文章编号:1671-4229(2022)04-0037-09

理想格上基于身份的加密算法研究

黄文晋[a],唐春明[b,c*],贾惠文[b,c]
(广州大学 a. 数学与信息科学学院; b. 广州数学中心;
c. 广东省广州市共建信息安全技术重点实验室,广东 广州 510006)

摘 要:格上基于身份的加密算法(Identity-Based Encryption,IBE)可以抵抗量子攻击,能有效解决公钥密码管理系统效率低的问题,因此,国内外学者提出了一系列基于格的身份加密方案。文章运用Jia等提出的基于非球形高斯的原像采样算法,对IBE方案中用户私钥的提取进行了改进。实验结果表明,在保证IBE加密与解密正确性的情况下,可以有效降低用户私钥的尺寸,提升IBE方案的空间效率。文章运用的基于非球形高斯的用户私钥提取算法有2个模式:①采用模式1后,在42.6-bit的安全性下,用户私钥的尺寸由21.75 kB减小至13.31 kB;在109.8-bit的安全性下,用户私钥的尺寸由50.36 kB减小至32.25 kB;②采用模式2后,在42.6-bit的安全性下,用户私钥的尺寸由21.75 kB减小至10.18 kB;在109.8-bit的安全性下,用户私钥的尺寸由50.36 kB减小至21.86 kB,相比于模式1,模式2能更有效地节省用户私钥的内存开销。

关键词:格密码; IBE; 非球形高斯采样
中图分类号:TP 309 **文献标志码**:A

Research on identity-based encryption algorithms on the ideal lattice

HUANG Wen-jin[a], *TANG Chun-ming*[b,c*], *JIA Hui-wen*[b,c]
(a. School of Mathematics and Information Science; b. Guangzhou Center for Applied Mathematics;
c. The Key Laboratory of Information Security Technology, Guangzhou 510006, China)

Abstract: Identity-Based Encryption (IBE) on lattices resists quantum attacks and effectively solves the problem of low efficiency of public key cryptography management systems, so scholars at home and abroad have proposed a series of lattice-based identity encryption schemes. In this paper, the extraction of user private keys in the IBE scheme is improved by using the prototype sampling algorithm based on non-spherical Gaussian proposed by Jia, et al. Experimental results show that under the condition of ensuring the correctness of IBE encryption and decryption, the size of the user's private key can be effectively reduced and the space efficiency of the IBE scheme can be improved. The non-spherical Gaussian-based user private key extraction algorithm used in this article has two modes: ① After adopting mode 1, the size of the user's private key is reduced from 21.75 kB to 13.31 kB under the security of 42.6-bit; under the security of 109.8-bit, the size of the user's private key is reduced from 50.36 kB to 32.25 kB; ② After adopting mode 2, under the security of 42.6-bit, the size of the user's private key is reduced from 21.75 kB to 10.18 kB; under the security of 109.8-bit, the size of the user's private key is reduced from 50.36 kB to 21.86 kB, which can more effectively save the memory overhead of the user's private key than mode 1.

Key words: lattice cryptography; IBE; non-spherical Gaussian

收稿日期:2022-09-10; **修回日期**:2022-10-13

作者简介:黄文晋(1997—),男,硕士研究生. E-mail:1770508188@qq.com
* 通信作者. E-mail:ctang@shu.edu.cn

引文格式:黄文晋,唐春明,贾惠文. 理想格上基于身份的加密算法研究[J]. 广州大学学报(自然科学版),2022,21(4):37-45.

随着网络通信的用户数量骤增以及网络环境对安全性的要求越来越高,公钥密码基础设施(Public Key Infrastructure, PKI)由于必须依赖数字证书,需要越来越强的存储能力、查询能力以及越来越高的安全性,其繁重的管理系统适应不了当今的网络环境。基于身份的加密机制(Identity-Based Encryption, IBE)是一种经典的公钥加密方案,其概念首次由 Shamir 提出,IBE 允许用户的身份信息作为公钥,比如用户的邮箱地址等等[1],加密时可以直接使用接收方的身份标识作为公钥,为公钥信息的管理提供了便利,解决了 PKI 效率低的问题。2001 年,Boneh 等[2]正式给出 IBE 的定义和安全模型,后来基于双线性映射和二次剩余假设构造的 IBE 方案被相继提出,但都无法抵抗量子攻击。

格密码(Lattices Cryptography)是一种后量子密码,经过十几年的快速发展,有着显著的特征和优势:能抵抗量子攻击、并行运算,以及格上某些困难问题存在最坏情况到平均情况的归约,给格密码方案提供了安全的保障。格密码的研究工作由 Ajtai 开始,他提出了格的困难问题可以作为格密码方案构造的安全基础[3],目前格的困难问题有 2 个:① Ajtai 提出的小整数解问题[3](Small Integer Solution Problem, SIS),还有非齐次版本的变体(Inhomogeneous Small Integer Solution Problem, I-SIS);②Regev[4]提出的容错学习问题(Learning With Errors Problem, LWE),他们都给出最坏情况下基于格的问题向平均情况下 SIS 问题和 LWE 问题的规约。在 2007 年和 2009 年,有学者分别提出这两种困难问题的基于环结构的变体[5-6],即 *R*-SIS 问题和 *R*-LWE 问题,其优点是储存更低,运算效率更高,同时也存在最坏情况下基于理想格的问题向平均情况下 *R*-SIS 问题和 *R*-LWE 问题规约的优良特性。

第一个基于格的 IBE 方案由 Gentry 等[7]提出,是基于 Dual-Regev 加密算法设计的。后来,有学者对此进行了研究和改进。2010 年,Agrawal 等[8]构建了基于格的 IBE 方案,称为 ABB 方案,他们使用的公钥矩阵是由两部分组成,私钥是分两步骤采样而得的,虽然后来有很多学者都一直沿用这种方案,但是公钥和私钥内存开销大,不切实际。2014 年,Ducas 等[9]构造了一种基于 NTRU 格的 IBE 方案,公钥矩阵是由 NTRU 格构建的,因此算法效率高。2018 年,Bert 等[10]提出基于 *R*-SIS 和 *R*-LWE 构建的 IBE 方案(Bert-Fouque-Roux-Sabt, BFRS),他们利用了 MP 提出的(Micciancio-Peikert, MP)的原像采样算法[11],并结合 GM(Genise-Micciancio, GM)提出了 G-格采样和扰动向量的方法[12],对私钥的提取作了改进和优化,虽然效率比 Ducas 等提出的基于 NTRU 格构建的 IBE 方案要高,但是公钥和用户私钥的尺寸还是不够小。而最近的研究工作由钱心缘等[13]提出了一种基于 *R*-SIS 和 *R*-LWE 构造的 IBE 方案(本文简称 QW 方案),对 BRFS 方案进行了优化,并且采用了分块复用技术,降低了密文膨胀率,但是这种技术始终存在不能降低所有用户私钥的内存空间、用户私钥的内存开销仍然比较大的缺点,还有,笔者认为 QW 方案中私钥提取算法的安全性还不够高。

结合以上的分析以及针对以上方案的不足,本文运用非球形高斯采样[14]的原理,对用户私钥提取算法进行改进,从而提升格上的 IBE 方案的空间效率。非球形高斯的原像采样原理由 Jia 等[14]在 2020 年提出,这种原像的分布不会泄露陷门信息,并且他们给出了 2 种模式:①第一种模式可以提升安全性,同时降低签名尺寸;②第二种模式在安全性几乎不变的情况下进一步降低签名尺寸。本文运用以上的原理和方法,在理想格上研究,对 QW 方案的用户私钥提取算法作改进,减小私钥的内存开销,提升方案的空间效率,力图提升方案的安全性。

1 基本理论

本部分介绍本文所需要的理论,包括格的相关定义及其理论、IBE 的基本架构、加解密原理和理想格上的原像采样算法。

1.1 格及其相关理论

定义 1(格[15]) 给定一组 n 维线性无关的向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$,格定义为

$$\Lambda = L(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m) = \{\sum_{i=1}^{m} x_i\boldsymbol{b}_i \mid x_i \in \mathbb{Z}\},$$

