计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(1):225−230 [doi: 10.15888/j.cnki.csa.007208]

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

基于格的可验证秘密共享方案①

彭　咏[1], 邵培南[1], 李　翔[1], 白建峰[2], 孟珂举[2]

[1](中国电子科技集团公司第三十二研究所, 上海 201808)
[2](中国科学技术大学 计算机科学与技术学院, 合肥 230026)
通讯作者: 彭　咏, E-mail: yongprof@mail.ustc.edu.cn

摘　要: 可验证秘密共享是密码学领域中的一项重要分支. 以往可验证秘密共享方案的有效性通常是基于离散对数的数学难题, 然而离散对数问题已经被证明在量子计算模型下是不安全的. 因此, 需要借助格难题去实现可以抵抗量子攻击的可验证秘密共享方案. 本文分析现有的可验证秘密共享方案, 针对现有方案计算效率低和无法抵御量子攻击的缺陷, 利用格密码学中的数学难题, 提出一种新的可验证秘密共享方案. 该方案相对于以往的可验证秘密共享方案, 具有更高的计算效率和抗量子攻击的特性.

关键词: 可验证秘密共享; 离散对数; 量子攻击; 格密码; 格难题

引用格式: 彭咏,邵培南,李翔,白建峰,孟珂举.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. http://www.c-s-a.org.cn/1003-3254/7208.html

Verifiable Secret Sharing Scheme Based on Lattice Cryptography

PENG Yong[1], SHAO Pei-Nan[1], LI Xiang[1], BAI Jian-Feng[2], MENG Ke-Ju[2]

[1](The 32nd Research Institute of China Electronics Technology Group Corporation, Shanghai 201808, China)
[2](School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China)

Abstract: Verifiable Secret Sharing (VSS) is an important cryptographic primitive in distributed computing. The most of pervious VSS almost depended on the commitments which was established under the computational assumption of discrete algorithm problem which had been proofed unsecure. So a quantum-resistant VSS scheme which can be applied in secret sharing schemes implemented by different methods is called for. In this study, we analyze the existing verifiable sharing schemes. In order to solve the flaws in the existing schemes, we propose a new scheme with the applicability to secret sharing implemented by lattice cryptography. In addition, it has higher verification efficiency compared to past schemes and resistance so far to cryptanalysis by quantum algorithms.

Key words: Verifiable Secret Sharing (VSS); discrete algorithm; quantum attack; Lattice cryptography; Lattice problem

1　概述

秘密共享最早由 Shamir[1]和 Blakley[2]与 1979 年提出. 秘密共享方案中存在一个可信的秘密持有者去分离一个秘密到多个不同的子份额. 秘密持有者需要将子份额分发给多个子份额持有者. 当秘密恢复时, 子份额持有者互相交换子份额用于恢复秘密. 为了避免子份额的持有者收到错误的子份额, 可验证秘密共享允许子份额持有者去验证自己收到的子份额. 后来的可验证秘密共享方案拓宽了原始的概念, 使得可验证体现在以下两个方面:

1) 秘密分发过程中, 子份额持有者验证从秘密持有者获得子份额的完整性和正确性.

① 基金项目: 上海市科学技术委员会建设基金 (17DZ2251400)
Foundation item: Construction Fund of Shanghai Science and Technology Commission (17DZ2251400)
收稿时间: 2019-05-21; 修改时间: 2019-06-21, 2019-06-27; 采用时间: 2019-07-01; csa 在线出版时间: 2019-12-27

2) 秘密恢复过程中, 秘密恢复者验证从其他子份额持有者那获得的子份额的正确性和完整性.

秘密共享自提出之后就得到了广泛关注, 并成为众多论文的研究热点[3−8]. 此外, 可验证秘密共享是密码学方向中的一个重要领域. 最早的方案是由文献[9]提出, 用以抵抗非法参与者欺骗攻击来提高秘密共享方案的安全性. 随后, 文献[10]提出基于文献[1]的非交互式的可验证秘密共享方案. 该方案利用离散对数的同态性去完成认证. 其安全性是基于离散对数的计算难题假设. 文献[11]总结并提出了一种公开秘密共享方案, 在其中有一种特别的属性. 任何一位参与者都允许检查自己收到子份额是不是正确的.

