文章编号:1671-4229(2024)03-0015-11

格上可撤销的基于身份的加密算法研究

巫俊强，唐春明*，贾惠文
(广州大学 数学与信息科学学院，广东 广州　510006)

摘　要：格上可撤销的基于身份的加密算法(RIBE)不仅能有效地解决实际生活中用户密钥撤销或更新的问题,还能抵抗量子算法攻击,吸引了众多密码学研究者的兴趣。文章通过运用基于近似陷门的非球面高斯采样技术,对 RIBE 方案中的系统公钥、用户私钥和更新密钥等生成算法进行改进,以缩减密钥尺寸,从而提高方案的空间效率。文章通过对同一水平下的解密错误率与原方案进行比较,可以观察到本方案的主公钥、主私钥、用户私钥、更新密钥和解密密钥的存储空间相较于原方案得到了一定的缩减。特别地,对于不同的安全级别,在保持同一解密错误率前提下,该方案的 MPK 尺寸缩减了 32.29% ~41.93%,MSK 尺寸缩减了 31.25% ~38.70%,用户私钥及解密密钥尺寸缩减了 59.13% ~69.95%,密文尺寸缩减了 32.27% ~41.91%。

关键词：格密码；RIBE；非球面高斯采样
中图分类号：TP309.7　　**文献标志码**：A

Research on revocable identity-based encryption algorithm on lattice

WU Jun-qiang, *TANG Chun-ming**, *JIA Hui-wen*
(College of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China)

Abstract: The lattice revocable identity-based encryption algorithm (RIBE) can not only effectively solve the problem of revoking or renewing a user key in real life, but it also resists quantum algorithm attacks, which has attracted the interest of many cryptography researchers. In this paper, the generation algorithms such as system public key, user private key and renewal key in the RIBE scheme are improved by using the aspherical Gaussian sampling technique based on approximate trapdoor. The key size is reduced to improve the spatial efficiency of the scheme. By comparing the decryption error rate with the original system at the same level, it was observed that the storage space of the main public keys, master private keys, user private keys, update keys and decryption keys of this system was reduced to a certain extent compared with the original system. In particular, for different security levels, under the premise of maintaining the same decryption error rate, the size of MPK of this scheme was reduced by 32.29% to 41.93%, the size of MSK reduced by 31.25% to 38.70%, the size of user private key and decryption key reduced by 59.13% to 69.95%, and the size of ciphertext reduced by 32.27% to 41.91%.

Key words: cell code; RIBE; gaussian sampling of aspheric surface

收稿日期：2023－09－18；**修回日期**：2024－01－04
项目基金：国家重点研发计划资助项目(2021YFB3100200)；国家自然科学基金资助项目(12171114)
作者简介：巫俊强(1997—)，男，硕士研究生. E-mail:1837236800@qq.com
* 通信作者. E-mail:ctang@gzhu.edu.cn
引文格式：巫俊强，唐春明，贾惠文. 格上可撤销的基于身份的加密算法研究[J]. 广州大学学报(自然科学版),2024,23(3):15-25.

基于身份的加密(Identity-Based Encryption, IBE)是保障信息安全的重要手段之一,是公钥加密(Public Key Encryption, PKE)的一种高级形式,由 Shamir[1]在1984年提出。与传统的PKE相反,主公钥MPK可用为任意用户加密明文。在2001年,Boneh等[2]基于双线性Diffie-Hellman假设,提出了第一个有效的IBE方案。随后,许多基于身份的加密和签名方案相继被提出[3-5]。

在实际应用中,用户的身份信息因某些原因需要从系统中撤销,如用户丢失了私钥或者不再是合法用户,则用户的私钥需要被撤销或者更新为新密钥。但是由于没有公开密钥基础设施(Public Key Infrastructure, PKI),与传统的PKE相比,IBE系统没有一种简单的方法来动态撤销恶意用户。随后,文献[2]中提出了一个简单的解决方案,即IBE系统的密钥生成中心KGC(Key Generation Center)在每个时间段T给每个未被撤销的用户ID发送一个身份的秘密密钥,只有被撤销的用户才会失去解密能力。不幸的是,该解决方案效率很低,因为当有大量用户参与系统,KGC必须在每个时间段发送许多密钥。在2008年,Boldyreva等[6]提出了一种实现有效撤销的新的解决方案,称为可撤销的基于身份的加密算法(Revocable Identity Based Encryption, RIBE),使得密钥更新的大小是系统用户数量的对数,这大大减轻了可信中心的负担,并且首次实现了非交互的密钥撤销,方案的效率也大大提高。随后,有关可撤销的IBE方案被陆续提出[7-9]。