其中 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 是格 Λ 的一组基,若定义 $\boldsymbol{B}$ 为格 Λ 的基矩阵,列由 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 组成,则格 Λ 可以由 $\boldsymbol{B}$ 生成,表示为

$$\Lambda = L(\boldsymbol{B}) = \{\boldsymbol{Bx} \mid \boldsymbol{x} \in \mathbb{Z}^m\},$$

格 Λ 的秩为 m,维数为 n,当 $n=m$ 时称其为满秩格。

定义 2(分圆多项式环[16-17]) 令 n 为正整数,有理数域 $\mathbb{Q}$ 上 n 次分圆域为 $\mathbb{Q}(\xi)$,同构于 $C_n = \mathbb{Q}[x]/\Phi_n(x)$,其中 ξ 是 n 次本原单位根,令 $\varphi(n)$ 为 n 的欧拉函数,C_n 为 $\mathbb{Q}$ 上 $\varphi(n)$ 维向量空间,$\Phi_n(x)$ 为 $\mathbb{Z}$ 上 $\varphi(n)$ 次不可约多项式。而 $\Phi_{2n}(x)$ 为 $2n$ 次分圆多项式,其中 n 为 2 的幂次方,定义 $R \equiv \mathbb{Z}[x]/\Phi_{2n}(x)$,即 $R \equiv \mathbb{Z}[x]/x^n+1$。令 $q \geqslant 2$ 且为正整数,定义 $R_q \equiv R/qR$,表示多项式

环 R 中每个多项式的系数模 q,即 $R_q \equiv \mathbb{Z}_q[x]/x^n+1$,本文基本在 R_q 下进行讨论和研究。

定义 3(理想格)　易知 $\mathbb{Z}_q^n$ 与环 R_q 是同构的,因此,环 R_q 可看作一种特殊的格。又因为 $\forall \gamma \in R, \delta \in R_q, \gamma\delta \in R_q$,所以 R_q 是 R 的理想。一般地,环 R_q 是环 R 的理想且与格 $\mathbb{Z}_q^n$ 同构,称之为理想格。

定义 4(多项式的系数嵌入[18])　R 和 R_q 为定义 2 中的多项式环,设 $p(x) \in R(R_q)$,多项式的系数嵌入定义为一个从多项式环到整数向量的映射

$$p(x) \mapsto \boldsymbol{p} = (p_0, \cdots, p_{n-1})。$$

令 $h(x) = \sum_{i=0}^{n-1} h_i(x^i)$,有反循环矩阵:

$$\psi(h) = \begin{bmatrix} h_0 & -h_{n-1} & -h_{n-2} & \cdots & -h_1 \\ h_1 & h_0 & -h_{n-1} & \cdots & -h_2 \\ h_2 & h_1 & h_0 & \cdots & -h_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n-1} & h_{n-2} & h_{n-3} & \cdots & h_0 \end{bmatrix} \in \mathbb{Z}^{n\times n}(\mathbb{Z}_q^{n\times n}),$$

而 $\psi(h) \times p$ 为 $p(x) \cdot h(x)$ 的系数嵌入。其中,映射 $\psi: R(R_q) \to \mathbb{Z}^{n\times n}(\mathbb{Z}_q^{n\times n})$ 是多项式环到反循环矩阵的映射,是另一种系数嵌入。特别地,当 $\alpha \in \mathbb{Z}(\mathbb{Z}_q) \subset R(R_q)$ 时,$\psi(\alpha) = \alpha \boldsymbol{I}_n \in \mathbb{Z}^{n\times n}(\mathbb{Z}_q^{n\times n})$。此外,设 $\boldsymbol{v}$ 是 $R(R_q)$ 上的 l 维向量,其系数嵌入为

$$(\boldsymbol{v}_0, \cdots, \boldsymbol{v}_{n-1}) \mapsto (v_{0,0}, \cdots, v_{0,n-1}, \cdots, v_{l-1,0}, \cdots, v_{l-1,n-1})。$$

定义 5(q 模格)　设 n, m, q 为正整数,给定矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$,定义

$$\Lambda_q^{\perp}(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{x} = 0 \bmod q\},$$

$$\Lambda_q(\boldsymbol{A}) = \{\boldsymbol{z} \in \mathbb{Z}^n \mid \exists \boldsymbol{s} \in \mathbb{Z}^m, \boldsymbol{A}\boldsymbol{s} = \boldsymbol{z} \bmod q\},$$

$$\Lambda_q^{u}(\boldsymbol{A}) = \{\boldsymbol{y} \in \mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{y} = \boldsymbol{u} \bmod q\},$$

若 $\boldsymbol{w}$ 为 $\boldsymbol{A}\boldsymbol{y} = \boldsymbol{u} \bmod q$ 的特解,则 $\Lambda_q^{u}(\boldsymbol{A}) = \Lambda_q^{\perp}(\boldsymbol{A}) + \boldsymbol{w}$。

定义 6(离散高斯函数[10])　对于任意的 $\boldsymbol{x} \in \mathbb{R}^n$,中心为 $\boldsymbol{c} \in \mathbb{R}^n$,宽度参数为 $s > 0$ 的离散高斯函数定义为 $\rho_{s,c}(\boldsymbol{x}) = \exp\left(-\pi \frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}\right)$。拓展宽度参数 $\boldsymbol{s}$ 的定义,协方差矩阵为 $\boldsymbol{\Sigma} > 0$($\boldsymbol{\Sigma}$ 表示为正定矩阵,且 $\boldsymbol{\Sigma} = \boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}$),中心为 $c \in \mathbb{R}^n$ 的离散高斯函数定义为

$$\rho_{\sqrt{\Sigma},c}(x) = \exp(-\pi(x-c)^{\mathrm{T}}\boldsymbol{\Sigma}^{-1}(x-c))。$$

定义 7(离散高斯分布[10])　格 Λ 上的离散高斯分布 $D_{\Lambda,\sqrt{\Sigma},c}$ 定义为

$$D_{\Lambda,\sqrt{\Sigma},c} = \frac{\rho_{\sqrt{\Sigma},c}(x)}{\rho_{\sqrt{\Sigma},c}(\Lambda)} = \frac{\rho_{\sqrt{\Sigma},c}(x)}{\sum_{x\in\Lambda}\rho_{\sqrt{\Sigma},c}(x)}。$$

定义 8(对偶格,光滑参数[14,19])　格 $\Lambda \subset \mathbb{R}^n$ 的对偶格定义为:$\Lambda^* = \{\boldsymbol{w} \mid \langle \boldsymbol{w}, \Lambda \rangle \subseteq \mathbb{Z}\}$。而光滑参数 $\eta_\varepsilon(\Lambda)$ 由 $\varepsilon > 0$ 参数化,定义为使得 $\rho_{1/s}(\Lambda^*) \leqslant 1+\varepsilon$ 成立的 $\boldsymbol{s}$ 的最小值。对于 $\Sigma > 0$,且格 $\Lambda \subset \mathrm{span}(\Sigma)$,若 $\rho_{\sqrt{\Sigma^{-1}}}(\Lambda^*) \leqslant 1+\varepsilon$,则定义 $\sqrt{\Sigma} \geqslant \eta_\varepsilon(\Lambda)$。

定义 9($R-\mathrm{SIS}_{q,\beta,m}$ 问题[20])　给定 m 个均匀随机的多项式 $a_i \in R_q$,定义 m 维向量 $\boldsymbol{a} = (a_0, \cdots, a_{m-1}) \in R_q^m$,求解一个非零的向量 $x \in R^m$,使得

$$\langle \boldsymbol{a}, \boldsymbol{x} \rangle = \boldsymbol{a}^{\mathrm{T}}\boldsymbol{x} = \sum_{i=0}^{m-1} a_i x_i = 0 \in R_q,$$