从方案设计角度来看, 已经有很多种秘密共享方案被提出. 大致可以分为两类.

第一类, 通过通信来完成子份额的验证. 大多数该类方案主要采用双变量多项式, 该类方案主要问题在于, 过多的通信导致验证低效. 比如, 当 n 个人参与恢复秘密时, 我们需要两两验证子份额的合法性, 总共需要进行$\frac{n(n-1)}{2}$ 轮通信. 此外, 在双变量多项式的秘密方案中, 每个子份额是一个多项式. 该类的秘密共享本身从信息率角度来看, 即秘密和子份额信息熵的比值, 是低效的. 它的信息率是该子份额多项式维度的倒数. 针对这其中的问题, 后来的研究者主要研究如何能够降低通信复杂度. 文献[12,13]已经展示了如果一个可被忽略的错误概率被允许的话, 过去的通信复杂度边界不再适用. 文献[14]在一个可忽略的错误概率被允许的情况下, 给出了确切的通信轮复杂度.

第二类, 采用数学难题来保证验证的安全性和有效性. 很多该类可验证秘密共享方案, 如著名的 Feldman[10]和 Pedersen[15]都是基于离散对数难题的. 该类的方案主要特点, 利用公开的参数信息进行验证, 可以做到非交互式的验证. 然而针对离散对数问题和大数分解难题, 文献[16]中 Shor 给出了一个高效的量子算法. 虽然 Pedersen[15]更是在 Feldman[10]的基础上, 提出了无条件安全的可验证秘密共享方案, 即安全性不依赖于数学难题. 即使离散对数能被解决, 也能保证子份额的安全性. 但一旦出现这种情况, 虽然能保证子份额的安全性, 但方案将无法保持有效性, 验证的过程可被任意伪造, 方案不再有效.

因此, 为了应对可能存在的量子计算机, 保证方案的有效性, 我们需要设计出一种可以抵抗量子攻击的新型无条件安全的可验证秘密共享方案.

本论文组织结构如下. 在第 2 节, 我们回顾一些基础的定义, 概念和定理. 在第 3 节, 提出具体的可验证秘密共享方案并描述如何进行子份额的验证. 在第 4 节, 分析方案的效率安全性, 比较其他的方案. 在结束语中做出全文的总结.

2 基础知识

2.1 秘密共享

定义 1. 访问结构

使$\{p_1,\cdots,p_n\}$代表所有参与者的集合. 一个集合$\mathcal{A}\subseteq 2^{\{p_1,\cdots,p_n\}}$是单调的如果满足$B\in\mathcal{A}$并且$B\subseteq C$, 则$C\subseteq\mathcal{A}$. 一个访问结构$\mathcal{A}\subseteq 2^{\{p_1,\cdots,p_n\}}$是集合$\{p_1,\cdots,p_n\}$的非空子集. $\mathcal{A}$中的集合为授权集而任何不在$\mathcal{A}$均为非授权集合. 则$\mathcal{A}$是该秘密共享方案的访问结构.

定义 2. 秘密共享[17]

假定 K 是秘密 s 的有限集合. 一个分发方案$\prod$和集合 K 实现访问结构$\mathcal{A}$在满足下列条件下称之为秘密共享.

正确性: 任意在$\mathcal{A}$中授权集合可以恢复秘密.

隐私性: 任意不在$\mathcal{A}$中的非授权集不能得到关于秘密的任何信息.

