基于理想格的高效模糊身份加密方案

吴立强[1)] 杨晓元[1),2)] 韩益亮[1)]

[1)](武警工程大学电子技术系武警部队密码与信息安全保密重点实验室 西安 710086)

[2)](西安电子科技大学网络信息安全教育部重点实验室 西安 710071)

摘 要 模糊身份加密方案(FIBE)是将用户的身份信息通过一个属性集合来表示,加密公钥则使用另一个属性集合表示,当且仅当这两个集合足够"相近"时,解密才能正常执行.这类密码体制能够容忍部分错误公钥信息,特别适用于某些用户身份信息不能被完全正确提取的场合.文中基于理想格上的困难问题,在标准模型下,提出了一种 IND-sID-CPA 安全的多比特 FIBE 方案,并将其安全性紧致地归约为判定性 R-LWE 困难假设,相比以前基于标准格上的 FIBE 方案,新方案具有公钥长度短、密文扩展率低的优势.

关键词 模糊身份加密;理想格;可证明安全;密码学

中图法分类号 TP309 **DOI 号** 10.3724/SP.J.1016.2015.00775

An Efficient FIBE Scheme Based on Ideal Lattices

WU Li-Qiang[1)] YANG Xiao-Yuan[1),2)] HAN Yi-Liang[1)]

[1)](*Key Laboratory of Cryptography & Information Security under the Chinese Armed Police Force, Department of Electronic Technology, Engineering University of the Armed Police Force, Xi'an* 710086)

[2)](*Key Laboratory of Network & Information Security, Ministry of Education, Xidian University, Xi'an* 710071)

Abstract A fuzzy identity-based encryption scheme, in which user identities are viewed as a set of descriptive attributes and public keys for encryption are viewed as another attributes set, can be decrypted correctly if and only if those two sets are close enough, so this system allows for a certain amount of error-tolerance in the identities, especially in the scene where some user identity information can't be derived properly. In this paper, an IND-sID-CPA secure multi-bit FIBE scheme was proposed based on hard problems from ideal lattices under the standard model, and its security was reduced to decisional R-LWE assumption tightly. Compared with prior FIBE schemes from standard lattices, the new construction has a shorter public key and a lower encryption blowup factor.

Keywords fuzzy identity-based encryption; ideal lattice; provably security; cryptography

1 引 言

在 2005 年欧密会上,Sahai 和 Waters[1] 首次提出了模糊身份加密(Fuzzy Identity-Based Encryption,FIBE)的概念.在 FIBE 系统中,用户的身份信息通过一个属性集合来表示,加密公钥也为一个属性集合,当且仅当这两个集合足够"相近"时,解密才能正常执行.这类密码体制能够容忍部分错误公钥信息,其容忍程度由衡量集合近似度的方法决定,特

收稿日期:2013-06-10;最终修改稿收到日期:2014-10-28.本课题得到国家自然科学基金(61272492,61103231,61103230)、陕西省自然科学基础研究计划项目(2011JM8012)资助.**吴立强**,男,1986 年生,硕士,讲师,主要研究方向为格密码、可证明安全理论.E-mail:latticewj@163.com.**杨晓元**,男,1959 年生,硕士,教授,主要研究领域为信息安全与密码学.**韩益亮**,男,1977 年生,博士,副教授,中国计算机学会(CCF)高级会员,主要研究方向为密码学、网络安全.

别适用于某些用户的身份信息不能被完全正确提取的场合,如生物特征的识别等.由于该文献首次将属性的概念应用到公钥密码中,因此也将 FIBE 称为属性基加密(Attribute-Based Encryption,ABE).FIBE 的提出是公钥密码学的一个重要革新,因为公钥不再局限于传统的单一实体描述,而是以实体属性的细粒度进行描述的,即公钥是一类细化的结构.解密条件也不仅仅是判定加密公钥与解密者的公钥是否相等,也可能是门限、访问树或者内积等函数的值.正是受到 FIBE 思想的启发,断言加密和函数加密等[2-3]构造灵活且实用的密码方案相继被提出.

目前,基于双线性对和标准格这两种数学工具分别实现了两个 FIBE 方案.文献[1]基于 DBDH(Decisional Bilinear Diffie-Hellman Assumption)假设,采用 Shamir 门限秘密共享的方法,构造了一种标准模型下选择身份安全(Selective-ID security)的 FIBE 方案,即当用户公钥属性集与加密公钥属性集的交集等于或大于规定数量的属性时,可正常解密.文献[4]在标准模型下,基于 LWE(Learning with Errors)困难问题[4],构造了一种选择身份 IND-CPA(Indistinguishability under Chosen Plaintext Attacks)安全的单比特 FIBE 方案,同时给出了将方案扩展到 IND-CCA(Indistinguishability under Chosen Ciphertext Attacks)安全的方法.LWE 的复杂性可以归约到格上的 gap-SVP(gap Shortest Vector Problem)和 SIVP(Shortest Independent Vectors Problem),因此该方案不仅具有线性的运算结构,还具有抵抗量子攻击和亚指数攻击的能力.但在效率方面,却存在密文扩展率高和公钥长度大的缺陷,严重影响了方案的实用性.

理想格的格基具有循环特点,即用一个主理想基可表达整个格,而传统的格需要若干个基才能表达,因此利用基于多项式商环的理想格构造出的公钥密码体制具有更紧致的密文和更短的密钥长度.2010 年 Lyubashevsky 等人[5]提出了 LWE 问题在环(Ring)上的变体——R-LWE,并将其复杂性归约到理想格上的经典困难问题;最近,Lyubashevsky 等人[6]进一步扩展了文献[5]中成果,给出了更为紧致和简洁的归约过程,并且设计了一些丰富的理想格上密码学工具.本文正是利用这些工具,设计了一些可满足身份型加密体制的核心算法和函数,从而在标准模型下构造了一种 IND-sID-CPA 安全的多比特 FIBE 方案,相比以前基于标准格上 LWE 的方案,新方案具有公钥长度短、密文扩展率低的优势.

本文第 2 节给出 FIBE 方案的概念、安全模型和判定性 R-LWE 困难假设;第 3 节介绍构造新方案的一些必备算法和函数;第 4 节描述新的 IND-sID-CPA 安全 FIBE 方案;第 5 节分析方案的正确性和效率,并给出严格的安全性证明;第 6 节对文章进行总结.