其中 $\|\boldsymbol{x}\| \leqslant \beta, 0 < \max_i(x_i) \leqslant \beta$。

定义 10($R-\mathrm{ISIS}_{q,\beta,m}$ 问题[20])　给定 m 个均匀随机的多项式 $a_i \in R_q$ 以及多项式 $\boldsymbol{u} \in R_q$,定义 m 维向量 $\boldsymbol{a} = (a_0, \cdots, a_{m-1}) \in R_q^m$,求解一个非零的向量 $\boldsymbol{x} \in R^m$,使得

$$\langle \boldsymbol{a}, \boldsymbol{x} \rangle = a^{\mathrm{T}}\boldsymbol{x} = \sum_{i=0}^{m-1} a_i x_i = u,$$

其中 $\|\boldsymbol{x}\| \leqslant \beta, 0 < \max_i(x_i) \leqslant \beta$。

定义 11(Decision $R-\mathrm{LWE}_{q,\chi,m}$ 问题[21-22])　给定 m 个独立的样本 $(a_i, b_i) \in R_q \times R_q$,对于由 (a_i, b_i) 组成的 $(\boldsymbol{a}, \boldsymbol{b}) \in R_q^m \times R_q^m$,需判断来自哪种分布:(1) $A_{s,\chi}$ 分布:$\boldsymbol{a} \leftarrow U(R_q^m)$,$\boldsymbol{b} = \boldsymbol{a}s + \boldsymbol{e}$,其中秘密 $s \leftarrow U(R_q)$(每个样本 (a_i, b_i) 中的 s 是固定),噪音 $\boldsymbol{e} \leftarrow \chi$;(2) $R_q^m \times R_q^m$ 上的均匀随机分布。

R-SIS 问题、*R*-ISIS 问题和 Decision *R*-LWE 问题的困难性:*R*-SIS 问题和 *R*-ISIS 问题是等价的;*R*-SIS 问题和 Decision *R*-LWE 的困难性与 GapSVP_γ/SIVP 困难问题等价的[20-22]。

引理 1[7]　设格 $\Lambda \subset \mathbb{R}^m$,其基矩阵为 $\boldsymbol{B}$,令 $\varepsilon > 0$,格 Λ 的光滑参数存在上界

$$\eta_\varepsilon(\Lambda) \leqslant \|\widetilde{\boldsymbol{B}}\| \sqrt{\ln(2m(1+1/\varepsilon)/\pi)}。$$

引理 2[23]　设 m 维格 Λ,其基矩阵为 $\boldsymbol{B}$,若 $s \geqslant \eta_\varepsilon(\Lambda)$,则 $\Pr_{x\leftarrow D_{\Lambda,s}}[\|\boldsymbol{x}\| \geqslant s\sqrt{m}] \leqslant negl(m)$,其中 $negl(m)$ 为关于 m 的可忽略函数。

引理 3[24]　设 $\boldsymbol{x} \in \mathbb{Z}^m$,$\|\boldsymbol{x}\| \leqslant s\sqrt{m}$,则储存向量 $\boldsymbol{x}$ 所需最大的比特数的下界为 $m(1+\lceil \log s \rceil)$。

引理 4[13]　设 n 阶多项式 $x \in R_q$,$y \in R_q$,x 的系数嵌入 $(x_1, \cdots, x_n)$ 服从中心点为 0,方差为 η 的高斯分布,而 y 的系数嵌入 $(y_1, \cdots, y_n)$ 服从中心点为 0,方差为 ξ 的高斯分布,则 $z = xy \in R_q$ 服从中心点为 0,方差为 $n\eta\zeta$ 的近似高斯分布。因为根据定义 2 的说明,$z = xy \in R_q$

的系数嵌入为

$$(z_1,\cdots,z_n)=(x_0,\cdots,x_n)\cdot\begin{bmatrix} y_0 & -y_{n-1} & -y_{n-2} & \cdots & -y_1 \\ y_1 & y_0 & -y_{n-1} & \cdots & -y_2 \\ y_2 & y_1 & y_0 & \cdots & -y_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_{n-1} & y_{n-2} & y_{n-3} & \cdots & y_0 \end{bmatrix}。$$

因此,$z=xy$ 的每一项系数为 $z_i=x_0y_i+x_1y_{i-1}+\cdots+x_iy_0-x_{i+1}y_{n-1}-x_{i+2}y_{n-2}-\cdots-x_{n-1}y_{i+1}$ 是 n 个分布为中心点为0,方差为 $\eta\zeta$ 的线性组合,因此,$z=xy$ 的系数嵌入服从中心点为0,方差为 $n\cdot\eta\zeta$ 的高斯分布。

1.2 基于身份的加密机制[7,10]

基于身份的加密机制包含4个算法:Setup、Extract、Encrypt 和 Decrypt。身份信息用作用户的公钥使用,在 IBE 中需要一个私钥生成中心(Private Key Generator, PKG),PKG 根据安全参数 λ 给出主公钥(Master Public Key, MPK)和主私钥(Master Secret Key, MSK),并用 msk 为每一个用户提取相应的私钥。

(1) Setup,给定安全参数 λ,算法 Setup 生成 mpk 和 msk,$\text{Setup}(1^\lambda)\rightarrow(mpk,msk)$。

(2) Extract,输入安全参数 λ、mpk、msk 和一个用户身份 id,然后利用私钥提取算法,输出属于该用户的私钥(Secret Key, SK),$sk_{id}\leftarrow\text{Extract}(mpk,msk,id)$。

(3) Encrypt,输入 mpk,用户身份 id、明文 M,输出密文 C,$C\leftarrow\text{Encrypt}(mpk,id,M)$。

(4) Decrypt,输入 sk、C,输出明文 M,$M\leftarrow\text{Decrypt}(sk_{id},C)$。

Dual-Regev 公钥加密最先由 Gentry 等[7]提出,本文使用基于环结构的版本。需要的参数有:多项式的阶 n,维数 m,以及高斯参数 s,α。

mpk 和 sk 的生成:$mpk=(\boldsymbol{a},u)$,其中 $u\leftarrow U(R_q)$,用户私钥 $\boldsymbol{x}\leftarrow D_{R^m,s}$,且满足 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=\boldsymbol{u}\in R_q$。

加密:设有一个多项式明文 $M\in R_2$,密文块 $(\boldsymbol{b},c)$ 是 $m+1$ 维的 R-LWE 样本,其中 $\boldsymbol{b}=\boldsymbol{a}s+\boldsymbol{e}$,秘密 $s\leftarrow U(R_q)$,$\boldsymbol{e}\leftarrow D_{R^m,\alpha}$,$c=us+e'+\lfloor q/2\rfloor\cdot M$,$e'\leftarrow D_{R,\alpha}$。

解密:解密密文需要通过私钥 $\boldsymbol{x}$ 进行计算,

$res=c-\boldsymbol{b}^{\mathrm{T}}\boldsymbol{x}=us+e'+\lfloor q/2\rfloor\cdot M-(\boldsymbol{a}^{\mathrm{T}}s+\boldsymbol{e}^{\mathrm{T}})\boldsymbol{x}$,$=e'-\boldsymbol{e}^{\mathrm{T}}\boldsymbol{x}+\lfloor q/2\rfloor\cdot M$,计算得出 res 的系数嵌入 res_i,若 res_i 与0的距离小于与 $\lfloor q/2\rfloor$ 的距离,则 $res_i=0$,否则 $res_i=1$。

若 $R-\text{LWE}_{q,m,D_{R,\alpha}}$ 困难问题成立,则 Dual-Regev 公钥加密方案是 IND-CPA 安全的[25]。

1.3 G-格的陷门与原像采样算法[11-12]

IBE 机制中,PKG 生成的用户公钥需要由 G-格来构造[11],提取用户的私钥则需要由 MP 提出的原像采样算法[11]来求解。下面对 G-格陷门[11]以及 MP 提出的原像采样算法[11]作简要的介绍。