2.2 格

格[18]是m维欧式空间$\mathbb{Z}^m$的n个线性无关向量组$\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_n$的整系数线性组合, 即:

$$\mathbf{L}(\mathbf{B})=\left\{\sum_{i=1}^{n}x_i\mathbf{b}_i : x_i\in\mathbb{Z},i=1,\cdots,n\right\}$$

向量组$\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_n$称为格的一组基. 同一个格可以用不同的格基表示. m称为格的维数, n称为格的秩. 有了格的定义, 下面我们将简单介绍格上常见的数学难题, 如: 最短向量问题, γ-近似最短向量问题 (SVP-γ), 最短线性无关向量问题. 这些数学难题, 已被用于构造基于格的公私钥密码方案.

最短向量问题 (Shortest Vector Problem, SVP): 给定格$\mathbf{L}$, 找一个非零格向量v, 满足对任意非零向量$\mathbf{u}\in\mathbf{L}$, $\|\mathbf{v}\|\leq\|\mathbf{u}\|$.

γ-近似最短向量问题 (SVP-γ): 给定格$\mathbf{L}$, 找一个非零格向量v, 满足对任意格中的非零向量$\mathbf{u}\in\mathbf{L}$, $\|\mathbf{v}\|\leq\gamma\|\mathbf{u}\|$.

最短线性无关向量问题 (Shortest Independent Vector Problem, SIVP): 给定一个秩为n的格 $\mathbf{L}$, 找n个线性无关的格向量s_i, 满足$\lambda_i(\mathbf{L}) = \|\mathbf{s}_i\|, (i = 1, \cdots, n)$. 其中$\lambda_i(\mathbf{L})$表示格 $\mathbf{L}$ 中第 i 个逐次最小的向量.

2.3 Ajtai 单向函数[19]

选定适合的整数q, n, m满足条件$m > n\log q$, $q = poly(n)$. 令$\mathbf{A} \in \mathbb{Z}_q^{n\times m}$为$n \times m$的矩阵, 矩阵中的元素均在$\mathbb{Z}_q$上. 该矩阵包含$m$个均匀随机的向量$a_i \in \mathbb{Z}_q^n$, 记为$\mathbf{A} = [a_1|\cdots|a_m]$, 其中$\{a_1, \cdots, a_m\}$相互线性无关.

给定函数$F_{\mathbf{A}}(x) = \mathbf{A}x(\bmod q), x \in \{0,1\}^m$, 反向计算出原像 x 的概率是可忽略的, 其中, $\{0,1\}^m$表示一个m位的 0, 1 字符串.

上述单向函数的构造十分简单, 且计算十分高效, 他的安全性依赖于格难题. 根据 Ajtai 文章[19]中结论, 我们有如下引理.

引理 1. 如果格上的近似最短向量问题 (SVP) 和近似最短线性无关向量问题 (SIVP) 是多项式时间不可解的, 对于$m > n\log q, q = poly(n)$, $F_{\mathbf{A}}(x)$是单向函数.

3 方案构造

本节介绍我们提出的可验证秘密共享方案. 该方案示基于 Shamir 的 (t, n) 秘密共享, 并且具有高效和抵抗量子攻击的特性.

3.1 符号

首先, 定义F_p 作为在素数p上的数域. P_i 表示第 i 个参与者, s_i表示P_i用于恢复秘密的子份额并且$s_i \in F_p$. 我们使用$\oplus$代表异或运算. 此外, 用$\mathbf{A} \in \mathbb{Z}_q^{n\times m}$表示一个由$n$个$m$维线性无关向量组成的矩阵, 其中$n, m$和$q$满足$m > n\log q$, $q = poly(n)$ $m = \lceil \log p \rceil$. 最后, 记$F_{\mathbf{A}}(x)$ 等于$\mathbf{A}x \bmod q$, 其中$x \in \{0,1\}^m$.

3.2 可验证秘密共享方案

该方案由以下 3 个步骤组成: 初始化阶段, 子份额分发阶段和秘密恢复阶段.