2 安全模型

2.1 标 记

符号 $i\subset[l]$ 表示分别取整数 $i=1,2,\cdots,l$.向量用黑体小写字母 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\cdots$ 表示,一般指列向量;矩阵用黑体大写字母 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\cdots$ 表示.设 $\mathbb{Z}[x]$ 和 $\mathbb{R}[x]$ 分别为系数为整数和实数的多项式集合.$R=\mathbb{Z}[x]/\langle \boldsymbol{f}(x)\rangle$ 是模 $\boldsymbol{f}(x)$ 的多项式环,$R_q=\mathbb{Z}_q[x]/\langle \boldsymbol{f}(x)\rangle$ 是模 $\boldsymbol{f}(x)$ 和系数在 $\mathbb{Z}_q$ 上的多项式环.长度为 m 的环多项式向量记作 $\hat{\boldsymbol{x}}=(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_m)\in R^m$,定义 $\hat{\boldsymbol{x}}$ 的两种乘法运算:

(1) $\hat{\boldsymbol{x}}\boldsymbol{y}=(\boldsymbol{x}_1\boldsymbol{y},\boldsymbol{x}_2\boldsymbol{y},\cdots,\boldsymbol{x}_m\boldsymbol{y})\in R^m,\hat{\boldsymbol{x}}\in R^m,\boldsymbol{y}\in R.$

(2) $\hat{\boldsymbol{x}}\otimes\hat{\boldsymbol{y}}=\sum_{i=1}^{m}(\boldsymbol{x}_i\boldsymbol{y}_i)\in R,\hat{\boldsymbol{x}}\in R^m,\hat{\boldsymbol{y}}\in R^m.$

设 $\boldsymbol{a}=a_0+a_1x+\cdots+a_{n-2}x^{n-2}+a_{n-1}x^{n-1}\in\mathbb{Z}_q[x]/\langle \boldsymbol{f}(x)\rangle,\hat{\boldsymbol{a}}\in R^m$,记

$$rot_{f,m}(\boldsymbol{a})=\begin{pmatrix}\boldsymbol{a}\\ \boldsymbol{a}x \bmod \boldsymbol{f}\\ \vdots\\ \boldsymbol{a}x^{m-1} \bmod \boldsymbol{f}\end{pmatrix},$$

$$Rot_{f,m}(\hat{\boldsymbol{x}})=\begin{pmatrix}rot_{f,m}(\boldsymbol{x}_1)\\ rot_{f,m}(\boldsymbol{x}_2)\\ \vdots\\ rot_{f,m}(\boldsymbol{x}_n)\end{pmatrix}\in R^{mn}.$$

若 m 不需要明确指出,可简记为 $rot_f(\boldsymbol{a})$ 和 $Rot_f(\hat{\boldsymbol{x}})$.

记向量 $\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})$ 的 Euclidean 范数为 $\|\boldsymbol{a}\|=\sqrt{a_{n-1}^2+a_{n-2}^2+\cdots+a_1^2+a_0^2}$.矩阵 $\boldsymbol{M}\in\mathbb{R}^{m\times n}$ 的 Euclidean 范数为 $\|\boldsymbol{M}\|=\max(\boldsymbol{m}_i)(1\leq i\leq m)$.$\boldsymbol{e}=Map_{M-v}(\hat{\boldsymbol{a}})$ 表示依次连接 $\boldsymbol{a}_i(i=1,\cdots,m)$ 的系数组成的一维列向量 $\boldsymbol{e}\in\mathbb{Z}^{mn}$,$\hat{\boldsymbol{a}}=Map_{v-M}(\boldsymbol{e})\in R^m$ 表示将 $\boldsymbol{e}\in\mathbb{Z}^{mn}$ 中各个分量依次作为环多项式向量 $\hat{\boldsymbol{a}}\in R^m$ 的系数.

对于一个素数 q,整数 m,n,矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,$m$ 维 q-ary 格定义为

$$\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m \text{ s.t. } \boldsymbol{Ae}=\boldsymbol{0}(\bmod q)\},$$

$$\Lambda_q^{u}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m \text{ s.t. } \boldsymbol{Ae}=\boldsymbol{u}(\bmod q)\}.$$

设 $\boldsymbol{x}$ 为 n 维向量，$\rho_s(\boldsymbol{x})$ 为中心为 0，标准差为 s 的 n 维高斯分布，即 $\rho_s(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}\|^2/s^2)$，那么对于格 L，记 $\rho_s(L)=\sum_{\boldsymbol{x}\in L}\rho_s(\boldsymbol{x})$，当 $\rho_s(L)$ 有界时，格 L 上的离散高斯分布[4]定义为

$$\exists \boldsymbol{y}\in L,\ \mathcal{D}_{L,s}(\boldsymbol{y})=\frac{\rho_s(\boldsymbol{y})}{\rho_s(L)}.$$

2.2　R-LWE 困难假设

假设 $\boldsymbol{f}(x)=x^n+1\in\mathbb{Z}[x]$，安全参数为 $n=2^p$ ($p\in\mathbb{Z}$)(保证 $\boldsymbol{f}(x)$ 不可逆)，$q\geq 2$，定义在 $\mathbb{Z}$ 上的离散噪声分布为 $\chi=\mathcal{D}_{\mathbb{Z},\delta}$，存在一个攻击者 $\mathcal{A}$ 和 R-LWE 随机预言机 $\mathcal{O}$，$\mathcal{O}$ 包含两个采样算法 $\mathcal{O}_\$$(随机均匀选取$(\boldsymbol{a},\boldsymbol{b})\in R_q\times R_q$)和 $\mathcal{O}_s$(设定秘密 $\boldsymbol{s}\in R_q$，选择均匀分布的环多项式 $\boldsymbol{a}$ 和系数取自 χ 的噪声 $\boldsymbol{e}$，计算$(\boldsymbol{a},\boldsymbol{b}=\boldsymbol{as}+\boldsymbol{e})\in R_q\times R_q$)，攻击者 $\mathcal{A}$ 向预言机 $\mathcal{O}$ 询问，$\mathcal{O}$ 随机利用 $\mathcal{O}_\$$ 或者 $\mathcal{O}_s$ 产生若干个实例$(\boldsymbol{a},\boldsymbol{b})$返回给攻击者 $\mathcal{A}$，如果 $\mathcal{A}$ 能够准确分辨出该实例来自 $\mathcal{O}_\$$ 或 $\mathcal{O}_s$ 的优势

$$Adv(A)=|Pr[A^{O_s}=1]-Pr[A^{O_\$}=1]|$$

是不可忽略的，那么就说 $\mathcal{A}$ 能够解决判定性 R-LWE 问题.

2.3　FIBE 的定义

一个基于身份的模糊加密方案(FIBE)包括以下 4 个算法：

FIBE.Setup$(\lambda,l)\rightarrow(PP,MSK)$：输入安全参数 λ 和最大身份长度 l，输出公共参数 PP 和主密钥 MSK.

FIBE.Extract$(PP,MSK,ID,k)\rightarrow SK_{ID}$：输入主密钥 MSK，公共参数 PP、用户身份 ID 和门限值 k，输出 ID 对应的解密密钥 SK_{ID}.

FIBE.Enc$(PP,M,ID')\rightarrow CT$：输入明文消息 M，加密公钥 ID' 和公共参数 PP，输出密文 $CT_{ID'}$.

FIBE.Dec$(PP,CT_{ID'},SK_{ID})\rightarrow M$：输入密文 $CT_{ID'}$，解密密钥 SK_{ID} 和公共参数 PP，如果 $|ID'\cap ID|\geq k$ 则输出消息 M，否则输出 $\perp$.

一个 FIBE 方案是正确的，对于 Setup 生成的所有(PP,MSK)，Extract 生成的所有用户私钥 SK_{ID}，明文空间内所有的消息 M，使用 Enc(M,ID')生成的所有密文 $CT_{ID'}$，如果 $|ID'\cap ID|\geq k$，那么

$$\mathrm{Dec}(PP,CT_{ID'},SK_{ID})=M.$$

2.4　IND-sID-CPA 安全模型

在 FIBE 方案中，非适应性选择挑战 ID 和选择明文攻击下的语义不可区分性(IND-sID-CPA)可以通过攻击者 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 之间的游戏来定义.

