

基于 LWE 两方数相等的保密计算协议

解 丹, 杨 波, 邵志毅, 徐彦蛟, 杜军强

(陕西师范大学计算机科学学院, 西安 710062)

摘 要: 保密地比较两方数是否相等是安全多方计算(SMC)问题中重要的研究内容, 其在数据挖掘、在线推荐服务、在线预定服务、医药数据库等领域有着重要应用。针对半诚实模型下两方保密比较协议无法抵抗恶意攻击的问题, 提出一种恶意模型下两方数相等的保密计算协议, 采用基于格上差错学习(LWE)困难性问题的公钥加密机制和 Paillier 加密方案, 使得存在恶意攻击者的情况下能够阻止恶意攻击行为发生, 同时证明协议在恶意模型下是安全的。分析结果表明, 该协议执行完成后不会泄露通信双方的私有信息, 与半诚实模型下两方保密比较协议相比, 能有效抵抗恶意攻击者的攻击, 为 SMC 通信提供了较好的解决方案。

关键词: 安全多方计算; 两方数相等; 半诚实模型; 恶意模型; 差错学习困难性问题; Paillier 加密方案

Secure Computation Protocol Based on LWE Two-party Numbers Equality

XIE Dan, YANG Bo, SHAO Zhi-yi, XU Yan-jiao, DU Jun-qiang

(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

【Abstract】 The equation test is an important part in Security Multi-party Computation(SMC). It has important application in the fields of data mining, recommendation service, online dating service, and medical database. According to the defects existing in the protocols of comparing two data based on security under the semi-honesty model, this paper proposes a secure computation protocol for two-party numbers equality test in the malicious model. The protocol uses the public-key encryption mechanism based on lattice Learning With Error(LWE) difficult problem and Paillier encryption scheme, it can prevent malicious attacks in the case of existing malicious attacker, and at the same time proves that agreement is safe under the malicious model. Analysis results prove that the protocol after the implementation is completed, and no private information in both communication parties is revealed. Compared with the protocols of comparing two data based on security under the semi-honesty model, the proposed protocol can effectively resist the attacks from the malicious adversary and provides a good solution for the communication with high needs.

【Key words】 Security Multi-party Computation(SMC); two-party numbers equality; semi-honesty model; malicious model; Learning With Error(LWE) difficulty problem; Paillier encryption scheme

DOI: 10.3969/j.issn.1000-3428.2013.12.026

1 概述

随着互联网的迅猛发展, 越来越多的个人、公司、政府部门等通过网络进行存储并提取信息、交换信息以及协同计算等其他重要工作。然而, 这类工作在给人类带来方便的同时也蕴藏着很多安全问题, 比如 2 个互不信任的用户或者 2 个互相竞争的团队需要进行合作时, 由于担心自己的隐私或数据安全, 每个用户都希望自己提供的信息或数据在不被其他人获悉的情况下完成合作。这样一类安全问题就是安全多方计算(Security Multi-party Computation,

SMC)研究的内容。

安全多方计算是解决一组互不信任的参与方之间保护隐私的协同计算问题, SMC 要确保输入的独立性、计算的正确性, 同时不泄露各自输入值给参与计算的其他成员。SMC 起源于 1982 年提出的百万富翁问题^[1]: 即 2 个百万富翁想要在不泄露互相的财富值的情况下比较两方财富的大小。姚氏百万富翁问题以及文献[2]提出的问题等都是很多安全多方计算问题的基础, 它们的提出对于现代社会多种商业活动具有重要意义, 其在电子选举^[3]、电子投标^[4]、电子拍卖^[5]、秘密共享^[6]、门限签名^[7]等场景中有着重要的作

基金项目: 国家自然科学基金资助项目(61272436); 广东省自然科学基金资助项目(10351806001000000)

作者简介: 解 丹(1988—), 女, 硕士研究生, 主研方向: 密码学, 信息安全; 杨 波, 教授、博士生导师; 邵志毅, 讲师、博士研究生; 徐彦蛟、杜军强, 硕士研究生