初始化阶段:

秘密持有者在F_p上随机生成一个$t-1$阶的多项式$f(x)$:

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1} \bmod p$$

其中, 秘密s即为多项式的常数项. 也就是说, $s = a_0$. 此外, 秘密持有者选择整数n, m和q满足$m > n\log q$, $q = poly(n)$, $m = \lceil \log p \rceil$. 这里我们可以将F_p上的一个元素看成一个 m 比特的二进制字符串. 最后生成m个线性无关的向量$\alpha_i \in \mathbb{Z}_q^n$, 记为$\mathbf{A} := [\alpha_1|\cdots|\alpha_m]$.

分发阶段:

(1) 秘密持有者计算$s_i = f(x_i)$并且随机从$\{0,1\}^m$中选择t_i, 将(s_i, t_i)一起发送给子份额持有者P_i. 注意到如果$s_i \neq s_j$且$t_i \neq t_j$, 那么$s_i \oplus t_i$ 一定不等于$s_i \oplus t_j$.

(2) 秘密持有者公开矩阵 $\mathbf{A}$, $F_{\mathbf{A}}(s_i \oplus t_i)$ 和s_i'的值, 其中$s_i' = s_i \oplus t_i$.

(3) 子份额持有者P_i收到(s_i, t_i)后, 首先要对自己接收到的子份额进行验证:

$$F_{\mathbf{A}}(s_i \oplus t_i) = \mathbf{A}(s_i \oplus t_i) \bmod q$$

如果验证所得到的子份额是正确的, 那么继续以下的骤, 如果验证失败, 则要求秘密持有者重新发送子份额.

秘密恢复阶段:

假设有k个子份额持有者参与恢复秘密s, 其中$k \geq t$, 他们需要执行以下步骤:

(1) 子份额持有者之间互相验证对方子份额的合法性, 具体操作如下:

$$F_{\mathbf{A}}\left(\sum (s_j')\right) = \sum F_{\mathbf{A}}(s_j \oplus t_j) \bmod q, j \in [k]$$

如果验证正确, 则继续下边的步骤. 否则, 我们可以通过以下操作检查每个参与者的身份从而确定哪个是非法的参与者.

$$F_{\mathbf{A}}(s_j') = A(s_j \oplus t_j) \bmod q, j \in [k]$$

(2) 参与秘密恢复的子份额持有者互相交换信息s_i并用所得到这些子份额采用 Shamir 秘密共享的方式去恢复秘密.

$$s = \sum_{i=1}^{k} s_i \prod_{1\leq j\leq k, j\neq i} \frac{x_j}{x_j - x_i} \bmod p$$

为证明验证秘密恢复阶段步骤 (1) 的正确性, 我们给出定理 1.

定理 1. 单向函数$F_{\mathbf{A}}$具有线性同态的特性, 并且满足以下公式:

$$\sum F_{\mathbf{A}}(s_i \oplus t_i) = F_{\mathbf{A}}\left(\sum (s_i \oplus t_i)\right) \bmod q$$

证明: 假设有k 个子份额持有者组成的授权集合, 他们的子份额构成$\Gamma = \{s_1, \cdots, s_k\}$. 每个$\Gamma$ 中的s_i 均绑定一个对应的随机值t_i, 所有的s_i和t_i都是从$\{0,1\}^m$中选取的. 使用$\mathbf{A} \in \mathbb{Z}_q^{n\times m}$表示一个由$n$个$m$维线性无关向量组

成的矩阵, 也就是说$\mathbf{A} := [\alpha_1|\cdots|\alpha_m]$. 那么有:

$$\sum_{i=1}^{k} F_{\mathbf{A}}(s_i \oplus t_i) = \sum_{i=1}^{k} \mathbf{A}(s_i \oplus t_i)$$
$$= \sum_{i=1}^{k} (\alpha_1, \cdots, \alpha_m)(s_i \oplus t_i) \bmod q$$

此外, 因为$(s_i \oplus t_i)$仍然是一个 m 比特位的二进制字符串, 可以被写为$\left(\delta_{i_1}, \cdots, \delta_{i_m}\right), \delta_{i_j} \in \{0,1\}$. 因此, 上述公式等于:

$$\sum_{i=1}^{k} \left(\alpha_1 \delta_{i_1} + \cdots + \alpha_m \delta_{i_m}\right) = \sum_{i=1}^{\mathrm{k}} \sum_{j=1}^{m} \alpha_j \delta_{i_j}$$
$$= \mathbf{A} \sum_{i=1}^{k} \left(\delta_{i_1}, \cdots, \delta_{i_m}\right) \bmod q$$

因此, 函数$F_{\mathbf{A}}$有线性同态性并且该定理成立.