1997年,Shor[10]证明了在量子攻击下,大整数素数分解和离散对数等问题都将在多项式时间内解决。这表明许多经典加密方案在未来将无法提供量子安全保障。因此,大量学者涌入了后量子密码研究领域。格密码作为后量子密码的经典类型之一,相比其他后量子密码而言有其独特的优势。

2012年,Chen等[11]构造出第一个基于格的RIBE方案,但是他们仅获得选择性安全。随后,一系列基于格的RIBE方案相继被提出。2019年,Ma等[12]以及Wang等[13]首次满足了自适应安全,其中,前者在随机预言机模型下和量子随机预言机模型下实现了适应性安全,但不具备匿名性,后者虽然满足匿名性,但在量子随机模型下无法满足适应性和安全性。令N为RIBE系统中的最大用户数,Wang等的RIBE方案密钥由$\log N$个底层为Agrawal等[14]的IBE方案密钥组成。因此,Wang等的RIBE方案存在大密钥问题。令k_{ID}为身份的长度,Ma等的RIBE方案的密文由$(k_{ID}+1)$个GPV密文组成[15],可见,Ma等的RIBE方案也存在较大的密文。2020年,Takayasu[16]基于Ma等[12]的方案基础上进一步改进,提出了新的方案,其在量子随机模型中实现了自适应安全,也满足匿名性,并且方案的密钥大小和密文大小与GPV IBE几乎相同,但是该方案主要是基于Micciancio等[17]提出的原像采样算法进行密钥的提取,用户密钥的内存开销仍然很大,空间效率利用低,实用性不太强。

2022年,为了近一步改进原像采样算法的安全性和签名尺寸,Jia等[18]提出了基于非球面高斯分布的JHT22原像采用算法,将原像采样算法中的离散球形高斯分布变为非球形高斯分布,且不泄露陷门的任何信息。由于签名和具体安全性与采样算法的高斯参数密切相关,上述技术提供了两者之间的折中,给出了针对不同情况下的两种模式,模式一主要为了提高算法的安全性,并缩减密钥尺寸;模式二主要为了缩减密钥的尺寸,但其安全性会比模式一要差。因此,考虑到方案[16]在系统公钥与用户私钥的存储方面的不足之处,本文利用基于近似陷门的非球面高斯分布技术[18]存在对系统公钥、用户私钥和更新密钥的生成算法进行改进,以提升格上RIBE方案的空间效率。

1 预备知识

1.1 格与高斯分布

定义1(格) 令$\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$是$n$个线性无关的$m$维向量。则由$\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$生成的$m$维格定义为$\Lambda=\{\boldsymbol{b}_1\boldsymbol{x}_1+\boldsymbol{b}_2\boldsymbol{x}_2+\cdots+\boldsymbol{b}_n\boldsymbol{x}_n \mid \boldsymbol{x}\in\mathbb{Z}\}$,即格是由一组线性无关向量的所有整数线性组合构成的向量全体。称$\boldsymbol{B}=[\boldsymbol{b}_1\mid\boldsymbol{b}_2\mid\cdots\mid\boldsymbol{b}_n]$为格$\Lambda$的基矩阵,则格$\Lambda$可表示为$\Lambda=\{\boldsymbol{B}\boldsymbol{x}\mid\boldsymbol{x}\in\mathbb{Z}^n\}$,其秩为$n$,维数为$m$,当$n=m$时,称为满秩格。

给定矩阵$\boldsymbol{A}\in\boldsymbol{Z}_q^{n\times m}$,可以定义如下$m$维格:

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

给定向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$,可以定义如下 m 维格:

$\Lambda_u^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^n \mid \boldsymbol{A}\boldsymbol{x}=\boldsymbol{u} \bmod q\}$。

定义 2(多项式环[19]) 设 n 为一个正整数,$q>0$,$\Phi(x)$ 为$\mathbb{Q}$上的不可约多项式,定义$\mathbb{R}=\mathbb{Z}[x]/\Phi(x)$为模 $\Phi(x)$ 的剩余类整系数多项式环,$\mathbb{R}_q=\mathbb{Z}_q[x]/\Phi(x)$ 为$\mathbb{Z}_q$上的剩余类整系数多项式环。本文的多项式环选定为$\mathbb{R}_q=\mathbb{Z}_q[x]/(x^n+1)$,其中,$n$ 为 2 的幂次方。