目标：攻击者 $\mathcal{A}$ 公布要攻击的 ID^*.

设置：挑战者 $\mathcal{C}$ 运行 FIBE.Setup 算法，公布 PP，保留主密钥 MSK.

询问阶段 I：攻击者 $\mathcal{A}$ 选择一系列 ID_j($|ID^*\cap ID_j|<k$)交给挑战者 $\mathcal{C}$ 进行私钥查询，挑战者 $\mathcal{C}$ 返回 ID_j 所对应的私钥 SK_{ID_j}.

挑战：攻击者 $\mathcal{A}$ 选择两个等长的明文 M_0 和 M_1，告知挑战者 $\mathcal{C}$，挑战者 $\mathcal{C}$ 随机选择 $b\in\{0,1\}$，使用 ID^* 加密 M_b，将密文给攻击者.

询问阶段 II：攻击者 $\mathcal{A}$ 再选择一系列的 ID_j($|ID^*\cap ID_j|<k$)进行私钥查询.

猜测：攻击者 $\mathcal{A}$ 输出 $M_{b'}$，如果 $b'=b$，则攻击者 $\mathcal{A}$ 获胜.

如果任何一个多项式时间的算法 $\mathcal{A}$ 在游戏中作为攻击者的优势 $Adv_A^{\text{IND-sID-CAP}}=|Pr[b=b']-1/2|$ 是可忽略的，则称该 FIBE 方案满足 IND-sID-CPA 安全.

3　重要算法和函数

3.1　陷门产生算法和原像抽样函数

定理 1[7].　存在理想格上陷门产生算法 IdealTrapGen，输入 $n,\sigma,r>0$，素数 $q,m\in\mathbb{Z}$ 和次数为 n 的多项式 $\boldsymbol{f}$，该算法能够在多项式时间内同时得到一个统计上接近均匀分布的多项式向量 $\hat{\boldsymbol{g}}=(\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_m)\in R_q^m$ 和陷门 $\boldsymbol{T}_{\hat{\boldsymbol{g}}}\in\mathbb{Z}_q^{mn\times mn}$，满足 $Rot(\hat{\boldsymbol{g}})^{\mathrm{T}}\cdot\boldsymbol{T}_{\hat{\boldsymbol{g}}}=\boldsymbol{0}$ 且 $\|\boldsymbol{T}_{\hat{\boldsymbol{g}}}\|\leq\widetilde{O}(\sqrt{n})$.

定理 2[8].　假设 $q\geq 2$，使用理想格上的陷门产生算法生成矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}(m>n)$ 和陷门 $\boldsymbol{T}_{\boldsymbol{A}}$，设 $\sigma\geq\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\omega(\sqrt{\log m})$，对于任意 $\boldsymbol{u}\in\mathbb{Z}_q^n$，存在一个多项式时间内算法 SamplePre$(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},\sigma)$，返回一个分布接近于 $\mathcal{D}_{\Lambda_q^u(\boldsymbol{A}),\sigma}$ 的 $\boldsymbol{x}\in\Lambda_q^u(\boldsymbol{A})$.

到目前为止，还不存在理想格上原像抽样函数，定理 2 中抽样函数是建立在标准格上的，对于环多项式向量的运算并不成立.但是可以证明，环运算和矩阵运算之间存在定理 3 中的关系.

定理 3.　设 $\hat{\boldsymbol{g}}=(\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_m)$ 是一个长度为 m 的环多项式向量，定义 $\boldsymbol{G}=Rot_f(\hat{\boldsymbol{g}})\in\mathbb{Z}^{mn\times n}$，那么

对任意一个环多项式 $\hat{\boldsymbol{c}}\in R^m$，$\hat{\boldsymbol{g}}\otimes\hat{\boldsymbol{c}}=\boldsymbol{C}^{\mathrm{T}}\cdot\boldsymbol{G}$ 成立，其中 $\boldsymbol{C}=Map_{M-v}(\hat{\boldsymbol{c}})\in\mathbb{Z}^{mn}$，$\boldsymbol{C}^{\mathrm{T}}\cdot\boldsymbol{G}$ 为矩阵乘法运算.

证明.

$$\begin{aligned}\hat{\boldsymbol{g}}\otimes\hat{\boldsymbol{c}}&=\sum_{i=1}^{m}\boldsymbol{g}_i\boldsymbol{c}_i=\sum_{i=1}^{m}[\boldsymbol{g}_i\boldsymbol{c}_{i,0}+(\boldsymbol{g}_i x \bmod \boldsymbol{f})\boldsymbol{c}_{i,1}+\cdots+\\&\qquad(\boldsymbol{g}_i x^{n-1}\bmod \boldsymbol{f})\boldsymbol{c}_{i,n-1}]\\&=\sum_{i=1}^{m}\begin{pmatrix}\boldsymbol{c}_{i,0}\\\boldsymbol{c}_{i,1}\\\vdots\\\boldsymbol{c}_{i,n-1}\end{pmatrix}^{\mathrm{T}}\begin{pmatrix}\boldsymbol{g}_i\\\boldsymbol{g}_i x \bmod \boldsymbol{f}\\\vdots\\\boldsymbol{g}_i x^{n-1}\bmod \boldsymbol{f}\end{pmatrix}\\&=\boldsymbol{C}^{\mathrm{T}}\cdot\boldsymbol{G},\end{aligned}$$

其中，$\boldsymbol{c}_{i,j}$ 表示多项式 $\boldsymbol{c}_i$ 的 j 个分量. 证毕

利用定理 3，我们可以构造出理想格上原像采样函数.

算法 1. Ideal-SamplePre($\hat{\boldsymbol{g}},\boldsymbol{T}_{\hat{\boldsymbol{g}}},\sigma,\boldsymbol{v}$).

输入：环多项式向量 $\hat{\boldsymbol{g}}\in R^m$，对应陷门 $\boldsymbol{T}_{\boldsymbol{g}}$，噪声控制参数 σ 和向量 $\boldsymbol{v}$

输出：多项式向量 $\hat{\boldsymbol{e}}\sim\mathcal{D}_{\mathbb{Z}^{m\times n},\sigma}$，满足 $\hat{\boldsymbol{g}}\otimes\hat{\boldsymbol{e}}=\boldsymbol{v}$

1. $\boldsymbol{G}=Rot_f(\hat{\boldsymbol{g}})\in\mathbb{Z}^{mn\times n}$；

2. $\boldsymbol{t}=\mathrm{SamplePre}(\boldsymbol{G},\boldsymbol{T}_{\hat{\boldsymbol{g}}},\boldsymbol{v},\sigma)\in\mathbb{Z}^{mn}$；

3. $\hat{\boldsymbol{e}}=Map_{v-M}(\boldsymbol{t})\in R^m$.

3.2 理想格中私钥提取算法

算法 2. Ideal-SampleLeft($\hat{\boldsymbol{g}},\boldsymbol{T}_{\hat{\boldsymbol{g}}},\boldsymbol{v},\sigma,id,\hat{\boldsymbol{a}},\hat{\boldsymbol{b}}$).