4 分析

在本节, 我们分析提出方案的效率以及安全性. 事实上, 我们的方案就是将 Ajtai 单向函数函数应用到 Shamir 方案中, 同时引入随机变量t_i, 使得可验证方案是无条件安全的. 即使最终格难题被破解, 也无法获得关于子份额的任何信息. 当然方案的有效性仍然依赖于格难题.

4.1 效率分析

首先, 我们需要考虑方案的信息率. 信息率是作为衡量一个秘密共享系统的重要手段, 被广泛用于衡量秘密共享方案本身的效率. 信息率σ被定义为秘密长度与最大子份额长度的比值, 也就是说:

$$\sigma = \frac{s}{\max_{i \in P}(s_i)}$$

在我们的方案中, 因为子份额不仅仅是单独的s_i, 而是一对值(s_i, t_i). 因此, 该方案的信息率为 1/2 而不是 1. 此外, 还有以下一些指标用于衡量可验证秘密共享方案的效率:

(1) 验证子份额时所要通信的轮数.

(2) 子份额持有者用于验证子份额合法性所需的通信数据量.

(3) 子份额持有者验证子份额合法性所要做出的运算量.

指标 (1) 和 (2) 用于衡量通信的效率, 也是大多数分析通信协议通信复杂度的指标. 指标 (3) 用于衡量计算的效率.

可验证秘密共享的轮数复杂度主要是在实际方案设计中需要考虑的. 通信轮数相较于通信量来言, 往往需要更多的时间. 因此, 在实际的通信协议中往往作为重要因素被考量. 我们的方案类似于方案[9,16], 是非交互式的可验证秘密共享, 在分发阶段, 并不需要在验证时额外交互信息. 在秘密恢复时, 仅仅只需要将自己的验证信息广播出去即可, 所以不会提高通信轮数, 通信的轮数复杂度可被忽略.

子份额持有者用于验证子份额合法性所需的比特数可以被分为以下两部分: 秘密持有者分发的信息和子份额持有者之间互相交互的信息. 第一部分与其它可验证秘密共享方案差别较大而后一部分和其它可秘密共享方案大致相同, 因此我们主要分析第一部分的信息量. 在我们的方案中, 秘密持有者需要公开一个矩阵$\mathbf{A} \in \mathbb{Z}_q^{n \times m}$和$F_{\mathbf{A}}(s_i \oplus t_i)$的值. 它总共包含的比特数如下:

$$mn \log q + n \log q \approx m^2 = \log^2 p$$

其中, $m = \lceil \log p \rceil$且$m > n \log q$. 也就是说, 我们的方案大约需要秘密持有者发送给子份额持有者$\log^2 p$比特信息用于完成验证.

在本文中, 计算开销是可以预估的. 为了更好的说明, 我们比较我们的方案与其它 3 篇基于 Shamir 秘密共享的可验证秘密共享方案. 假设所有的秘密和子份额的空间都是在F_p, 我们将F_p上一次乘法运算记为 1 次运算.

我们只在此比较子份额持有者用于验证其它子份额合法性所需要的计算量. 在我们的方案中, 子份额持有者仅仅需要在很小的整数中进行线性运算. 总共所需要在$\mathbb{Z}_q$中执行$n \log p$乘法运算, 其中$\log p > n \log q$. 为了方便比较计算复杂度, 我们通过除以2^n将我们的结果从$\mathbb{Z}_q$转化到$\mathbb{Z}_q$.