定义 3(多项式的系数嵌入,多项式相乘[19])

设$\mathbb{R}$为定义 2 中的 n 维多项式环,令 $h(x)\in\mathbb{R}$,则多项式的系数嵌入定义为一个多项式环到整数向量的映射:$h(x)\mapsto\boldsymbol{h}=(x_0,\cdots,x_{n-1})\in\mathbb{Z}^n$,上述映射建立了环与 n 维整数向量空间$\mathbb{Z}^n$之间的联系。

令 $g(x)=\sum_{i=0}^{n-1}g_i x^i\in\mathbb{R}$, 对应的反循环矩阵定义为

$$\varphi(x)=\begin{bmatrix} g_0 & -g_{n-1} & \cdots & -g_1 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-1} & g_{n-2} & \cdots & g_0 \end{bmatrix}\in\mathbb{Z}^{n\times n},$$

而 $\varphi(x)\cdot\boldsymbol{h}$ 为 $h(x)\cdot g(x)$的系数嵌入。特别地,对于 $\alpha\in\mathbb{Z}\subset\mathbb{R}$,有 $\varphi(\alpha)=\alpha\cdot\boldsymbol{I}_n\in\mathbb{Z}^{n\times n}$。

定义 4($Ring-SIS_{q,m,\beta}$问题[20]) 给定一个均匀随机的 $a\in\mathbb{R}^m$,找到一个短的原像 $\boldsymbol{x}\in\mathbb{R}^m$ ($\|a\|\leqslant\beta$),满足 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=0\in\mathbb{R}_q$。

定义 5($R-Approx.\ ISIS_{m,q,\alpha,\beta}$问题[21]) 给定一个 $\boldsymbol{a}\in\mathbb{R}_q^m$,$\boldsymbol{y}\in\mathbb{R}_q$,找到一个短的原像 $\boldsymbol{x}\in\mathbb{R}^m$,满足 $\|\boldsymbol{x}\|\leqslant\boldsymbol{\alpha}$,使得存在一个 $\boldsymbol{z}\in\mathbb{R}$,对于 $\|\boldsymbol{z}\|\leqslant\beta$ 有 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=\boldsymbol{y}+\boldsymbol{z}\pmod q$。

定义 6($R-LWE$ 分布[22]) 定义秘密多项式 $\boldsymbol{s}\in\mathbb{R}_q$,$R-LWE$ 分布 $A_{s,\chi}$的输出形式为($\boldsymbol{a},\boldsymbol{b}=\boldsymbol{s}\times\boldsymbol{a}+\boldsymbol{e}$),其中,$\boldsymbol{a}\leftarrow U(\mathbb{R}_q)$,$\boldsymbol{e}\leftarrow\chi$,χ 是$\mathbb{R}_q$上的错误分布。

定义 7($Decision\ R-LWE_{q,\chi,m}$问题[22]) 给定 m 个独立样本 $(\boldsymbol{a}_i,\boldsymbol{b}_i)\in\mathbb{R}_q\times\mathbb{R}_q$, $Decision\ R\text{-}LWE_{q,\chi,m}$问题需判断样本$(\boldsymbol{a}_i,\boldsymbol{b}_i)$是取自均匀随机多项式还是取自 $R-LWE$ 分布 $A_{s,\chi}$。

定义 8(高斯函数[23]) 对任意的 $\boldsymbol{x},\boldsymbol{c}\in\mathbb{R}^n$以及实数 $s>0$,定义高斯函数$\rho_{s,c}(x)=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|/s^2)$,其中,$c$ 称为高斯函数的中心,s 称为高斯函数的高斯偏差。

定义 9(离散高斯分布[23]) n 维格 Λ 的离散高斯分布 $D_{\Lambda,s,c}$定义为

$D_{\Lambda,s,c}=\rho_{s,c}(\boldsymbol{x})/\sum_{x\in\Lambda}\rho_{s,c}(\boldsymbol{x})=\rho_{s,c}(\boldsymbol{x})/\rho_{s,c}(\Lambda)$。

定义 10(光滑参数[24]) 给定一个 n 维格 Λ 和一个正有理数 $\varepsilon>0$,光滑参数 $\eta_\varepsilon(\Lambda)$定义为使得$\rho_{1/\sigma}(\Lambda^*/\{0\})\leqslant\varepsilon$ 成立的最小正整数 σ,其中,$\Lambda^*=\{y\in span(\boldsymbol{B})\mid\forall\boldsymbol{x}\in\Lambda(\boldsymbol{B}),<\boldsymbol{x},\boldsymbol{y}>\in Z\}$称为格 Λ 的对偶格。