在理想格上,基于 Ajtai 提出的陷门函数[3]:$f_a(\boldsymbol{x})=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}$,给定目标 $u\in R_q$ 和随机的多项式向量 $\boldsymbol{a}\in R_q^m$,求解一个短的原像 $\boldsymbol{x}\in R^m$ 使得 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=u$ 成立,R-ISIS 问题的困难性说明了求解 $\boldsymbol{x}$ 是困难的。对此困难问题,MP[11]构造了 G-格、利用了陷门 $\boldsymbol{T}$ 求解 $\boldsymbol{x}$。结合 IBE 机制,用户私钥 $\boldsymbol{x}$ 是利用主私钥 $\boldsymbol{T}$ 进行原像采样算法而得,在没有陷门 $\boldsymbol{T}$ 的情况下,提取用户私钥 $\boldsymbol{x}$ 是困难的。

理想格上,$\boldsymbol{g}$-向量是由常量多项式组成的,定义为

$$\boldsymbol{g}^{\mathrm{T}}=(1,b,\cdots,b^{k-1})\in R^{1\times k},$$

其中,$k=\lceil\log_2 b\rceil$。格 $\Lambda_q^{\perp}(\boldsymbol{g}^{\mathrm{T}})$ 存在基矩阵 $\boldsymbol{B}_q$,其施密特正交化矩阵满足 $\|\tilde{\boldsymbol{B}}_q\|\leqslant\sqrt{b^2+1}$。本文理想格上的 $\boldsymbol{g}$-格采样的高斯参数为 $\sigma,\sigma\geqslant\sqrt{b^2+1}\cdot r$。

用户公钥多项式向量 $\boldsymbol{a}\in R_q^m$ 是由均匀随机的 $\bar{\boldsymbol{a}}\in R_q^{m-k}$、具有代数结构的 $\boldsymbol{g}$-向量和陷门 $\boldsymbol{T}\in R_q^{(m-k)\times k}$ 组成以及计算而得的,即 $\boldsymbol{a}=[\bar{\boldsymbol{a}}\,|\,h\boldsymbol{g}^{\mathrm{T}}-\bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$;陷门 $\boldsymbol{T}$ 是由小多项式组成的矩阵,每个多项式元素的系数是服从$\mathbb{Z}$上的参数为 τ 的高斯分布。补充说明:标签是 $h\in R_q$ 可逆的。由公钥向量 $\boldsymbol{a}$ 的构造可得如下关系:

$$\boldsymbol{a}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{T}\\ \boldsymbol{I}_k\end{bmatrix}=h\boldsymbol{g}^{\mathrm{T}}。$$

通常情况下,公钥向量使用 hermite 正规形式[18],即 $\bar{\boldsymbol{a}}=(1,\hat{\boldsymbol{a}})\in R_q^{1\times(m-k)}$,$\hat{\boldsymbol{a}}\leftarrow U(R_q^{m-k-1})$。

原像采样算法问题,是如何求解一个短的原像 $\boldsymbol{x}\in R^m$,使得 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=u$ 成立的问题,在 QW 方案中,原像采样算法沿用的是 GM 提出的 G-格采样方法和扰动向量采样算法[12],不妨记作 GM-SamplePolyG 算法[12]和 GM-SampleP 算法[12],其步骤如下:

算法 1.1[10-12] $\text{SamplePre}(\boldsymbol{a},u,\boldsymbol{T},h,s,\sigma)$

输入:公钥向量 $\boldsymbol{a}\in R_q^m$,目标向量 $u\in R_q$,陷门 $\boldsymbol{T}\in R_q^{(m-k)\times k}$,用户标签 $h\in R_q$,高斯宽度参数 s,σ,

输出:$\boldsymbol{x}\in R^m$,使得 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=u$ 成立,

(1) $\boldsymbol{p}\leftarrow\text{GM-SampleP}(q,s,\sigma,\boldsymbol{T})$,$v=h^{-1}(u-\boldsymbol{a}\boldsymbol{p})$,

(2) $\boldsymbol{z}\leftarrow\text{GM-SamplePolyG}(\sigma,v)$,$\boldsymbol{x}=\boldsymbol{p}+\begin{bmatrix}\boldsymbol{T}\\ \boldsymbol{I}_k\end{bmatrix}\boldsymbol{z}$

返回:$\boldsymbol{x}$。

其中, GM-SamplePolyG 是采样 z 的算法, 即 $z \leftarrow D_{\Lambda_q^{\perp}(g^{\mathrm{T}}),\sigma,v}$,而在理想格上,算法是对目标向量 $\boldsymbol{v}$ 的系数嵌入进行 $\boldsymbol{g}$-格采样,首先对 $\boldsymbol{v}$ 分成 n 个 v_i,然后分别对 v_i 执行算法 GM-SamplePolyG,使得 $\boldsymbol{g}^{\mathrm{T}}\boldsymbol{z}_i' = \boldsymbol{v}_i$, $\boldsymbol{z}_i' \in \mathbb{Z}^k$,再组合成 $\boldsymbol{z}' = (\boldsymbol{z}_1', \cdots, \boldsymbol{z}_n') \in \mathbb{Z}^{nk}$,最后 $\boldsymbol{z} = \boldsymbol{P}_g \boldsymbol{z}_n' \in R^k$;而 GM-SampleP 则是采样扰动向量 $\boldsymbol{p}$ 的算法,最后的向量 $\boldsymbol{p}$ 服从分布 $D_{R_q^m,\sqrt{\Sigma_p}}$。(其中 $\boldsymbol{\Sigma}_p, \boldsymbol{T}, \boldsymbol{I}_k$ 为块矩阵,每一块子矩阵都是反循环矩阵)。

原像 $\boldsymbol{x}$ 服从的分布为 $\boldsymbol{\Sigma}_x = \boldsymbol{\Sigma}_p + \sigma^2 \begin{bmatrix} \boldsymbol{T} \\ \boldsymbol{I}_k \end{bmatrix} [\boldsymbol{T} \quad \boldsymbol{I}_k] = s^2 \boldsymbol{I}_m$,另外原像采样算法的正确性由此体现[11]

$$\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x} = \boldsymbol{a}^{\mathrm{T}}\boldsymbol{p} + \boldsymbol{a}^{\mathrm{T}} \begin{bmatrix} \boldsymbol{T} \\ \boldsymbol{I}_k \end{bmatrix} \boldsymbol{z} = \boldsymbol{a}^{\mathrm{T}} p + h\boldsymbol{g}^{\mathrm{T}}\boldsymbol{z} = \boldsymbol{a}^{\mathrm{T}} p + hh^{-1}(u - \boldsymbol{a}^{\mathrm{T}}\boldsymbol{p}) = u。$$

2　基于非球形高斯的原像采样[14]

Jia 等[14]为了进一步减小原像采样算法中原像的尺寸,以及提高算法的安全性,提出了一种基于非球形高斯分布的原像采样方法。

在球形高斯上的原像采样上,最终输出的原像服从分布 $D_{\Lambda_q^{\perp}(\boldsymbol{a}),s,u}$,而在非球形高斯采样中,原像则服从新的分布,新的协方差矩阵:$\boldsymbol{\Sigma} = \tilde{s}^2 \boldsymbol{I}_2 \oplus \tilde{s}^2 \boldsymbol{I}_k$,这种原像服从的分布是不会泄露陷门 T 的信息的[14]。

扰动向量 $\boldsymbol{p}$ 服从的协方差矩阵为

$$\boldsymbol{\Sigma}_p = \sum - \sigma^2 \begin{bmatrix} \boldsymbol{T} \\ \boldsymbol{I}_{k-l} \end{bmatrix} [\boldsymbol{T}^{\mathrm{T}} \quad \boldsymbol{I}_{k-l}] = \begin{bmatrix} \tilde{s}^2 \boldsymbol{I}_2 - \sigma^2 \boldsymbol{T}\boldsymbol{T}^{\mathrm{T}} & -\sigma^2 \boldsymbol{T} \\ -\sigma^2 \boldsymbol{T}^{\mathrm{T}} & (\tilde{s}^2 - \sigma^2)\boldsymbol{I}_k \end{bmatrix} \tag{1}$$