下面我们将从通讯量, 计算量和适用性 3 个方面, 比较本文方案和以往方案. 通讯量是秘密恢复阶段, 每个参与者需要广播多少比特的验证信息. 计算量是每个在于者在最坏情况的计算复杂度来表示. 比较结果如表 1 所示.

在表 1 中, Schoenmakers 的方案[20]取决于公钥密码, 所以无法进行评估. 此外, 我们使用“普适”去代表我们方案的适用性. 它代表我们的方案可以应用于任何的方式构造的秘密共享方案中, 例如基于拉格朗日

插值多项式, 基于中国剩余定理, 基于超平面空间, 基于线性码等密码共享方案. 显然, 我们的方案相对于其它可验证秘密共享方案具有更好的计算效率.

表 1 本方案与已有方案的性能比较

方案	通讯量	计算量	适用性
Fledman[10]	$\log p$	$t\log p\log(t-1)$	多项式
Pedersen[15]	$\log p$	$t\log p\log(t-1)$	多项式
Schoenmakers[20]	-	-	普适
Ours	$\log p$	$t\log p\log(t-1)$	普适

4.2 安全性分析

我们的方案是基于 Shamir 秘密共享, 所以任何授权集合都应该能够恢复秘密而任何的非授权集合都不应该能恢复秘密. 此外, 我们还需要考虑验证过程的安全性, 也就是说子份额持有者在验证子份额合法性时是否泄漏了秘密.

定理 2. 本文方案的验证机制, 包括分发和秘密恢复过程, 基于 Ajtai 单向函数, 满足不可区分和不可伪造特性.

证明: 在我们的方案中, $s_i\oplus t_i$ 满足均匀随机分布. 此外, Ajtai 单向函数$F_{\mathbf{A}}(s_i\oplus t_i)$是均匀随机分布. 我们不能够区分$F_{\mathbf{A}}(s_i\oplus t_i)$和$F_{\mathbf{A}}\left(s_j\oplus t_j\right)$当$i\neq j$. 所以该验证机制满足不可区分的特性.

为了证明绑定特性, 我们需要证明不存在 概率多项式时间的算法去找到两个不同的s_i. 也就是说, 不存在 概率多项式时间的算法去找到$s_i\neq s_j\in\{0,1\}^m$使得$\mathbf{A}s_i\equiv\mathbf{A}s_j(\mathrm{mod}\ q)$. 如果我们找得到, 那么存在$\mathbf{A}\left(s_i-s_j\right)\equiv 0(\mathrm{mod}\ q)$. 因为$s_i\neq s_j\in\{0,1\}^m$, 我们有$\left(s_i-s_j\right)\in\{-1,0,1\}^m$, 构成了一个针对格难题中小整数问题的一个解法, 而小整数问题被认为是一个不可解的数学难题. 因此, 本方案中验证机制满足不可伪造性.

我们已经证明了我们方案的验证机制满足不可区分和不可伪造两个特性. 不可区分特性意味着方案的验证过程不会泄露秘密的任何信息. 不可伪造特性意味着只有正确的子份额才能通过验证. 在上述证明过程中, 不可区分和不可伪造均是依赖于格难题.

定理 3. 即使 Ajtai 单项函数被破解, 验证子份额的过程也不会泄露任何秘密的信息.

证明: 根据引理 1, 我们知道 Ajtai 单项函数可以被约简为格难题中的近似最短线性无关向量问题. 至今还没有任何多项式时间的算法去解决近似最短线性无关向量问题. 假设近似最短独立向量问题和 Ajtai 单项函数都被破解, 攻击者可以从$F_{\mathbf{A}}(s_i\oplus t_i)$得到值$s_i\oplus t_i$. 因为$t_i$是在子份额空间中的随机值, 所以$s_i\oplus t_i$是随机分布在子份额空间的, 从而我们无法从$s_i\oplus t_i$得到任何秘密的信息. 这就表明了, 即使 Ajtai 单项函数被破解, 验证子份额的过程也不会泄露任何秘密的信息.