收稿日期: 2012-11-02 **修回日期:** 2012-12-29 **E-mail:** xied111@163.com

用。其中, 比较 2 个数是否相等就是安全多方计算的一个重要研究问题, 也是其他很多问题, 比如求集合包含关系问题^[8]、求集合的交集问题^[9-10]等的基础。文献[11]提出基于差错学习(Learning With Error, LWE)困难性问题假设保密地比较两方数是否相等的协议, 该协议的安全性基于半诚实模型, 然而现实网络中往往存在着很多恶意攻击者, 这使得存在缺陷的半诚实模型下的两方保密比较协议不足以抵抗恶意攻击行为。基于此, 本文提出一种恶意模型下比较两方数是否相等的保密计算协议。该协议的安全性基于格上的 LWE 问题的公钥加密机制和 Paillier 加密方案, 使得存在恶意攻击者的情况下能够阻止恶意攻击行为发生, 确保通信双方的信息安全。在协议执行完成后, 不会泄漏通信双方的私有信息, 如果任一方有恶意攻击行为, 则最终输出结果不会暴露, 严格按照协议执行一方的信息安全。

2 预备知识

2.1 格定义

从几何学角度来描述, 格是 n 维空间中规则排列的离散的无限点集, 其形式化定义为:

定义 1(格) 格是由 \mathbb{R}^n 中的 k 个线性无关向量 b_1, b_2, \dots, b_k 的整数线性组合构成的集合:

$$L(b_1, b_2, \dots, b_k) = \left\{ \sum_{i=1}^k x_i b_i : x_i \in \mathbb{Z} \right\}$$

其中, k 称为格 L 的秩; n 称为 L 的维数, 且 $k \leq n$, 当 $k=n$ 时, L 称为满秩格; 向量组 b_1, b_2, \dots, b_k 称为 L 的一组基。将基作为列向量采用矩阵 $B=[b_1, b_2, \dots, b_k] \in \mathbb{R}^{n \times k}$ 来表示, 格 L 可以表示为 $L(B)=\{Bx : x \in \mathbb{Z}^k\}$ 。

一个格可以由不同的基来表示, 在解决格上相关问题时, 即使同一个算法, 如果选择不同的基作为输入, 算法实际运行的时间和结果差别也可能十分明显。所以, 有必要研究如何找到有利于解决问题的那一组基。选择这样一组基的过程就是格基归约。目前最好的格基归约算法是由文献[12]提出的 LLL(Lenstra, Lenstra and Lovasz)算法。

2.2 LWE 困难性假设与基于 LWE 问题的公钥加密体制

文献[13]将 LWE 困难性假设问题描述为: 平均情况的 $LWE_{q,x}$ 是以不可忽略的概率区分矩阵 $A_{S,x}$ 与 $\mathbb{Z}_q^n \times \mathbb{Z}_q$ 上的均匀分布。若 LWE 是困难的, 则 $A_{S,x}$ 上变量的集合是伪随机的。

定理 1 设 $\alpha \in (0,1)$, 素数 $q = q(n)$ 且 $\alpha \cdot q > 2\sqrt{n}$, 若存在一个有效的算法(包括量子算法)解决 LWE_{q,Ψ_α} , 则存在一个有效的量子算法解决最坏情况问题最短向量问题(GapSVP₁)和最短独立向量问题(SIVP), 其中, 近似因子 $\gamma(n) = \tilde{O}(n/\alpha)$ 。

文献[10]给出基于 LWE 问题公钥加密体制, 具体如下:

(1)LWEKeyGen: $A \in \mathbb{Z}_q^{n \times m}$ 为一随机矩阵, 随机均匀选取一非零向量 $s \leftarrow \mathbb{Z}_q^n$ 为私钥, 公钥为向量 $p = A^T s + x \in \mathbb{Z}_q^m$, 其中, x 的每个分量 $x_i \in \mathcal{X}(i \in [m])$ 是独立的。

(2)LWEEnc(p, b): 为加密每个比特 $b \in \{0,1\}$, 随机选取 $e \in D_{z^m, s}$, 输出向量:

$$(u, c) = (Ae, p^T e + b \lfloor q/2 \rfloor) \in \mathbb{Z}_q^{n+1}$$

(3)LWEDec(u, c): 计算 $b' = c - s^T u \in \mathbb{Z}_q$, 若 b' 与 0 的距离比与 $\lfloor q/2 \rfloor \bmod q$ 的距离近, 则输出 0, 否则输出 1。