根据引理 2,不考虑关于 n 的可忽略概率,原像的 l_2 范数下界为

$$\sqrt{\bar{s}^2 \cdot 2n + \tilde{s}^2 kn} \tag{2}$$

根据引理 3,原像的存储尺寸的下界为

$$2n(1 + \lceil \log \bar{s} \rceil) + kn(1 + \lceil \log \tilde{s} \rceil) \approx 2n(1 + \log \bar{s}) + kn(1 + \log \tilde{s}) \tag{3}$$

为了保证原像采样算法的正确性,需要满足[14]:$\boldsymbol{\Sigma}_p - \frac{5}{4} \begin{bmatrix} \boldsymbol{T} \\ \boldsymbol{I}_{k-l} \end{bmatrix} [\boldsymbol{T}^{\mathrm{T}} \quad \boldsymbol{I}_{k-l}]$是正定矩阵,通过证明,他们确定了 $\bar{s}^2 = \frac{\tilde{s}'\sigma' \mathrm{s}_1(\boldsymbol{T})}{\sqrt{\tilde{s}^2 - \sigma'^2}}, \sigma'^2 = \sigma^2 + \frac{5}{4} r^2$。

上文式(2)决定了算法的安全性,而式(3)决定了原像的存储尺寸,在保证算法的正确性(上文所述)的前提下,基于非球形高斯采样的原像采样算法提出了 2 种模式[14]:①模式 1 为了提高安全性,使式(2)最小,通过计算取 $\bar{s}^2 = (1 + \frac{1}{\mathrm{s}_1(\boldsymbol{T})}\sqrt{\frac{k}{2}}) \cdot (\mathrm{s}_1(\boldsymbol{T}))^2 \cdot \sigma'^2$ 以及 $\tilde{s}^2 = (1 + \mathrm{s}_1(\boldsymbol{T}) \cdot \sqrt{\frac{2}{k}}) \cdot \sigma'^2$;②模式 2 为了最大化降低原像的尺寸,使式(3)最小,通过计算取 $\bar{s}^2 = (1 + \frac{k}{2}) \cdot (\mathrm{s}_1(\boldsymbol{T}))^2 \cdot \sigma'^2$ 以及 $\hat{s}^2 = (1 + \frac{2}{k}) \cdot \sigma'^2$。

下面给出基于非球型高斯的原像采样算法[14],用 NS-SamplePre、TrapGen、NS-GM-SampleP、GM-SamplePolyG 分别表示运用非球面高斯采样原理的原像采样算法、陷门生成算法、扰动采样算法以及 $\boldsymbol{g}$-格采样算法(以下所表示的矩阵都是由块矩阵组成的)。

首先,TrapGen 算法[10]生成陷门 $\boldsymbol{T}$ 和用户公钥向量 $\boldsymbol{a}, \boldsymbol{T} \leftarrow D_{R^{2\times k},\tau}, \boldsymbol{a} = [\bar{\boldsymbol{a}} \mid h\boldsymbol{g}^{\mathrm{T}} - \bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$,如下:

算法 2.1[10] TrapGen($q, \tau, \bar{\boldsymbol{a}}, h$)

输入:环模 q,高斯参数 τ, $\bar{\boldsymbol{a}} \in R_q^{m-k}$ 和标签 $h \in R_q$,若没有 $\bar{\boldsymbol{a}}$ 和 h,则执行第(1)步,

输出:陷门 $\boldsymbol{T} \in R_q^{(m-k)\times k}$ 和公钥向量 $\boldsymbol{a} \in R_q^m$

(1) $\hat{\boldsymbol{a}} \leftarrow U(R_q^{m-k-1})$, $\bar{\boldsymbol{a}} = (1, \hat{\boldsymbol{a}}) \in R_q^{1\times(m-k)}$, $h = 1$,

(2) $\boldsymbol{T} \leftarrow D_{R_q^{(m-k)\times k},\tau}$, $\boldsymbol{a} = [\bar{\boldsymbol{a}} \mid h\boldsymbol{g}^{\mathrm{T}} - \bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$,

返回:$(\boldsymbol{a}, \boldsymbol{T})$

然后基于非球面高斯原理[14]进行原像采样,如算法 2.2:

算法 2.2[14] NS-SamplePre($\boldsymbol{T}, \boldsymbol{a}, \sigma, \bar{s}, \tilde{s}, h, u$)

输入:公钥向量 $\boldsymbol{a} \in R_q^m$,陷门 $\boldsymbol{R} \in \boldsymbol{T}^{2\times k}$,可逆元素 $h \in R_q$,目标 $u \in R_q$,高斯参数 $\sigma, \bar{s}, \tilde{s}$,

输出:短的原像 $\boldsymbol{x} \in R^m$,服从参数 $\bar{s}, \tilde{s}$ 的非球形高斯分布,其协方差矩阵为 $\boldsymbol{\Sigma} = \bar{s}^2 \boldsymbol{I}_2 \oplus \tilde{s}^2 \boldsymbol{I}_{k-l}$,

(1)采样 $\boldsymbol{p} \leftarrow$ NS-GM-SampleP($q, \sigma, \bar{s}, \tilde{s}, \boldsymbol{T}$),

(2)计算 $v = h^{-1}(u - \boldsymbol{a}\boldsymbol{p})$,

(3)采样 $\boldsymbol{z} \leftarrow$ GM-SamplePolyG(σ, v),

(4)计算 $\boldsymbol{x} = \boldsymbol{p} + \begin{bmatrix} \boldsymbol{T} \\ \boldsymbol{I}_k \end{bmatrix} \boldsymbol{z}$,

返回:$\boldsymbol{x} \in R^{2+k-l}$。

其中,算法 NS-GM-SampleP 按照算法 GM-SampleP[12]执

行,但扰动向量 $\boldsymbol{p}$ 服从的协方差矩阵为 $\boldsymbol{\Sigma}_p = \begin{bmatrix} \tilde{s}^2\boldsymbol{I}_2 - \sigma^2\boldsymbol{T}\boldsymbol{T}^{\mathrm{T}} & -\sigma^2\boldsymbol{T} \\ -\sigma^2\boldsymbol{T}^{\mathrm{T}} & (\tilde{s}^2-\sigma^2)\boldsymbol{I}_k \end{bmatrix}$,然后再按照 GM-SampleP[12] 法进行扰动向量的采样;而算法 GM-SamplePolyG[12] 是 $\boldsymbol{g}$ - 格采样算法,输入目标 $v \in R_q$,高斯宽度参数 σ,输出 $\boldsymbol{z} \in R^k$,满足 $\boldsymbol{g}^{\mathrm{T}}\boldsymbol{z} = v$。

3 基于非球形高斯的 IBE 方案

针对 QW 方案的用户私钥尺寸大,本文在理想格上运用基于非球形高斯的原像采样算法[14],对 QW 方案中的用户私钥提取算法做了改进,而加密算法和解密算法不是本文改进的地方,因此,本文不沿用 QW 方案中的压缩技术、解压技术以及不引入明文扩张参数。

3.1 基于非球形高斯的 IBE 方案

本文的 IBE 方案,在 Extract 算法中运用了基于非球形高斯的原像采样算法[14],因此,用 New-Extract 表示;而加密和解密算法,如本文 2.2 所述,因此,便直接用 Encrypt 算法和 Decrypt 算法表示。为方便,设 $m = 2 + k$。本文的 IBE 方案的参数包括:安全参数 λ,多项式的阶 n,环模 q,维数 m 和高斯参数 $\sigma, \bar{s}, \tilde{s}, \tau$。