输入：用户 $id\in\{0,1\}^n$，$\hat{\boldsymbol{g}},\hat{\boldsymbol{a}},\hat{\boldsymbol{b}}\in R_q^m$ 和陷门 $\boldsymbol{T}_{\hat{\boldsymbol{g}}}\in\mathbb{Z}^{mn\times mn}$，$\sigma\geq\|\boldsymbol{T}_{\hat{\boldsymbol{g}}}\|\omega(\sqrt{\log m})$

输出：私钥 $\hat{\boldsymbol{e}}_{id}\sim\mathcal{D}_{\mathbb{Z}^{2m\times n},\sigma}$，满足 $\hat{\boldsymbol{e}}_{id}\otimes\hat{\boldsymbol{f}}_{id}=\boldsymbol{v}$

1. 将 id 编码为环多项式 $u(id)\in R_q$；

2. 随机选取统计分布服从 $\mathcal{D}_{\mathbb{Z}^{m\times n},\sigma}$ 的 $\hat{\boldsymbol{e}}_1\in R^m$；

3. 计算 $\boldsymbol{v}_1=(\hat{\boldsymbol{a}}+u(id)\hat{\boldsymbol{b}})\otimes\hat{\boldsymbol{e}}_1$；

4. $\hat{\boldsymbol{e}}_2=\text{Ideal-SamplePre}(\hat{\boldsymbol{g}},\boldsymbol{T}_{\hat{\boldsymbol{g}}},\boldsymbol{v}-\boldsymbol{v}_1,\sigma)\in R^m$，显然有 $\hat{\boldsymbol{e}}_2\sim\mathcal{D}_{\mathbb{Z}^{m\times n},\sigma}$；

5. 用户私钥为 $\hat{\boldsymbol{e}}_{id}=\begin{pmatrix}\hat{\boldsymbol{e}}_1\\\hat{\boldsymbol{e}}_2\end{pmatrix}\in R^{2m}$.

4 方案描述

假设用户身份属性向量 $\boldsymbol{ID}$ 由 l 个长度为 n 的比特串构造，即 $\boldsymbol{ID}=(id_1,id_2,\cdots,id_l)$，其中 $id_i\in\{0,1\}^n$，安全参数 $n=2^p$，$p\in\mathbb{Z}$，$\boldsymbol{f}(x)=x^n+1$，$q\geq n^3$ 是素数满足 $q\equiv 3 \bmod 8$，$\sigma=m\cdot\omega(\log n)$，$r=1+\log_3 q$，$m=(\lceil\log q\rceil+1)\sigma+r=\widetilde{O}(1)$，$R_q=\mathbb{Z}_q[x]/\boldsymbol{f}(x)$. 门限值 k 表示当用户身份向量和加密公钥向量中至少需要 k 个属性值相同时，才能成功解密.

4.1 FIBE.Setup(n)

(1) 随机选择均匀分布的 $\boldsymbol{u}\in R_q$；

(2) 对于 $i=[l]$，

① 使用 ideal-TrapGen(n) 产生 $\hat{\boldsymbol{g}}_i\in R_q^m$ 和陷门 $\boldsymbol{T}_{\hat{\boldsymbol{g}}_i}\in\mathbb{Z}_q^{mn\times mn}$，$\|\boldsymbol{T}_{\hat{\boldsymbol{g}}_i}\|\leq\widetilde{O}(\sqrt{n})$；

② 随机选取系数均匀分布的环多项式向量 $\hat{\boldsymbol{a}}_i\in R_q^m$、$\hat{\boldsymbol{b}}_i\in R_q^m$.

(3) 系统参数和主密钥分别为

$PP=(\{\hat{\boldsymbol{a}}_i,\hat{\boldsymbol{b}}_i,\hat{\boldsymbol{g}}_i\}_{i\in[l]},\boldsymbol{u},q,\boldsymbol{f})$，$MSK=(\{\boldsymbol{T}_{\hat{\boldsymbol{g}}_i}\}_{i\in[l]})$.

4.2 FIBE.Extract(PP,MSK,ID,k)

输入公共参数 PP，主密钥 MSK 和用户属性向量 $\boldsymbol{ID}=(id_1,id_2,\cdots,id_l)$，门限值 $k<l$.

(1) 分别对 $\boldsymbol{u}=(u_1,u_2,\cdots,u_n)\in R_q$ 的每个分量使用 Shamir 秘密共享方案，生成 l 个份额. 即对于 $i\in[l]$，选择一个系数均匀分布的 $k-1$ 次多项式 $\boldsymbol{p}_i\in\mathbb{Z}_q[x]$ 满足 $\boldsymbol{p}_i(0)=\boldsymbol{u}_i$.

(2) 对于 $j\in[l]$，构造第 j 个份额向量 $\boldsymbol{v}_j=(v_{j,1},v_{j,2},\cdots,v_{j,n})=(\boldsymbol{p}_1(j),\boldsymbol{p}_2(j),\cdots,\boldsymbol{p}_n(j))\in R_q$，根据 Shamir 秘密共享方案中系数的相关性，存在系数 L_j 使得

$$\boldsymbol{u}=\sum_{j=1}^{l}L_j\boldsymbol{v}_j.$$

(3) 对于 $i\in[l]$，取身份 id_i，构造

$$\hat{\boldsymbol{f}}_{id_i}=\begin{pmatrix}\hat{\boldsymbol{g}}_i\\\hat{\boldsymbol{a}}_i+\boldsymbol{u}(id_i)\hat{\boldsymbol{b}}_i\end{pmatrix}.$$

通过 ideal-SampleLeft($\hat{\boldsymbol{g}}_i,\boldsymbol{T}_{\hat{\boldsymbol{g}}_i},\boldsymbol{v}_i,\sigma,id_i,\hat{\boldsymbol{a}}_i,\hat{\boldsymbol{b}}_i$) 计算私钥 $\hat{\boldsymbol{e}}_{id_i}\in R^{2m}$，满足 $\hat{\boldsymbol{f}}_{id_i}\otimes\hat{\boldsymbol{e}}_{id_i}=\boldsymbol{v}_i$.

(4) 输出私钥 $SK_{ID}=(\hat{\boldsymbol{e}}_{id_1},\hat{\boldsymbol{e}}_{id_2},\cdots,\hat{\boldsymbol{e}}_{id_l})$.

4.3 FIBE.Encrypt

输入公共参数 PP，身份属性 $ID'=(id_1',id_2',\cdots,id_l')\subset R_q^l$，加密消息看作系数为 $\{0,1\}$ 的环多项式 $\boldsymbol{m}\in R$.