定理 2 若 LWE_{q,Ψ_α} 是困难的, 上述加密体制在选择明文攻击下是安全的^[14]。

2.3 Paillier 加密方案及其性质

文献[15]中 Paillier 基于离散对数问题的陷门机制(该机制基于合数次剩余类, 即次数设置为一个难分解的整数 $n=pq$, 其中, p, q 为 2 个大素数)提出一种加密方案, 称为 Paillier 加密方案, 在本文中, 使用这种加密体制对通信双方的承诺进行计算, 保证了恶意模型下的安全性。

Paillier 加密方案具体如下:

设 $n=pq$, 随机选取 $g \in \mathcal{B}$, 通过 $\gcd(L(g^\lambda \bmod n^2), n) = 1$ 来验证。

公开钥: (n, g)

秘密钥: (p, q)

加密: 明文 $m < n$, 随机选取 $r < n$

$$\text{密文 } c = g^m r^n \bmod n^2$$

解密: 密文 $c < n^2$

$$\text{明文 } m = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$$

2.4 恶意参与者模型及恶意模型下的安全性定义

定义 2(恶意参与者模型) 在存在恶意参与者的模型中, 恶意参与者可能在协议初始阶段或是协议执行中途提供任意的输入, 也有可能恶意参与者得到其自己的输出后就终止协议, 这些是任何一个协议都无法避免的。

通过实际/理想模型来定义安全性。安全性通过比较攻击者在实际模型中获得的信息与其在理想模型(存在可信第三方)中获得的信息, 若是不可区分的, 则称协议是安全的。

定义 3(恶意模型下的安全性) 设 $f: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^* \times \{0,1\}^*$ 是一个函数, 其中, $f_1(x,y)(f_2(x,y))$ 表示 $f(x,y)$ 的第 1(2)个元素。 Π 是计算 f 的双方计算协议。 Π 保密地计算 f , 如果对于任意的、在实际模型中可以接受的概率多项式时间算法对 $\bar{A} = (A_1, A_2)$ 都存在一个对于理想模型可接受的概率多项式时间算法对 $\bar{B} = (B_1, B_2)$, 使得:

$$\{IDEAL_{f, \bar{B}(z)}(x, y)\}_{x,y,z} \stackrel{C}{=} \{REAL_{\Pi, \bar{A}(z)}(x, y)\}_{x,y,z}$$

其中, $x, y, z \in \{0,1\}^*, |x| = |y|, |z| = \text{poly}(|x|)$ 。

3 恶意模型下两方数相等的保密计算协议

设 Alice 和 Bob 分别有一个数 m_A 和 m_B , 他们想保密地比较 m_A 和 m_B 是否相等, $H_1(\cdot): \{0,1\}^* \rightarrow \mathbb{Z}_q^n$ 为一抗碰撞的杂凑函数, 解决方案描述如下。

协议 恶意模型下基于 LWE 的两方数相等的保密计算协议

输入 2 个数 $m_A \in \{0,1\}^*$ 、 $m_B \in \{0,1\}^*$

输出 若 $m_A=m_B$, 则 $f(m_A, m_B)=1$; 若 $m_A \neq m_B$, 则 $f(m_A, m_B)=0$

约定 协议开始执行后, 通信双方不得随意更改自己的输入值, 否则另一方可随时终止协议。

(1) Alice 和 Bob 分别计算 $s_A = H_1(m_A)$ 、 $s_B = H_1(m_B)$; Alice 根据误差分布 χ_A 选取向量 x_A , 然后生成 $p_A = A^T s_A + x_A$ 。

(2) Alice 随机选取 $r \in \{0,1\}^k$, 对其中的每个比特 $b_i \in \{0,1\}$, 选取 $e_i \in D_{z^m, r}$, 计算 $(u_i, c_i) = (Ae_i, p_A^T e_i + b_i \lfloor q/2 \rfloor)$; 然后将向量 $(u, c) = ((u_1, c_1), (u_2, c_2), \dots, (u_k, c_k))$ 发送给 Bob。

(3) Bob 收到 $(u, c) = ((u_1, c_1), (u_2, c_2), \dots, (u_k, c_k))$ 后, 用 s_B 作为私钥, 对 (u, c) 用算法 $LWE_{Dec}(u, c)$ 进行解密, 获得向量 $r' = \{b'_1, b'_2, \dots, b'_k\}$; Bob 拥有同态公钥加密系统的公钥 $g=1+n$ 、 $n=pq$ (n 为 2 个大素数的乘积) 以及私钥 λ 。Bob 调用 Paillier 加密方案, 计算向量 $C_B = \{c'_1, c'_2, \dots, c'_k\}$, 其中, $c'_i = g^{b'_i} y_i^n \bmod n^2$, $y_i \in \mathbb{Z}_q^n$, 发送 C_B 给 Alice。