(1) Setup$(1^{\lambda}) \rightarrow (mpk, msk)$

a. 使用算法 TrapGen$(q, \tau, \bar{\boldsymbol{a}}, h = 0)$ 生成 $\boldsymbol{a} = [\bar{\boldsymbol{a}} \mid -\bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}} \in R_q^m$ 和 $\boldsymbol{T} \in R^{2\times k}$。其中 $\hat{\boldsymbol{a}} \leftarrow U(R_q^1)$,$\bar{\boldsymbol{a}} = (1, \hat{\boldsymbol{a}}) \in R_q^{1\times 2}$,$\boldsymbol{T} \leftarrow D_{R_q^{2\times k}, \tau}$。

b. 生成目标 $u \leftarrow U(R_q)$。

得到 $mpk = (\boldsymbol{a}, u) \in R_q^{m+1}$,$msk = \boldsymbol{T} \in R^{2\times k}$。

(2) New-Extract$(mpk, msk, id) \rightarrow sk_{id}$

a. 利用散列函数计算用户的身份标识 $h_{id} = H(id)$。

b. 计算用户公钥 $\boldsymbol{a}_{id} = \boldsymbol{a}^{\mathrm{T}} + [0 \mid h_{id}\boldsymbol{g}^{\mathrm{T}}]^{\mathrm{T}} = [\bar{\boldsymbol{a}} \mid h_{id}\boldsymbol{g}^{\mathrm{T}} - \bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$。

c. 用算法 NS-SamplePre$(\boldsymbol{T}, \boldsymbol{a}, \sigma, \bar{s}, \tilde{s}, h_{id}, u)$ 采样短的原像 $\boldsymbol{x}$,使得 $\boldsymbol{a}_{id}^{\mathrm{T}}\boldsymbol{x} = u$ 成立,$\boldsymbol{x}$ 服从分布 $D_{R^m, \Sigma}$,其中 $\Sigma = \bar{s}^2\boldsymbol{I}_2 \oplus \tilde{s}^2\boldsymbol{I}_{k-l}$。

得到用户私钥 $sk_{id} = \boldsymbol{x}$。

(3) Encrypt$(mpk, id, M = (m_1, \cdots, m_n) \in R_2) \rightarrow C$。

a. 按照算法 Setup 计算 $\boldsymbol{a}_{id}$。

b. 采样 R-LWE 的秘密 $s \leftarrow U(R_q)$ 以及噪声 $\boldsymbol{e} \leftarrow D_{R^m,\alpha}$,$e' \leftarrow D_{R,\alpha}$。

c. 计算辅助密文 $\boldsymbol{b} = \boldsymbol{a}_{id}s + \boldsymbol{e}$,然后计算密文块:$c = us + e' + \lfloor q/2 \rfloor \cdot M$。

得到密文组$(\boldsymbol{b}, c)$,其中 $\boldsymbol{b} \in R_q^m$,$c \in R_q$,完成加密。

(4) QW-Decrypt$(sk_{id}, (\boldsymbol{b}, c)) \rightarrow res = (res_1, \cdots, res_n)$

对密文块解密:$res = c' - \boldsymbol{b'}^{\mathrm{T}}\boldsymbol{x}$,$res \in R_q$ 为明文块,设 res 的系数嵌入为 res_i,若 res_i 与 0 的距离小于与$\lfloor q/2 \rfloor$的距离,则 $res_i = 0$,否则 $res_i = 1$。

最后得到明文块 $res = (res_1, \cdots, res_n)$,完成解密。

3.2 方案的正确性分析与误差分析

经过 Encrypt 算法以及 Decrypt 算法的计算后存在误差,因此,本方案的正确性是由误差的 l_2 范数上界不能超过一定的范围来保证的[10],Decrypt 算法解得的密文 $res = c - \boldsymbol{b}^{\mathrm{T}}\boldsymbol{x}$,与$\lfloor q/2 \rfloor \cdot M$ 相比发现存在误差 $\varepsilon = e' - (\boldsymbol{e}^{\mathrm{T}})\boldsymbol{x}$。只要保证该误差的 l_2 范数的上界 $\|\varepsilon\|$不超过$\lfloor q/4 \rfloor$,即要求 $\|\varepsilon\| < \lfloor q/4 \rfloor$,便可以保证本方案加解密的正确性。

由上文可知,误差为 $\varepsilon = e' - (\boldsymbol{e}^{\mathrm{T}})\boldsymbol{x}_i$,且由本方案的信息可知 $e' \leftarrow D_{R,\alpha}$,$\boldsymbol{e} \leftarrow D_{R^m,\alpha}$以及 $\boldsymbol{x}$ 服从分布 $D_{R^m,\Sigma}$,其中 $\Sigma = \bar{s}^2\boldsymbol{I}_2 \oplus \tilde{s}^2\boldsymbol{I}_k$;此时,$(\boldsymbol{e}^{\mathrm{T}})\boldsymbol{x}$ 的每一个系数服从以 0 为中心,标准差为 $2\alpha\bar{s} + k\alpha\tilde{s}$ 的高斯分布,因此,$\varepsilon = e' - (\boldsymbol{e}^{\mathrm{T}})\boldsymbol{x}$ 则服从以 0 为中心,标准差为 $2\alpha\bar{s} + k\alpha\tilde{s} + \alpha$ 的分布。要保证本方案解密的正确性,根据 $\|\varepsilon\| < \lfloor q/4 \rfloor$得:

$$(2\alpha\bar{s} + k\alpha\tilde{s} + \alpha)t\sqrt{n} < \lfloor q/4 \rfloor \tag{4}$$

其中 t 为高斯函数的尾切参数[10]。

3.3 方案的安全性分析

为了证明本文的 IBE 方案是 IND-sID-CPA 的,采用安全游戏序列的方法,需要攻击者 A 和具备 IND-sID-CPA 能力的挑战者 B 进行 4 轮安全游戏,而在最后一轮游戏中,攻击者 A 很难从密文块中得到明文信息[13],最后一轮攻击者的优势为 0,因此,本部分只考虑前三轮游戏,然后计算攻击者 A 拥有的优势,从而证明本文的 IBE 方案是 IND-sID-CPA 的。

在第一轮游戏中,IBE 方案的 New-Setup 算法生成 mpk 为 $\boldsymbol{a} = [\bar{\boldsymbol{a}} \mid -\bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$ 以及目标 $u \in R_q$,都是均匀随机的,此时攻击者 A 的优势为 0。

在第二轮游戏中,攻击者 A 选择一个意欲挑战的身份 id^*,并发出关于身份 id 秘钥的询问。首先,挑战者 B 需要利用算法 TrapGen$(q, \tau, \bar{\boldsymbol{a}}, h = -h_{id^*})$ 计算得出 $\boldsymbol{a} = [\bar{\boldsymbol{a}}^{\mathrm{T}} \mid -h_{id}\boldsymbol{g}^{\mathrm{T}} - \bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$,并将 $mpk = (\boldsymbol{a}, \boldsymbol{u}) \in R_q^{m+r}$ 发送给攻击者 A。然后,如果 $id \neq id^*$,此时 $\mathrm{a}_{id} = [\bar{\boldsymbol{a}}^{\mathrm{T}} \mid (h_{id} - h_{id^*})\boldsymbol{g}^{\mathrm{T}} - \bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$,则挑战者 B 需要利用算法 NS-SamplePre$(\mathbf{R}, \boldsymbol{a}, \sigma, \bar{s}, \tilde{s}, h_{id} - h_{id^*}, u)$ 计算出关于身份 id 的私钥 $\boldsymbol{x}$,满足 $\boldsymbol{a}_{id}^{\mathrm{T}}\boldsymbol{x} = u$,并将 $\boldsymbol{x}$ 发送给攻击者 A;如果 $id =$

id^*,此时 $\boldsymbol{a}_{id}=[\bar{\boldsymbol{a}}^{\mathrm{T}}\mid -\bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$,无需回复攻击者 A 发出的关于私钥的询问。由于 $\boldsymbol{a}=[\bar{\boldsymbol{a}}^{\mathrm{T}}\mid -h_{id}\boldsymbol{g}^{\mathrm{T}}-\bar{\boldsymbol{a}}^{\mathrm{T}}\boldsymbol{T}]^{\mathrm{T}}$ 与 $U(R_q^m)$ 在统计上是不可区分的,攻击者 B 无法得到陷门 $\boldsymbol{T}$,因此,求解关于身份 id 的秘钥是困难的。此轮游戏,攻击者 A 至多只有求解 $R-\mathrm{ISIS}_{q,\beta,m}$ 问题的优势,而且非球形高斯采样的原理说明原像 sk_{id} 的 l_2 范数更加小,因此,求解本方案的 $R-\mathrm{ISIS}_{q,\beta,m}$ 问题难度更大,攻击者在此轮游戏的优势更加小。