(1) 设 $D=(l!)^2$；

(2) 随机均匀选取 $\boldsymbol{s}\in R_q$；

(3) 对于 $i\in[l]$，

① 取身份 id_i 构造 $\hat{\boldsymbol{f}}_{id_i}=\begin{pmatrix}\hat{\boldsymbol{g}}_i\\\hat{\boldsymbol{a}}_i+\boldsymbol{u}(id_i')\hat{\boldsymbol{b}}_i\end{pmatrix}$；

② 随机选择系数服从分布 $\mathcal{D}_{\mathbb{Z}^{m\times n},\delta}$ 的环多项式向量 $\hat{\boldsymbol{e}}_x\in R^m$；随机产生 m 个环多项式向量 $\hat{\boldsymbol{r}}_1,\hat{\boldsymbol{r}}_2,\cdots,\hat{\boldsymbol{r}}_m\in R^m$，其系数取自 $\{-1,1\}$，$\hat{\boldsymbol{e}}_y=(\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_1,\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_2,\cdots,\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_m)\in R^m$；

③ 计算 $\hat{\boldsymbol{c}}_i=\hat{\boldsymbol{f}}_{id_i'}\boldsymbol{s}+D\begin{pmatrix}\hat{\boldsymbol{e}}_x\\\hat{\boldsymbol{e}}_y\end{pmatrix}\in R_q^{2m}$.

(4) 选择噪声 $\boldsymbol{e}_z \in R$；

(5) 计算 $\boldsymbol{c}_0 = \boldsymbol{us} + D\boldsymbol{e}_z + \boldsymbol{m}\lfloor q/2 \rfloor \in R_q$.

输出密文 $CT_{ID'} = (\boldsymbol{c}_0, \{\hat{\boldsymbol{c}}_i\}_{i\in[l]})$.

4.4 FIBE.Decrypt(SK_{ID}, $CT_{ID'}$)

输入 PP，私钥 SK_{ID} 和密文 $CT_{ID'}$.

(1) 设 $J \subset [l]$ 表示属性向量中 $\boldsymbol{ID}$ 和 $\boldsymbol{ID}'$ 中匹配元素集合，如果 $|J| < k$，输出 $\perp$，否则计算 Lagrange 系数 L_j 使得

$$\sum_{j\subset J} L_j \boldsymbol{v}_j = \sum_{j\subset J} L_j (\hat{\boldsymbol{f}}_{id_j} \otimes \hat{\boldsymbol{e}}_{id_j}) = \boldsymbol{u}.$$

(2) 计算 $\boldsymbol{m}' = \boldsymbol{c}_0 - \sum_{j\subset J} L_j \hat{\boldsymbol{e}}_j \otimes \hat{\boldsymbol{c}}_j \bmod q$，当 $\boldsymbol{m}'$ 的系数在 $(\lfloor q/4 \rfloor, \lfloor 3q/4 \rfloor]$ 时设为 1，否则为 0.

5 方案分析

5.1 正确性

定理 4. 设 $q > 2tDmnc\delta\sigma$，$c \geq 1$，$t > 15$，利用上述方案产生的密钥加密消息 $\boldsymbol{m}$，那么解密算法以趋近于 1 的概率正确恢复出原文.

证明.

$$\begin{aligned}\boldsymbol{m}' &= \boldsymbol{c}_0 - \sum_{j\subset J} L_j \hat{\boldsymbol{e}}_j \otimes \hat{\boldsymbol{c}}_j \bmod q \\ &= \boldsymbol{us} + D\boldsymbol{e}_z + \boldsymbol{m}\lfloor q/2 \rfloor - \sum_{j\subset J} L_j \hat{\boldsymbol{e}}_j \otimes \left(\hat{\boldsymbol{f}}_{id_j}\boldsymbol{s} + D\begin{pmatrix}\hat{\boldsymbol{e}}_x \\ \hat{\boldsymbol{e}}_y\end{pmatrix}\right) \\ &= \boldsymbol{m}\lfloor q/2 \rfloor + \underbrace{\left(\boldsymbol{us} - \sum_{j\subset J} L_j \hat{\boldsymbol{e}}_j \otimes \hat{\boldsymbol{f}}_{id_i}\boldsymbol{s}\right)}_{=0 \bmod q} + \\ &\quad \underbrace{D\left(\sum_{j\subset J} L_j \hat{\boldsymbol{e}}_j \otimes \begin{pmatrix}\hat{\boldsymbol{e}}_x \\ \hat{\boldsymbol{e}}_y\end{pmatrix} + \boldsymbol{e}_z\right)}\end{aligned}$$

密文要正确解密，必须要求噪声

$$D\left(\sum_{j\subset J} L_j \hat{\boldsymbol{e}}_j \otimes \begin{pmatrix}\hat{\boldsymbol{e}}_x \\ \hat{\boldsymbol{e}}_y\end{pmatrix} + \boldsymbol{e}_z\right)$$

中每一个系数的绝对值不超过 $\lfloor q/4 \rfloor$，下面介绍几个定理来分析噪声的上界.

定理 5[9]. 设 $c \geq 1$，$C = c\exp\left(\frac{1-c^2}{2}\right) < 1$，那么对于任意的实数 $s > 0$ 和 $n \geq 1$，都存在：

$$Pr[\|\mathcal{D}_{\mathbb{Z}^n,s}\| > cs\sqrt{n/2\pi}] \leq C^n.$$

定理 6[9]. 对于任意的实数 $s > 0$，$T > 0$ 和 $\boldsymbol{x} \in \mathbb{R}^n$，有

$$Pr[|\langle \boldsymbol{x}, \mathcal{D}_{\mathbb{Z}^n,s}\rangle| > Ts\|\boldsymbol{x}\|] \leq 2\exp(-\pi T^2).$$

定理 7[4]. 设 $D = (l!)^2$，给定 $k \leq l$ 个数 $I_1, \cdots, I_k \subset [1, 2, \cdots, l]$，定义 Lagrange 系数

$$L_j = \prod_{i\neq j} \frac{-I_i}{(I_j - I_i)}.$$

那么对于 $1 \leq j \leq k$，DL_j 是整数，且满足 $|DL_j| \leq D^2 \leq (l!)^4$.

由于私钥向量 $\hat{\boldsymbol{e}}_j$ 和噪声向量 $\hat{\boldsymbol{e}}_x$ 的系数服从分布 $\mathcal{D}_{\mathbb{Z}^{2m\times n},\sigma}$ 和 $\mathcal{D}_{\mathbb{Z}^{m\times n},\delta}$，且 $\hat{\boldsymbol{e}}_y = (\hat{\boldsymbol{e}}_x \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{e}}_x \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{e}}_x \otimes \hat{\boldsymbol{r}}_m) \in R^m$，所以对于任意的 $1 \leq i \leq m$，有 $\|\hat{\boldsymbol{e}}_{yi}\| \leq \sqrt{mn}\|\hat{\boldsymbol{e}}_{xi}\|$. 根据定理 5，存在一个 $c \geq 1$，使 $\|\hat{\boldsymbol{e}}_{xi}\| \leq c\delta\sqrt{n/2\pi}$. 由环多项式的运算规则，噪声多项式的每一系数相当于 $\sqrt{DL_j m(mn)} \leq Dm\sqrt{n}$ 个系数服从 $\mathcal{D}_{\mathbb{Z}^n,\sigma}$ 分布的 $\boldsymbol{x} \in \mathbb{Z}^n$ 和服从 $\mathcal{D}_{\mathbb{Z}^n,\delta}$ 分布的 $\boldsymbol{y} \in \mathbb{Z}^n$ 的内积，因此解密失败的概率为

$$\begin{aligned}&Pr[Dm\sqrt{n}|\langle \boldsymbol{x}, \boldsymbol{y}\rangle| \geq q/4] \\ &= Pr[|\langle \boldsymbol{x}, \boldsymbol{y}\rangle| \geq q/(4Dm\sqrt{n})] \\ &= Pr[|\langle \boldsymbol{x}, \boldsymbol{y}\rangle| \geq T\sigma\|\boldsymbol{y}\|] \\ &< 2\exp(-\pi T^2),\end{aligned}$$

而 $T = \frac{q}{4Dm\sqrt{n}\sigma\|\boldsymbol{y}\|} \geq \frac{\sqrt{2\pi}q}{4Dm\sqrt{n}\chi\sigma c\sqrt{n}} = t \geq 15$.