引理 1[15] 设 $\boldsymbol{B}$ 是 m 维格 Λ 的一组基,令 $\varepsilon>0$,则有

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

引理 2[24-25] 设 $\boldsymbol{B}$ 是 m 维格 Λ 的一组基,若 $s\geqslant\eta_\varepsilon(\Lambda)$,则有

$Pr_{x\leftarrow D_{\Lambda,s}}[\|x\|\geqslant s\sqrt{m}]\leqslant negl(m)$。

引理 3[26] 设向量 $\boldsymbol{v}\in\mathbb{Z}^m$满足 $\|\boldsymbol{v}\|\geqslant s\sqrt{m}$,则存储这个向量所需的最大位数不超过 $m\cdot(1+\lceil\log s\rceil)$。

引理 4[15,24] 令 $\sigma>16\sqrt{\log 2m/\pi}$, $\boldsymbol{u}\in\mathbb{Z}_q^n$,$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,$H_\infty(D_{\Lambda_u^{\perp}(\boldsymbol{A}),\sigma})\geqslant m-1$ 大概率成立。

引理 5[27] 设$\mathbb{R}_q$为 n 维多项式环,多项式 $\boldsymbol{x},\boldsymbol{y}\in\mathbb{R}_q$,其中,$\boldsymbol{x}\leftarrow D_{\mathbb{R}_q,\eta}$, $\boldsymbol{y}\leftarrow D_{\mathbb{R}_q,\varepsilon}$且相互独立,令 $\boldsymbol{z}=\boldsymbol{x}\cdot\boldsymbol{y}$,则有 $\boldsymbol{z}\leftarrow D_{\mathbb{R}_q,n\cdot\varepsilon\eta}$。

引理 6[28] q,ϱ,m 是正整数,r 是正实数,满足 $r>\max\{\omega(\sqrt{\log m}),\omega(\sqrt{\log\varrho})\}$,取 $\boldsymbol{b}\in\mathbb{Z}^m$,$\boldsymbol{z}\leftarrow D_{\mathbb{Z}^m,r}$,则存在一个多项式时间算法 ReRand,满足对任意的 $\boldsymbol{V}\in\mathbb{Z}^{m\times\varrho}$,取 $\sigma>\|\boldsymbol{V}\|_2$,有 $ReRand(\boldsymbol{V},\boldsymbol{b}+\boldsymbol{z},r,\sigma)$输出 $\boldsymbol{b}'^{\mathrm{T}}=\boldsymbol{b}^{\mathrm{T}}+\boldsymbol{z}'^{\mathrm{T}}$,其中,$\boldsymbol{z}'$以 $2^{-\Omega(n)}$ 统计接近于 $D_{\mathbb{Z}^\varrho,2r\sigma}$。

引理 7[18] 令 $\sum=\tilde{s}^2\boldsymbol{I}_{2n}\oplus\tilde{s}^2\boldsymbol{I}_{(k-l)n}$,算法 $ApproSamPre(\boldsymbol{A},\boldsymbol{R},\tilde{s},\tilde{s},\cdot)$ 可简记为$\boldsymbol{A}^{-1}(\cdot)$,下面两个分布是统计不可区分的:

$$\{(\boldsymbol{A},\boldsymbol{x},\boldsymbol{u},\boldsymbol{e}):\boldsymbol{u}\leftarrow U(\mathbb{Z}_q^n),\boldsymbol{x}\leftarrow\boldsymbol{A}^{-1}(\boldsymbol{u}),\ \boldsymbol{e}=\boldsymbol{u}-\boldsymbol{A}\boldsymbol{x}(\bmod q)\},$$

$$\{(\boldsymbol{A},\boldsymbol{x},\boldsymbol{u},\boldsymbol{e}):\boldsymbol{x}\leftarrow D_{\mathbb{Z}^m,\sqrt{\Sigma}},\boldsymbol{e}\leftarrow D_{\mathbb{Z}^n,\sigma\sqrt{(b^{2l}-1)/(b^2-1)}},\ \boldsymbol{u}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{e}(\bmod q)\}。$$