在第三轮游戏中,攻击者 A 选择 2 段明文 $M_0,M_1\in R_2$,发送给挑战者 B,挑战者 B 选择 $b_0\in\{0,1\}$,并对 M_{b_0} 按照 Encrypt 算法进行加密,得到挑战密文组$(\boldsymbol{b}^*,c^*)$,并发送给挑战者 A。挑战者要么区分挑战密文组是来自以下的哪种分布:①$\boldsymbol{b}^*=\boldsymbol{a}_{id}^{\mathrm{T}}s+\boldsymbol{e}\in R_q^m$ 以及 $c^*=us+e'\lfloor q/2\rfloor\cdot M_{b_0}\in R_q$;②$R_q^m\times R_q$ 上的均匀随机分布,要么猜测以 1/2 的概率猜测挑战密文组是通过加密 M_0 还是通过加密 M_1 而得。由于 Decision R-LWE 问题的困难性,要区分以上 2 种分布是很困难的,与求解秘密 s 的困难性是等价的,因此,在这轮游戏中攻击者 A 的优势至多只有求解 Decison $R-\mathrm{LWE}_{q,\chi,\omega}$ 问题的优势。

综合以上 3 轮安全游戏,由于本方案的设计是基于 $R-\mathrm{ISIS}_{q,\beta,\omega}$ 问题 Decison $R-\mathrm{LWE}_{q,\chi,\omega}$ 问题的困难性,攻击者 A 具有的优势:$\mathrm{Adv}_{\mathrm{IBE}}^{\text{IND-sID-CPA}}(\mathrm{A})\leqslant\mathrm{Adv}_{q,\beta,m}^{R-\mathrm{ISIS}}(\mathrm{A})+\mathrm{Adv}_{q,\chi,m}^{\text{Decison }R-\mathrm{LWE}}(\mathrm{A})+negl(\lambda)$,可见攻击者 A 优势是可忽略的,因此本方案是 IND-sID-CPA 的。

4　方案的结果与分析

本文的 IBE 方案,运用了基于非球形高斯[14]的原像采样算法对用户私钥采样算法做了改进,相比于 QW 方案,用户私钥的尺寸减小了,提升了方案空间效率。本文的 IBE 方案有以下参数;多项式的阶 n;环模 $q,b,k=\lceil\log_b q\rceil$;多项式向量的维数 $m=2+k$;$\boldsymbol{g}$-格采样的高斯参数取 $\sigma=\sqrt{b^2+1}\cdot r$;陷门 $\boldsymbol{T}$ 的标准差 τ;用户私钥 $\boldsymbol{x}$ 服从非球形高斯分布的参数 $\bar{s}$、$\tilde{s}$,以及噪声的高斯参数 α。根据 3.2 的分析,要保证 IBE 方案加解密正确性,即使得 $\varepsilon=e'-(\boldsymbol{e}^{\mathrm{T}})\boldsymbol{x}<\lfloor q/4\rfloor$ 成立,因此,相关参数需要满足式(4)。根据 QW 方案[13],取高斯函数的尾切参数 $t=8$。

本方案运用了基于非球形高斯的原像采样原理后,其中模式 2 可以减小用户私钥 $\boldsymbol{x}$ 的尺寸,模式 1 可以减小用户私钥 $\boldsymbol{x}$ 的 l_2 范数的上界,同时也可以降低用户私钥的尺寸。表 1 为 2 种方案在用户私钥 $\boldsymbol{x}$ 的尺寸以及用户私钥 $\boldsymbol{x}$ 的 l_2 范数上界的对比。

表 1　用户私钥尺寸和范数上界的对比

Table 1　Comparison of the upper bound of the norm and size of the user's private key

用户私钥	文献[13]	本研究
sk_{id} 尺寸	$nm(1+\log\xi)$	$2n(1+\log\bar{s})+nk(1+\log\tilde{s})]$
$\|\boldsymbol{x}\|$	$\xi\sqrt{nm}$	$\sqrt{\bar{s}^2\cdot 2n+\tilde{s}^2kn}$

以下是对用户私钥 $\boldsymbol{x}$ 服从的非球形高斯分布的两个参数 $\bar{s},\tilde{s}$ 的取值进行说明:

模式 1 最大化提高安全性,使 $\|\boldsymbol{x}_i\|$ 最小化,在保证原像采样算法的正确性的情况下,通过计算得 $\bar{s}^2=(1+\frac{1}{\mathrm{s}_1(\boldsymbol{T})}\sqrt{\frac{k}{2}})\cdot(\mathrm{s}_1(\boldsymbol{T}))^2\cdot\sigma'^2$,$\tilde{s}^2=(1+\mathrm{s}_1(\boldsymbol{T})\cdot\frac{k}{2})\cdot\sigma'^2$;模式 2 为了最大化降低原像 $\boldsymbol{x}$ 的尺寸,使 $2n(1+\log\bar{s})+kn(1+\log\tilde{s})$ 最小,且在保证原像采样算法的正确性下,通过计算得 $\bar{s}^2=(1+\frac{k}{2})\cdot(\mathrm{s}_1(\boldsymbol{T}))^2\cdot\sigma'^2$ 以及 $\tilde{s}^2=(1+\frac{2}{k})\cdot\sigma'^2$。其中,以上 2 种模式中 σ'^2 的取值为 $\sigma^2+\frac{5}{4}r^2$。

本文采用 BKZ 算法[14]来评估本方案的安全性,第一种是评估求解 R-ISIS 问题的困难性,即 ISIS 问题的安全性,第二种是评估公钥的随机性,即评估 LWE 问题的安全性[14]。LWE 问题的安全性由参数 n,q 和陷门 T 的标准差 τ 决定;而 ISIS 问题的安全性则由原像 $\|x_i\|$ 的上界 β 决定。BKZ 算法是通过估计 SVP Oracle 的时间复杂度来评估安全性的,在问题 $\mathrm{ISIS}_{n,q,\beta,m}$ 中,求解一个向量,其 l_2 范数为 $2^{2\cdot\sqrt{n\log q\log\delta_0}}$,因此,令 $\beta=\sqrt{\bar{s}^2\cdot 2n+\tilde{s}^2kn}=2^{2\cdot\sqrt{n\log q\log\delta_0}}$,求解 δ_0,再根据 $\delta_0\approx(\frac{\kappa}{2\pi e}(\pi\kappa)^{\frac{1}{\kappa}})^{\frac{1}{2(\kappa-1)}}$ 求 κ,最后计算 $2^{0.292\kappa}$ 的值,就是 SVP Oracle 的时间复杂度。

通过以上分析,本文将在 2 种模式下与 QW 方案比较,计算用户私钥 sk_{id} 的尺寸(以 kB 为单位),以及评估 ISIS 问题的安全性和 LWE 问题的安全性。

5　结　论

本文运用基于非球形高斯的原像采样算法[14],对 QW 方案的私钥提取算法进行了改进,在保证 IBE 的正确性的情况下,降低其私钥 sk_{id} 的尺寸,以及提升了 ISIS