通过以上证明, 我们得到我们的方案是无条件安全的. 换言之, 格难题保证了可验证的有效性, 即使格难题被破解, 我们的方案依旧不会泄露子份额的任何信息. 即本方案的验证机制是无条件安全的.

5 结束语

我们在本文展示了基于格的可验证秘密共享方案, 能够在秘密分发和恢复过程中, 验证子份额的合法性. 同时该方案具备无条件安全的特性, 即使格难题被其他什么未知工具破解, 也能保证子份额的安全性.

本方案通过与已有方案的比较, 我们的方案具有以下特性: 更高的效率; 量子攻击抵抗性; 普适性 (可以应用于任何数学工具实现的秘密共享方案).

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 1979 International Workshop on Managing Requirements Knowledge. New York, NY, USA. 1979. 313–318.

3 李新超, 钟卫东, 刘明明, 等. 基于秘密共享的 SM4 算法 S 盒实现方案. 计算机工程, 2018, 44(11): 148–153.

4 王俞力, 杜伟章. 向量空间上无可信中心的动态多秘密共享方案. 计算机工程, 2017, 43(7): 163–169. [doi: 10.3969/j.issn.1000-3428.2017.07.027]

5 顾为玉, 苗付友, 何晓婷. 基于二元对称多项式的公平秘密共享方案. 计算机工程与应用, 2016, 52(13): 38–42, 109. [doi: 10.3778/j.issn.1002-8331.1601-0192]

6 张红军, 刘珂, 牟占生. 基于格的门限秘密共享算法. 计算机工程, 2016, 42(6): 139–143, 150. [doi: 10.3969/j.issn.1000-3428.2016.06.024]

7 梁建武, 刘晓书, 程资. 基于图态和中国剩余定理的量子秘密共享方案. 通信学报, 2018, 39(10): 72–78. [doi: 10.11959/j.issn.1000-436x.2018220]

8 彭巧, 田有亮. 基于多线性 Diffie-Hellman 问题的秘密共享方案. 电子学报, 2017, 45(1): 200–205. [doi: 10.3969/j.issn.

0372-2112.2017.01.027]

9 Chor B, Goldwasser S, Micali S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults. Proceedings of the 26th Annual Symposium on Foundations of Computer Science. Portland, OR, USA. 1985. 383–395.

10 Feldman P. A practical scheme for non-interactive verifiable secret sharing. Proceedings of the 28th Annual Symposium on Foundations of Computer Science. Los Angeles, CA, USA. 1987. 427–438.

11 Stadler M. Publicly verifiable secret sharing. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Saragossa, Spain. 1996. 190–199.

12 Fitzi M, Garay J, Gollakota S, *et al*. Round-optimal and efficient verifiable secret sharing. Proceedings of the 3rd Theory of Cryptography Conference. New York, NY, USA. 2006. 329–342.

13 Patra A, Choudhary A, Rabin T, *et al*. The round complexity of verifiable secret sharing revisited. Proceedings of the 29th Annual International Cryptology Conference. Santa Barbara, CA, USA. 2009. 487–504.

14 Kumaresan R, Patra A, Rangan C P. The round complexity of verifiable secret sharing: The statistical case. Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore. 2010. 431–447.

15 Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing. Proceedings of the Annual International Cryptology Conference. Santa Barbara, CA, USA. 1992. 129–140.

16 Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 1999, 41(2): 303–332. [doi: 10.1137/S0036144598347011]

17 Beimel A. Secret-sharing schemes: A survey. Proceedings of the 3rd International Conference on Coding and Cryptology. Qingdao, China. 2011. 11–46.

18 王小云, 刘明洁. 格密码学研究. 密码学报, 2014, 1(1): 13–27.

19 Ajtai M. Generating hard instances of lattice problems extended abstract. Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. Philadelphia, PA, USA. 1996. 99–108.

20 Schoenmakers B. A simple publicly verifiable secret sharing scheme and its application to electronic voting. Proceedings of the 19th Annual International Cryptology Conference. Santa Barbara, CA, USA. 1999. 148–164.