显然，概率 $2\exp(-\pi T^2)$ 是可忽略不计的，所以新方案将会以趋近于 1 的概率正确解密. 证毕.

5.2 安全性

定理 8. 假设判定性 R-LWE 问题是困难的，那么新的 FIBE 方案是 IND-sID-CPA 安全的.

证明.

方案安全性证明采用“game-hopping”方法①.

游戏序列：

Game 0. 攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间真实的非适应性选择挑战 ID 和选择明文攻击，如 2.4 小节中 IND-sID-CPA 安全模型，设 $\mathcal{A}$ 要攻击的身份为 ID^*.

Game 1. 在 Game 0 中，挑战者公开的系统参数 $\hat{\boldsymbol{a}}_i$ 取自均匀分布，Game 1 中环多项式 $\hat{\boldsymbol{a}}_i$ 不是随机选取，而通过 $\hat{\boldsymbol{a}}_i = (\hat{\boldsymbol{g}}_i \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{g}}_i \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{g}}_i \otimes \hat{\boldsymbol{r}}_m) - \boldsymbol{u}(id_i^*)\hat{\boldsymbol{b}}_i$ 计算得到，$\hat{\boldsymbol{r}}_1, \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{r}}_m$ 为加密阶段选取的随机环多项式向量，其余参数的选取与 Game 0 相同.

Game 2. 对 Game 1 中参数进行如下修改：$\hat{\boldsymbol{g}}_i \in R^m$ 系数在 $\mathbb{Z}_q$ 上随机均匀选取，不含陷门. 利用 Ideal-TrapGen 产生含有陷门 $\boldsymbol{T}_{\hat{\boldsymbol{b}}_i}$ 的 $\hat{\boldsymbol{b}}_i$，挑战者利用后门 $\boldsymbol{T}_{\hat{\boldsymbol{b}}_i}$ 使用算法 3 为用户 $ID(|ID^* \cap ID| < k)$ 生成私钥.

① Dent A W. A note on game-hopping proofs. http://eprint.iacr.org/2006/260.pdf

算法 3. Ideal-SampleRight($\hat{\boldsymbol{g}}, \boldsymbol{v}, \sigma, id, \hat{\boldsymbol{a}}, \hat{\boldsymbol{b}}, \boldsymbol{T}_{\hat{b}}$).

输入:用户 $id \in \{0,1\}^n$, 环多项式向量 $\hat{\boldsymbol{g}} \in R_q^m$, $\hat{\boldsymbol{a}} \in R_q^m$, $\hat{\boldsymbol{b}}$ 和陷门 $\boldsymbol{T}_{\hat{b}}$

输出:用户 id 的私钥 $\hat{\boldsymbol{e}}_{id} \sim \mathcal{D}_{\mathbb{Z}^{2m\times n},\sigma}$ 且 $\hat{\boldsymbol{e}}_{id} \otimes \hat{\boldsymbol{f}}_{id} = \boldsymbol{v}$

1. $\hat{\boldsymbol{f}}_{id} = \begin{pmatrix} \hat{\boldsymbol{g}} \\ \hat{\boldsymbol{a}} + u(id)\hat{\boldsymbol{b}} \end{pmatrix}$

$= \begin{pmatrix} \hat{\boldsymbol{g}} \\ (\hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_m) + (u(id) - \boldsymbol{u}(id^*))\hat{\boldsymbol{b}} \end{pmatrix}$;

2. 使用如下算法构造 $\hat{\boldsymbol{f}}_{id}$ 的陷门 $\boldsymbol{T}_{\hat{f}_{id}}$.

2.1. 对于 $1 \leq i \leq mn$, $\boldsymbol{c}_i$ 为陷门 $\boldsymbol{T}_{\hat{b}}$ 第 i 列, $\hat{\boldsymbol{t}}_i = Map_{v-M}(\boldsymbol{c}_i) \in R^m$, 那么 $\hat{\boldsymbol{b}} \otimes \hat{\boldsymbol{t}}_i = \boldsymbol{0}$, 设

$$\hat{\boldsymbol{t}}_i' = \begin{pmatrix} -\sum_{j=1}^{m} \hat{\boldsymbol{r}}_i(\hat{\boldsymbol{t}}_i[j]) \\ \hat{\boldsymbol{t}}_i \end{pmatrix}$$

其中 $\hat{\boldsymbol{t}}_i[j]$ 表示 $\hat{\boldsymbol{t}}_i$ 的第 j 个向量, 则 $\hat{\boldsymbol{f}}_{id} \otimes \hat{\boldsymbol{t}}_i' = \hat{\boldsymbol{g}} \otimes \left(-\sum_{j=1}^{m} \boldsymbol{r}_i(\hat{\boldsymbol{t}}_i[j])\right) + ((\hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_m) - (u(id) - u(id^*))\hat{\boldsymbol{b}}) \otimes \hat{\boldsymbol{t}}_i = \boldsymbol{0}$.

2.2. 对于 $1+mn \leq i \leq 2mn$, 设 $\boldsymbol{c}_i$ 为单位矩阵 $\boldsymbol{I}_{mn}$ 第 $i-mn$ 列, $\hat{\boldsymbol{t}}_i = Map_{v-M}(\boldsymbol{c}_i) \in R^m$, 选取一个 $\hat{\boldsymbol{w}}_i$ 使得 $(u(id) - u(id^*))\hat{\boldsymbol{b}} \otimes \hat{\boldsymbol{w}}_i = \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{t}}_i$ (这里没有限制 $\hat{\boldsymbol{w}}_i$ 的长度, 所以容易找到满足条件的 $\hat{\boldsymbol{w}}_i$),

$$\hat{\boldsymbol{t}}_i' = \begin{pmatrix} \hat{\boldsymbol{t}}_i - \sum_{j=1}^{m} \hat{\boldsymbol{r}}_i(\hat{\boldsymbol{w}}_i[j]) \\ \hat{\boldsymbol{w}}_i \end{pmatrix}$$

显然有 $\hat{\boldsymbol{f}}_{id} \otimes \hat{\boldsymbol{t}}_i' = \boldsymbol{0}$.

2.3. $\boldsymbol{T}_{\hat{f}_{id}} = (Map_{M-v}(\hat{\boldsymbol{t}}_1'), Map_{M-v}(\hat{\boldsymbol{t}}_2'), \cdots, Map_{M-v}(\hat{\boldsymbol{t}}_{2mn}'))$, $\|\boldsymbol{T}_{\hat{f}_{id}}\| \leq \|\boldsymbol{T}_{\hat{b}}\| \sqrt{m}\omega(\sqrt{\log m})$ 且 $\widetilde{\boldsymbol{T}}_{\hat{f}_{id}}$ 中 $2mn$ 个向量线性无关(证明可以类似参考文献[11]).