问题的安全性,但未能提升方案的安全性。

本研究未能提升方案的安全性,是因为需要保证IBE方案加解密的正确性,即相关参数需要满足$(2\alpha\bar{s}+k\alpha\tilde{s}+\alpha)t\sqrt{n}<\lfloor q/4\rfloor$成立,而又因为主私钥$\boldsymbol{T}$的标准差$\tau$和噪声$e$,$e$的高斯参数$\alpha$需要保持相等一致才能保证解密的低出错率,受环模$q$和$n$的取值的影响,高斯参数$\alpha$取值较小,$\tau$也较小,主私钥$\boldsymbol{T}$的系数嵌入比较大的概率在中心点0附近取得,因此,用户公钥$\boldsymbol{a}_{id}$的随机性较小;当τ较小时,$\|\boldsymbol{x}\|$也较小。由以上分析可得,与ISIS问题的安全性相比,LWE问题的安全性低,因此,本文基于非球形高斯采样的IBE方案,虽然可以提升ISIS的安全性,但仍无法在实际意义上提升方案的安全性。如何提升理想格上IBE方案的安全性将是我们后续研究的工作。

但本研究的贡献在于有效降低了用户私钥的尺寸,提升了方案的空间效率。由表2所示,本方案的模式1中,在42.6-bit的安全性下,用户私钥的尺寸由21.75 kB减小至13.31 kB,ISIS问题的安全性由127.9-bit提升至172.8-bit;在109.8-bit的安全性下,用户私钥的尺寸由50.36 kB减小至32.25 kB,ISIS问题的安全性由286.7-bit提升至373.8-bit,虽然模式1可以提高ISIS问题的安全性,但由于LWE问题的安全性相对较低,因此,无法提升方案的安全性。本方案的模式2在ISIS问题的安全性几乎一样的情况下可以更有效地降低用户私钥sk_{id}的尺寸,在42.6-bit的安全性下,用户私钥的尺寸由21.75 kB减小至10.18 kB;在109.8-bit的安全性下,用户私钥的尺寸由50.36 kB减小至21.86 kB,节省了大约60%的内存空间,相比于模式1,模式2能更有效地节省用户私钥的内存开销。综合表2可得,本方案的用户私钥可以节省大约40% ~60%的内存空间。

表2 QW方案[13]与本方案在用户私钥尺寸与安全性上的对比

Table 2 Comparison of the secret key size and security

参数	$n=512,b=2,k=\lceil\log q\rceil=27,\tau=3.3,\alpha=3.3$			$n=1024,b=2,k=\lceil\log q\rceil=29,\tau=5,\alpha=3.3$		
	文献[13]	模式1	模式2	文献[13]	模式1	模式2
$\bar{s}$	1 118.68	15 624.98	58 409.37	2 339.82	2 631.19	10 299.20
$\tilde{s}$		186.28	8.30		74.57	8.27
$\|\boldsymbol{x}\|$	136 314.39	40 963.89	141 407.24	416 882.40	119 765.25	426 090.87
sk_{id}	21.75	**13.31**	**10.18**	50.375	**32.25**	**21.875**
ISIS	127.90	172.86	126.98	286.74	373.76	284.32
LWE	42.63	42.63	42.63	109.79	109.79	109.79

注:τ是陷门$\boldsymbol{T}$的标准差,$\bar{s}$和$\tilde{s}$是用户私钥sk_{id}服从的高斯参数,sk_{id}的尺寸单位是kB,$\|\boldsymbol{x}\|$是sk_{id}的l_2范数上界,ISIS和LWE表示ISIS问题的安全性和LWE问题的安全性

综上所述,本研究运用了基于非球形高斯的原像采样算法[14],对QW方案的私钥提取算法进行了改进,本方案的2种模式均可有效地减少用户私钥的内存开销。虽然无法提升IBE方案的安全性,但实验结果表明,模式1可以提升ISIS的安全性,并且减小了用户私钥的尺寸;模式2在ISIS安全性几乎一样的情况下,能更有效地节省用户私钥的内存开销。

参考文献:

[1] Shamir A. Identity-based cryptosystems and signature schemes[C]//Proceedings of CRYPTO 1984. Berlin:Springer,1984:47-53.

[2] Boneh D,Franlin M. Identity-Based encryption from the weil pairing[C]//Proceedings of CRYPTO 2001. Berlin:Springer,2001:213-220.

[3] Ajtai M. Generating hard instances of lattices problems[C]//Proceedings of STOC. New York: ACM,1996:99-108.

[4] Regev O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM,2009,56(6):1-40.

[5] Micciancio D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions[J]. Computations Complexity,2007,16(4):365-411.

[6] Stehle D, Steinfleld R, Tanaka K, et al. Efficient public key encryption based on ideal lattices[C]//Proceedings of AI-

SACRYPT. Berlin:Springer,2009:617-635.

[7] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]//Proceedings of the 40th ACM Symp on Theory of Computing. New York:ACM,2008:197-206.

[8] Agrawal S, Boneh D, Boyen X. Efficient lattice (H)IBE in the standard model[C]//Proceedings of EUROCRYPT 2010. Berlin:Springer,2010:553-572.

[9] Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices[C]//Proceedings of ASIACRYPT 2014. Berlin:Springer,2014:22-41.

[10] Bert P, Fouqaue P, Roux A, et al. Practical implementation of ring-SIS/LWE based signature and IBE[C]//Proceedings of PQCrypto. Cham:Springer,2018:271-291.

[11] Micciancio D, Peikert C. Trapdoors for Lattices: Simpler, tighter, faster, smaller[C]//Proceedings of EUROCRYPT 2012. Berlin: Springer,2012:700-718.

[12] Genise N, Micciancio D. Faster Gaussian sampling for trapdoor lattices with arbitrary modulus[C]//Proceedings of EUROCRYPT. Cham: Springer,2018:174-203.

[13] 钱心缘,吴文渊. 基于 R-SIS 和 R-LWE 构建的 IBE 加密方案[J]. 计算机科学,2021,48(6):315-323.

[14] Jia H, Hu Y, Tang C. Lattice-based hash-and-sign signatures using approximate trapdoor, revisited[J]. IET Information Security,2021,16(1):41-50.

[15] Regev O. Lecture 1 introduction[EB/OL]. (2004-11-01)[2022-09-15]. https://cims.nyu.edu/~regev/teaching/lattices_fall_2004/ln/introduction.pdf.

[16] Micciancio D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions[J]. Computational Complexity,2007,16(4):365-411.

[17] Lyubashevsky V, Micciancio D, Peikert C, et al. A modest proposal for FFT hashing[C]//Proceedings of FSE. Berlin: Springer,2008:54-72.

[18] Chen Y, Genise N, Mukherjee P. Approximate trapdoors for lattices and smaller hash-and-sign signatures[C]//Proceedings of ASIACRYPT. Berlin:Springer,2019:3-32.

[19] Peikert C. An efficient and parallel Gaussian sampler for lattices[C]//Proceedings of CRYPTO 2010. Berlin: Springer, 2010:80-97.

[20] Peikert C, Rosen A. Efficient collision-resistant hashing from worst case assumptions on cyclic lattices[C]//Proceedings of TCC. Berlin: Springer,2016:145-166.

[21] Stehl'e D, Steinfleld R, Tanaka K, et al. Efficient public key encryption based on ideal lattices[C]//Proceedings of AISACRYPT. Berlin: Springer,2009:617-635.

[22] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer,2010:1-23.

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

[24] Bansarkhani R E, Buchmann J A. Improvement and efficient implementation of a lattice-based signature scheme[C]//Proceedings of SAC 2013. Berlin: Springer,2013:48-67.

[25] Lyubashevsky V, Peikert C, Regev O. A toolkit for ring-LWE cryptography[C]//Proceedings of EUROCRYPT 2013. Berlin: Springer,2013:35-41.

【责任编辑:孙向荣】