注意: $C_B = \{c'_1, c'_2, \dots, c'_k\}$ 对 Alice 来说是一系列随机数, Alice 根据 $C_B = \{c'_1, c'_2, \dots, c'_k\}$ 无法推导出 r' 的任何信息 (Paillier 加密方案的安全性^[15]), 也就是说, Alice 若想获得 b'_i 的值, 相当于解决 Paillier 加密, 即解决大数分解问题, 这是困难的。而且, 对于 $c'_i = g y_i^n \bmod n^2$, 当 $b'_i=0$ 时, $c'_i = y_i^n \bmod n^2$, 当 $b'_i=1$ 时, $c'_i = g y_i^n \bmod n^2$ 。

(4) Alice 接收到 C_B 后, 对 r 的每个比特 b_i 计算:

$$C_i = \begin{cases} g^{-1} c'_i & \text{当 } b_i = 1 \text{ 时} \\ (c'_i)^k & \text{当 } b_i = 0 \text{ 时} \end{cases}$$

然后计算 $C = \prod_{i=1}^k C_i \bmod n^2$, 发送 C 给 Bob。

注意: 对于 C_i , 当 $b_i=1$ 时: 若 $b'_i=1$ (即 $b_i = b'_i$), 则 $C_i = g^{-1} \cdot g y_i^n \bmod n^2 = y_i^n \bmod n^2$; 若 $b'_i=0$ (即 $b_i \neq b'_i$), 则 $C_i = g^{-1} y_i^n \bmod n^2$; 当 $b_i=0$ 时: 若 $b'_i=0$ (即 $b_i = b'_i$), 则 $C_i = (y_i^n)^k \bmod n^2 = y_i^{nk} \bmod n^2$; 若 $b'_i=1$ (即 $b_i \neq b'_i$), 则 $C_i = (g y_i^n)^k \bmod n^2 = g^k y_i^{nk} \bmod n^2$ 。

可以看出, 若 r 与 r' 的每一位都相等, 则 $C_i = y_i^n \bmod n^2$ 或 $C_i = y_i^{nk} \bmod n^2$, 再根据 C 的计算式, 则 C 的

最终结果为关于 y_i 的表达式, 不含 g , 由此可以得出结论: 若 $r = r'$, 则 $C = g^x y^n \bmod n^2$, 解出 $x=0$ 。

(5) Bob 用私钥 λ 恢复出 $C = g^x y^n$ 中的 (x, y) , 若 $x=0$ 说明 $r = r'$, 输出 $f(m_A, m_B)=1$; 否则说明 $r \neq r'$, 输出 $f(m_A, m_B)=0$ 。同时发送 y 给 Alice。

(6) Alice 接收到 y 后, 验证 $y^n \bmod n \equiv C \bmod n$ 是否成立, 若不成立, 说明 Bob 欺骗, 终止协议; 若成立, 则验证 $y^n \bmod n^2 \equiv C \bmod n^2$ 是否成立, 若成立, 则输出 $f(m_A, m_B)=1$; 否则输出 $f(m_A, m_B)=0$ 。

注意:

$$\begin{aligned} C \bmod n &= g^x y^n \bmod n = (1+n)^x y^n \bmod n = \\ &= (1 + C_x^1 \cdot 1^{x-1} \cdot n) y^n \bmod n = \\ &= 1 \cdot y^n \bmod n = y^n \bmod n \end{aligned}$$

定理 3 协议在恶意模型下安全地比较了两方数是否相等。即对于现实协议中具有概率多项式时间计算能力的敌手 A 收买 Alice (Bob) 执行协议, 存在理想模型中的具有概率多项式时间计算能力的敌手模拟器 S 收买 Alice (Bob) 执行理想模型, 使得:

$$\{IDEAL_{f, \bar{B}(z)}(x, y)\}_{x, y, z} \stackrel{C}{=} \{REAL_{\Pi, \bar{A}(z)}(x, y)\}_{x, y, z}$$

其中, $x, y, z \in \{0,1\}^*$, $|x| = |y|$, $|z| = poly(|x|)$ 。

敌手 A 在现实协议中得到的信息与理想模型中得到的信息是计算不可区分的。

证明: 从两方面来分析该协议的安全性, 即 Alice 被敌手 A 收买和 Bob 被敌手 A 收买 2 种情形。在这 2 种情形中分别为他们构造一个模拟器 S 。