1.2　可撤销的基于身份的加密体制

一个标准的 RIBE 方案[29] 主要由 7 个算法构

成(*Setup*、*Enc*、*GenSk*、*KeyUp*、*GenDk*、*Dec* 和 *Rev*)包括相应的身份空间*ID*,明文空间M,时间空间T。

(1)$Setup(1^\lambda)\rightarrow(MPK,MSK)$

给定系统参数λ作为输出,则加密算法输出系统主公钥*MPK*和主私钥*MSK*。

(2)$Enc(MPK,ID,T,M)\rightarrow ct_{ID,T}$

给定主公钥*MPK*,用户身份*ID*,时间T和明文M作为输入,则加密算法生成密文$ct_{ID,T}$。

(3)$GenSk(MPK,MSK,ID)\rightarrow sk_{ID}$

给定主公钥*MPK*,主私钥*MSK*,用户身份*ID*作为输入,则密钥生成算法生成用户的私钥sk_{ID}。

(4)$KeyUp(MPK,MSK,T,RL_T)\rightarrow ku_T$

给定主公钥*MPK*,时间T,主私钥*MSK*以及撤销列表RL_T作为输入,则密钥更新算法输出属于时间T的更新密钥集合ku_T。

(5)$GenDk(MPK,sk_{ID},ku_T)\rightarrow dk_{ID,T}$ 或 $\perp$

给定主公钥*MPK*,用户私钥sk_ID以及更新密钥集合ku_T作为输入,则解密密钥生成算法输出用户的解密密钥$dk_{ID,T}$。如果该用户在时间T被撤销了,则该算法运行失败,输出 $\perp$。

(6)$Dec(MPK,dk_{ID,T},ct_{ID,T})\rightarrow M$

给定主公钥*MPK*,用户解密密钥$dk_{ID,T}$以及密文$ct_{ID,T}$作为输入,则解密算法生成对应的明文M。

(7)$sRev(ID,T,RL_T)\rightarrow RL_T$

给定用户身份*ID*,时间T以及撤销列表RL_T,则解密算法更新撤销列表RL_T。

1.3 近似陷门

为了改进高斯原像采样算法空间效率,2019年,Chen等[21]提出了近似原像采样算法(以下用CGM19算法来表示该算法),将G陷门修改为近似陷门来解决近似ISIS问题,使得在近似陷门中,m的维数减小到接近原陷门的一半,并且随着m的减少高斯参数s也随之减少,从而使得公钥和私钥的尺寸都减小。接下来将对其在环上的版本进行简单的介绍。

Chen等给出了环上的近似ISIS问题($R-ApproxISIS_{m,q,\alpha,\beta}$),即给定一个$\boldsymbol{a}\in\mathbb{R}_q^m,\boldsymbol{y}\in\mathbb{R}_q$,找到一个短的原像$\boldsymbol{x}\in\mathbb{R}^m$,当$\|\boldsymbol{x}\|\leqslant\alpha$时,存在一个$z\in\mathbb{R}$,$\|z\|\leqslant\beta$,有$\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=\boldsymbol{y}+z(\mathrm{mod}q)$,求解$\boldsymbol{x}$是非常困难的,但在存在陷门的情况下,求解$\boldsymbol{x}$是简单可行的。

在环上,近似陷门是由常量多项式构成,定义:

$$\boldsymbol{f}^{\mathrm{T}}=(\boldsymbol{b}^l,\cdots,\boldsymbol{b}^k)\in\mathbb{R}_q^{k-l},$$

其中,$k=\lceil\log_b^q\rceil$,l表示从g-向量删除的低价维数。对应的随机元素$\boldsymbol{a}\in\mathbb{R}_q^m$变为

$$\boldsymbol{a}^{\mathrm{T}}=[(1,\hat{\boldsymbol{a}})\mid\boldsymbol{f}^{\mathrm{T}}-(1,\hat{\boldsymbol{a}})\boldsymbol{R}]\in\mathbb{R}^{1\times(2+k-l)}=\mathbb{R}^m,\ \hat{a}\in U(\mathbb{R}_q),$$

其中,陷门$\boldsymbol{R}\in\mathbb{R}^{k-l}$是由小的多项式组成的矩阵,满足:

$$\boldsymbol{F}=\boldsymbol{I}_n\otimes(\boldsymbol{b}^l,\cdots,\boldsymbol{b}^{k-1})=\boldsymbol{a}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{R}\\ \boldsymbol{I}_{k-l}\end{bmatrix},\ \boldsymbol{R}\leftarrow D_{\mathbb{R}^{2\times(k-l)},\tau}。$$