3. $\hat{\boldsymbol{e}}_{id} = \text{ideal-SamplePre}(\hat{\boldsymbol{f}}_{id}, \boldsymbol{T}_{\hat{f}_{id}}, \boldsymbol{v}, \sigma) \in R^m$, 满足 $\hat{\boldsymbol{e}}_{id} \sim \mathcal{D}_{\mathbb{Z}^{2m\times n},\sigma}$.

Game 3. 挑战密文为随机选取互相独立的环多项式向量 $(\boldsymbol{c}_0, \{\hat{\boldsymbol{c}}_i\}_{i\in[l]}) \in R_q \times R_q^{ml}$, 其余设置与 Game 2 中相同.

序列转移: Game 0 到 Game 1. 对多项式时间内的攻击者 $\mathcal{A}$ 而言, Game 0 和 Game 1 概率不可区分, 使用剩余哈希引理在环上的变体(引理 1)容易证明.

引理 1[11]. 设 R 是一个有限环, $\hat{\boldsymbol{a}} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m) \in R^m$ 是一组任意的环多项式, 另有 $\hat{\boldsymbol{b}} \in R^m$ 服从均匀分布且互不相关, 那么 $\hat{\boldsymbol{a}} \otimes \hat{\boldsymbol{b}}$ 在理想 $\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m \rangle$ 上是均匀分布的.

Game 1 到 Game 2. 私钥生成过程对攻击者 $\mathcal{A}$ 是不可见的, 而 $\mathcal{A}$ 获得的私钥 $\hat{\boldsymbol{e}}_{ID}$ 在统计上仍然服从分布 $\mathcal{D}_{\mathbb{Z}^{2ml\times n},\sigma}$, 且满足 $\hat{\boldsymbol{f}}_{ID} \otimes \hat{\boldsymbol{e}}_{ID} = \boldsymbol{0}$. 所以攻击者在 Game 1 中得到的优势与在 Game 2 中得到的优势相当.

Game 2 到 Game 3. 假设攻击者 $\mathcal{A}$ 有不可忽略的优势来区分 Game 2 和 Game 3, 那么挑战者 $\mathcal{C}$ 就可以解决判定性 R-LWE 问题.

如 R-LWE 定义中描述, 存在一个 R-LWE 采样预言机 $\mathcal{O}$, 其随机从 $\mathcal{O}_\$$ 或 $\mathcal{O}_s$ 中选取一些采样作为输出, 挑战者 $\mathcal{C}$ 通过下面的模拟过程与攻击者 $\mathcal{A}$ 进行交互来解决判定性 R-LWE 问题.

实例化: $\mathcal{C}$ 向预言机 $\mathcal{O}$ 询问并接收 $lm+1$ 个 R-LWE 采样, 标记为 $(\boldsymbol{w}_1, \boldsymbol{v}_1), \{(\boldsymbol{w}_1^1, \boldsymbol{v}_1^1), (\boldsymbol{w}_1^2, \boldsymbol{v}_1^2), \cdots, (\boldsymbol{w}_1^m, \boldsymbol{v}_1^m)\}, \cdots, \{(\boldsymbol{w}_l^1, \boldsymbol{v}_l^1), (\boldsymbol{w}_l^2, \boldsymbol{v}_l^2), \cdots, (\boldsymbol{w}_l^m, \boldsymbol{v}_l^m)\} \subset (R_q \times R_q)^{(lm+1)}$.

攻击目标: $\mathcal{A}$ 向 $\mathcal{C}$ 公布它要攻击的目标 ID^*.

设置: $\mathcal{C}$ 构造如下系统参数:

(1) 对于 $i \subset [l]$, $\hat{\boldsymbol{g}}_i = (\boldsymbol{w}_i^1, \boldsymbol{w}_i^2, \cdots, \boldsymbol{w}_i^m)$;

(2) $\boldsymbol{u} = \boldsymbol{w}_1$;

(3) 其余系统参数设置与 Game 2 中的相同.

询问: 当攻击者 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 询问时, $\mathcal{C}$ 如 Game2 中完成私钥询问过程.

挑战: 当攻击者 $\mathcal{A}$ 给挑战者 $\mathcal{C}$ 发送加密消息 $\boldsymbol{m}$ 时, 挑战者 $\mathcal{C}$ 如下构造密文, 对于所有的 $i \subset [l]$:

(1) 设 $\hat{\boldsymbol{c}}_i' = (\boldsymbol{v}_i^1, \boldsymbol{v}_i^2, \cdots, \boldsymbol{v}_i^m)$;

(2) $\hat{\boldsymbol{c}}_i = \begin{pmatrix} \hat{\boldsymbol{c}}_i' \\ (\hat{\boldsymbol{c}}_i' \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{c}}_i' \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{c}}_i' \otimes \hat{\boldsymbol{r}}_m) \end{pmatrix}$;

(3) $\boldsymbol{c}_0 = \boldsymbol{v}_0 + \boldsymbol{m}\lfloor q/2 \rfloor$;

(4) 挑战者 $\mathcal{C}$ 从 $\{0,1\}$ 中随机选取 r, 如果 $r=0$, 密文 $CT_{ID^*} = (\boldsymbol{c}_0, \{\hat{\boldsymbol{c}}_i\}_{i\in[l]})$ 构造如上, 否则随机选取均匀分布的环多项式向量 $\boldsymbol{CT}_{ID^*} = (\boldsymbol{c}_0, \{\hat{\boldsymbol{c}}_i\}_{i\in[l]})$, 将 CT_{ID^*} 发送给攻击者 $\mathcal{A}$.

如果实例化过程中预言机 $\mathcal{O}$ 输出的分布来自 $\mathcal{O}_s$, 那么密文 CT_{ID^*} 的分布与 Game 2 中分布相同, 原因如下:

第一, $\hat{\boldsymbol{f}}_{id_i^*} = \begin{pmatrix} \hat{\boldsymbol{g}}_i \\ (\hat{\boldsymbol{g}}_i \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{g}}_i \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{g}}_i \otimes \hat{\boldsymbol{r}}_m) \end{pmatrix}$ 服从均匀分布;

第二, 设 $\hat{\boldsymbol{c}}_i' = \hat{\boldsymbol{g}}_i \boldsymbol{s} + \hat{\boldsymbol{e}}_x$, 那么密文第二部分为

$$\hat{\boldsymbol{c}}_i = \begin{pmatrix} \hat{\boldsymbol{c}}_i' \\ (\hat{\boldsymbol{c}}_i' \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{c}}_i' \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{c}}_i' \otimes \hat{\boldsymbol{r}}_m) \end{pmatrix}$$

$$=\begin{pmatrix}\hat{\boldsymbol{g}}_i\boldsymbol{s}+\hat{\boldsymbol{e}}_x\\(\hat{\boldsymbol{g}}_i\otimes\hat{\boldsymbol{r}}_1,\hat{\boldsymbol{g}}_i\otimes\hat{\boldsymbol{r}}_2,\cdots,\hat{\boldsymbol{g}}_i\otimes\hat{\boldsymbol{r}}_m)\boldsymbol{s}+\\(\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_1,\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_2,\cdots,\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_m)\end{pmatrix}$$

$$=\hat{\boldsymbol{f}}_{id_i^*}\boldsymbol{s}+\begin{pmatrix}\hat{\boldsymbol{e}}_x\\(\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_1,\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_2,\cdots,\hat{\boldsymbol{e}}_x\otimes\hat{\boldsymbol{r}}_m)\end{pmatrix}.$$

第一部分为 $\boldsymbol{c}_0=\boldsymbol{v}_1+\boldsymbol{m}\lfloor q/2\rfloor$. 两部分都与 Game 2 中挑战的密文分布相同.