3.1 Alice 被收买的情况

A 为收买 Alice 的敌手, 构造理想模型中的 S 来模拟 A 。

(1) S 从 A 得到输入 m_A , Bob 拥有输入 m_B 。

(2) S 要求可信第三方 (Trusted Third Party, TTP) 计算 $s_A = H_1(m_A)$, 并根据误差分布 χ_A 选取向量 x_A , 然后生成向量 $p_A = A^T s_A + x_A$, 并将 s_A 和 p_A 发送给自己。Bob 也通过 TTP 计算 $s_B = H_1(m_B)$ 。

(3) S 要求 TTP 随机选取 $r \in \{0,1\}^k$, 并对每个比特 $b_i \in \{0,1\}$, 选取 $e_i \in D_{z^m, r}$, 计算 $(u_i, c_i) = (Ae_i, p_A^T e_i + b_i \lfloor q/2 \rfloor)$; 然后将 $(u, c) = ((u_1, c_1), (u_2, c_2), \dots, (u_k, c_k))$ 发送给 Bob。

(4) Bob 将 s_B 发送给 TTP, 要求 TTP 用算法 $LWE_{Dec}(u, c)$ 对 (u, c) 进行解密, 获得 $r' = \{b'_1, b'_2, \dots, b'_k\}$; 并将 r' 、公钥 $g=1+n$ 、 $n=pq$ 及私钥 λ 发送给 TTP。

(5) Bob 将公钥 $g=1+n$ 、 $n=pq$ 及私钥 λ 发送给 TTP, 并要求 TTP 计算 $C = \prod_{i=1}^k C_i \bmod n^2$ 的值, 并将 C 的值发送给 S 和 Bob。

(6) S 要求 TTP 恢复出 $C = g^x y^n$ 中 (x, y) 的值, 并将 x 值发送给 Bob, 将 y 值发送给 S 。

(7) S 要求 TTP 为其验证 $y^n \bmod n \equiv c \bmod n$ 是否成立, 若不成立, 终止协议; 若成立, S 输出 A 想要得到的输出。

由上述模拟过程可以看出, S 在理想模型中有可信第三方存在的情况下所模拟到的信息与实际观察到的信息是计算不可区分的。从协议执行过程以及约定可以看出, 若 S 在协议开始执行后更改自己的输入, 即有 2 种情况:

(1) S 计算 C 后, 发送一个随机值而非正确的 C 值给 Bob, 在这种情况下, 通过承诺及验证, Bob 通过私钥 λ 恢复出的 (x, y) 也一定是错误的, 这样 Bob 没有得到正确的结果, 而 S 也无法通过其他信息获得正确的比较结果。

(2) S 计算出 $(\mathbf{u}, \mathbf{c}) = ((u_1, c_1), (u_2, c_2), \dots, (u_k, c_k))$ 后, 使用一个随机向量代替 (\mathbf{u}, \mathbf{c}) , 发送给 Bob。在这种情况下, $(\mathbf{u}, \mathbf{c}) = ((u_1, c_1), (u_2, c_2), \dots, (u_k, c_k))$ 值不正确, 而 S 仍然能够得到正确的比较结果的概率最大为 $\frac{1}{2^k}$ 。

这是因为:

(1) 若 $r \neq r'$, 而 S 发送给 Bob 的 (\mathbf{u}, \mathbf{c}) 值使得 Bob 验证的结果是 $r = r'$, 这种情况发生的概率最大为 $\frac{1}{2^k}$, 因为 r 是 k 位的随机数, 2 个随机数的一位对应相等的概率为 $1/2$, 那么 k 位都对应相等的概率为 $\frac{1}{2^k}$ 。

(2) 若 $r = r'$, 而 S 发送给 Bob 的 (\mathbf{u}, \mathbf{c}) 值使得 $r \neq r'$ 。这种情况下 S 还能够得出 $r = r'$ 的结果是不可能的。根据 $C = g^x y^n$ 的值进行分析。

