda_{i_2},y_{i_2}),(\lambda_{i_3},y_{i_3}))\to S$.
  1) $b_{i_h}=\prod_{h'=1,h'\neq h}^3 \frac{\lambda_{i_{h'}}}{\lambda_{i_{h'}}-\lambda_{i_h}}$, 则 $b_1=3, b_2=2, b_3=1$.
  2) 输出 $S=\Sigma_{h=1}^3 b_{i_h}\cdot y_{i_h}=3\times 3+2\times 3+1\times 3=9+6+3=3=f_{2,3}(2)$.