如果实例化过程中预言机 $\mathcal{O}$ 输出的分布来自 $\mathcal{O}_\$$，那么根据引理 1，通过计算得到密文分布统计上服从随机均匀分布，而在 Game 3 中，密文 $(\boldsymbol{c}_0,\{\hat{\boldsymbol{c}}_i\}_{i\in[l]})$ 正是随机取于均匀分布.

猜测：询问过后，$\mathcal{A}$ 给出一个猜想 $b'\in\{0,1\}$，这里 $b'=1$ 意味着攻击者 $\mathcal{A}$ 正在与 Game2 交互，挑战者 $\mathcal{C}$ 回答 R-LWE 挑战的猜测 $\beta'=b'$，这里 $\beta'=1$ 意味着上述实例 $(\boldsymbol{w}_i,\boldsymbol{v}_i)$ $(1\leq i\leq lm+1)$ 服从 R-LWE 分布，否则 $\beta'=0$ 表示实例服从随机均匀分布.

以上完成了对挑战者 $\mathcal{C}$ 的描述，可以看出如果 $\mathcal{A}$ 能够以不可忽略的优势区分 Game 2 和 Game 3，那么挑战者 $\mathcal{C}$ 能够以绝对的优势解决判定性 R-LWE 问题.

通过以上 4 个等价游戏，我们将新方案的安全性紧凑地归约为判定性 R-LWE 困难性假设，证明了其满足 IND-sID-CPA 安全.　　证毕.

5.3　效率分析

基于格上困难问题的 FIBE 方案只包括群上的加法和乘法，不涉及双线性对的复杂运算和大整数运算，比传统的基于对技术的 FIBE 方案效率明显提高. 表 1 是本文基于理想格上 FIBE 方案和基于标准格上 FIBE 方案[4]（ABVVW11 方案）的效率比较. 可以看出，本文的 FIBE 每次处理的消息为一个 n 比特的块矩阵，加解密过程都是在多项式环上进行，通过快速傅里叶变换 FFT（Fast Fourier Transform）可以大幅度提高加解密速度，虽然表中两种方案中公钥大小和密文扩展率的表达式是相同的，但当这两种方案达到相同安全级别时，本文基于 R-LWE 的方案需要的采样数 m 很小，因此公钥大小和密文扩展率得到降低. 在私钥长度方面，新方案的长度约为 ABVVW11 方案的 2 倍，但是考虑到私钥在本地安全储存的，因此这个缺陷对方案的整体效率影响不大.

表 1　两种不同方案的相关加密算法效率对比

方案	采样数	公钥大小/bit	私钥长度/bit	明文长度	密文扩展率	运算方法
ABVVW 方案[4]	$m=\Omega(n\log q)$	$3mln\log q$	ml	单比特	$(2ml+1)\log q$	矩阵运算
本文方案	$m=\Omega(\log q)$	$3mln\log q$	$2nml$	n 比特	$(2ml+1)\log q$	FFT 运算

6　结　论

模糊身份加密体制能够容忍部分错误公钥信息，使得解密更为灵活和实用，已经成为近几年来研究的一个热点，而一种密码体制要应用于实际环境，必须在保证其安全性的前提下尽可能地提高其执行效率. 本文基于 R-LWE 困难假设，在标准模型下构造了一种 IND-sID-CPA 安全的多比特 FIBE 方案，相比于以前基于标准格上 LWE 的方案，新方案公钥长度更短，密文扩展率更低.

参　考　文　献

[1] Sahai A, Waters B. Fuzzy identity based encryption// Proceedings of the Eurocrypt 2005. Aarhus, Denmark, 2005: 457-473

[2] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data// Proceedings of the ACM CCS 2006. Alexandria, Virginia, USA, 2006: 89-98

[3] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products// Proceedings of the Eurocrypt 2008. Istanbul, Turkey, 2008: 146-162

[4] Agrawal S, Boyen X, Vaikuntanathan V, et al. Functional encryption for threshold functions (or, fuzzy IBE) from lattices//Proceedings of the Public Key Cryptography (PKC 2012). Darmstadt, Germany, 2012: 280-297

[5] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings//Proceedings of the EUROCRYPT 2010. Monaco and Nice, French, 2010: 1-23

[6] Lyubashevsky V, Peikert C, Regev O. A toolkit for ring-LWE cryptography//Proceedings of the EUROCRYPT 2013. Athens, Greece, 2013: 35-54

[7] Stehlé D, Steinfeld R, Tanaka K, Xagawa K. Efficient public key encryption based on ideal lattices//Proceedings of the ASIACRYPT 2009. Tokyo, Japan, 2009: 617-635

[8] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions//Proceedings of the STOC 2008. Victoria, British Columbia, Canada, 2008: 197-206

[9] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing, 2007, 37(1): 267-302

[10] Banaszczyk W. Inequalites for convex bodies and polar reciprocal lattices in Rn. Discrete & Computational Geometry, 1995, 13(1): 217-231

[11] Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model//Proceedings of the EUROCRYPT 2010. Monaco and Nice, French, 2010: 553-572

[12] Lyubashevsky V, Micciancio D. Generalized compact knapsacks are collision resistant//Proceedings of the Automata, Languages and Programming (ICALP 2006). 2006: 144-155

WU Li-Qiang, born in 1986, M. S., lecturer. His research interests include cryptosystems based on lattices and provable security theory.

YANG Xiao-Yuan, born in 1959, M. S., professor. His research interests mainly include information security and cryptography.

HAN Yi-Liang, born in 1977, Ph.D., associate professor. His research interests mainly include cryptography and network security.

Background

This work is supported by the National Natural Science Foundation of China (Nos. 61272492, 61103231, 61103230) and the Natural Science Basic Research Plan in Shaanxi Province of China (2011JM8012). In these projects, many key problems relate to analogical design of Identity Related Encryption (IRE), such as IBE, HIBE, FIBE and ABE, based on the pairing backbone and the lattices backbone, which will construct efficient and provably security IRE schemes, including ideal lattices based IRE, fully secure lattices based IRE under the standard model, through learning from the pairing based key techniques, or using the lattices based techniques. At present, the main drawback of cryptography based on standard lattices is its limited efficiency, in this paper, we use a hard problem from ideal lattices that is R-LWE assumption, to overcome this obstacle. The advantage of ideal lattices based cryptographic primitives over lattices based cryptographic primitives is that they can achieve more compact ciphertext and smaller key sizes by a factor of n, and thus adds more efficiency. So ideal lattices with their compact structure would help us to make the IRE schemes more practical and efficient.