假设 r 中对应位为 1 而 r' 中对应位为 0 的位数为 α , r 中对应位 0 而 r' 中对应位为 1 的位数为 β 。那么根据 $C = \prod_{i=1}^k C_i \bmod n^2$ 的计算公式, 忽略 y_i 项, g 的指数为 $\beta k - \alpha$, 若要使得 $r = r'$, 则要有 $C = g^x y^n$ 中 $x=0$, 即 $\beta k - \alpha = 0$, 而 $\beta \leq k$, $\alpha \leq k$, 所以, $\beta k - \alpha = 0$ 是不可能的。这种情况下 S 和 Bob 都得不到正确的比较结果。

综上所述, S 发送错误的 (\mathbf{u}, \mathbf{c}) 后, S 已知正确结果而 Bob 得到错误结果的概率最大为 $\frac{1}{2^k}$, 并且 S 不会得到任何与 Bob 输入有关的信息。

3.2 Bob 被收买的情况

构造理想模型中的 S 来模拟 A 所得到的信息。

这一模拟过程与 Alice 的模拟过程类似, 在此不做赘述。同样地, S 在这一过程中不会得到任何与 Alice 输入有关的任何信息。因此, 协议满足安全性。

4 结束语

如何设计高效、安全、保密地比较双方或多方数值大小(或相等)的协议是一个极具挑战的问题, 也是密码学中的一项重要研究任务。目前大多数安全多方计算协议都是基于半诚实模型下的安全性, 考虑现实网络中的恶意攻击行

为无法避免, 本文提出一种在恶意模型下可有效抵抗恶意攻击者的安全协议。该协议的设计思路是基于格上 LWE 困难性假设问题和 Paillier 加密方案, 分析结果表明, 该协议可在恶意模型下公平安全高效地进行两方数是否相等的保密计算协议, 解决了在半诚实模型下无法抵抗恶意攻击者的恶意行为的缺陷, 并证明其在恶意模型下的安全性。今后将针对格上的困难性问题设计恶意模型下的解决方案, 为云计算上的应用设计更加安全高效的多方安全计算协议。

参考文献

- [1] Yao A. Protocols for Secure Computation[C]//Proc. of the 23rd IEEE Symposium on Foundations of Computer Science. Chicago, USA: IEEE Computer Society, 1982.
- [2] Goldreich O, Micali S, Wigderson A. How to Play Any Mental Game[C]//Proc. of the 19th Annual ACM Conference on Theory of Computing. New York, USA: ACM Press, 1987.
- [3] Selker T, Goler J. The SAVE System-secure Architecture for Voting Electronically[J]. BT Technology Journal, 2004, 22(4): 89-95.
- [4] Burtch K O. Linux Shell Scripting with Bash[M]. [S. l.]: Sams Publishing, 2004.
- [5] Stevens R, Rago S. Advanced Programming in the UNIX Environment[M]. [S. l.]: Addison-Wesley, 2005.
- [6] Shamir A. How to Share a Secret[J]. Communications of the ACM, 1979, 22(11): 612-613.
- [7] Han Y, Okamoto T, Qing S. Proxy Signatures, Revisited[M]. Berlin, Germany: Springer-Verlag, 1997: 223-232.
- [8] 李顺东, 司天歌, 戴一奇. 集合包含与几何包含的多方保密计算[J]. 计算机研究与发展, 2005, 42(10): 1647-1653.
- [9] Kissner L, Song D. Privacy-preserving Set Operations[C]//Proc. of the 25th Annual International Cryptology Conference. Santa Barbara, USA: [s. n.], 2005.
- [10] Freedman M J, Nissim K, Pinkas B. Efficient Private Matching and Set Intersection[C]//Proc. of International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken, Switzerland: [s. n.], 2004.
- [11] 夏峰, 杨波, 张明武, 等. 基于 LWE 的集合相交和相等的两方保密计算[J]. 电子与信息学报, 2012, 34(2): 462-467.
- [12] Lenstra A K, Lenstra H W, Lovasz L. Factoring Polynomials with Rational Coefficients[J]. Annals of Mathematics, 1982, 261(4): 515-534.
- [13] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[J]. Journal of the ACM, 2009, 56(6): 1-40.
- [14] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for Hard Lattices and New Cryptographic Constructions[C]//Proc. of the 40th Annual ACM Symposium on Theory of Computing. New York, USA: ACM Press, 2008.
- [15] Paillier P. Public-key Cryptosystems Based on Composite-degree Residuosity Classes[C]//Proc. of International Conference on the Theory and Application of Cryptographic Techniques. New York, USA: ACM Press, 1999.