采用近似陷门的原像采样算法和MP12算法几乎相同,除了在第二步的G-lattice采样中原像的前l个分量会被删除。具体采样过程如下:给予一个$\boldsymbol{u}\in\mathbb{R}_q$,对短的$\boldsymbol{x}\in\mathbb{R}^{2+k-l}$进行采样,使得$\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}\approx\boldsymbol{u}\in\mathbb{R}_q$。

(1)搅扰采样:$\boldsymbol{p}\leftarrow D_{\mathbb{R}^{2+k-l},\sqrt{\Sigma_q}}$,其中,

$$\boldsymbol{\Sigma}_q=s^2\boldsymbol{I}-\sigma^2\begin{bmatrix}\boldsymbol{R}\boldsymbol{R}^{\mathrm{T}} & \boldsymbol{R}^{\mathrm{T}}\\ \boldsymbol{R} & \boldsymbol{I}\end{bmatrix},$$

是带有反循环块的块矩阵。

(2)计算$\boldsymbol{v}=\boldsymbol{u}-\boldsymbol{a}^{\mathrm{T}}\boldsymbol{p}\in\mathbb{R}_q$,且采样$\boldsymbol{z}\leftarrow RingGSAMCUT(\boldsymbol{v},\sigma)$。

(3)计算近似原像:$\boldsymbol{y}=\boldsymbol{p}+\begin{bmatrix}\boldsymbol{R}\\ \boldsymbol{I}\end{bmatrix}\boldsymbol{z}\in\mathbb{R}^{2+k-l}$。

接下来介绍一下$RingGSAMPCUT(\boldsymbol{u},\sigma)$算法:

算法1 $RingGSAMPCUT(\boldsymbol{u},\sigma)$

输入:环$\mathbb{R}_q$中的元素$\boldsymbol{u}$,以及高斯参数σ

1. 采样$\boldsymbol{x}_i\leftarrow GSAMCUT(u_i,\sigma)$,其中,$i\in\{0,\cdots,n-1\}$
2. 令$\boldsymbol{x}=\{\boldsymbol{x}_0,\cdots,\boldsymbol{x}_{n-1}\}\in\mathbb{Z}^{n(k-l)}$
3. 返回$\boldsymbol{z}=\boldsymbol{P}_f\boldsymbol{x}\in\mathbb{R}^{k-l}$

输出:$\boldsymbol{z}\in\mathbb{R}^{k-l}$满足$\boldsymbol{F}\boldsymbol{z}\approx\boldsymbol{u}\in\mathbb{R}_q$

$RingGSAMPCUT(u,\sigma)$算法首先在环上对目标$\boldsymbol{u}$的系数嵌入的每一个分量u_i进行g-格采样得到$\boldsymbol{x}'_i(\boldsymbol{x}'_i\in\mathbb{Z}^k)$,然后删去前$l$个分量得到$\boldsymbol{x}_i(\boldsymbol{x}_i\in\mathbb{Z}^{k-l})$,接下来再组合在一起成为$\boldsymbol{x}=(\boldsymbol{x}_0,\cdots,\boldsymbol{x}_{n-1})\in\mathbb{Z}^{n(k-l)}$,最后通过一个线性变换$\boldsymbol{P}_f$得到$\boldsymbol{z}=\boldsymbol{P}_f\boldsymbol{x}$。

1.4 基于非球形高斯的近似原像采样算法

为了近一步改进原像采样算法的安全性和签名尺寸,文献[18]提出了基于非球面高斯分布的

JHT22 原像采用算法。上述算法主要是通过改变分布,即将离散球形高斯分布变为了非球形高斯分布,且不泄露陷门的任何信息。由于签名大小和具体安全性与采样算法的高斯参数密切相关,该技术提供了两者之间的折中。具体地说,针对不同的目标设置了两种参数模式。模式一可以实现“双赢”局面,即获得具体的安全性并同时减小签名大小。模式二旨在进一步减小签名大小,而不会降低安全级别,接下来将对其进一步描述(为了表示方便,取 $w = n(k-l)$)。

(1) 搅扰向量的协方差修改为

$$\boldsymbol{\Sigma}_q = \begin{bmatrix} \bar{s}^2 \boldsymbol{I}_{2n} & \\ & \tilde{s}^2 \boldsymbol{I}_w \end{bmatrix} - \sigma^2 \begin{bmatrix} \boldsymbol{R} \\ \boldsymbol{I}_w \end{bmatrix} [\boldsymbol{R}^{\mathrm{T}} \quad \boldsymbol{I}_w]。$$

(2) 原像的 l_2 范数的上界变为

$$\sqrt{\bar{s}^2 2n + \tilde{s}^2 w}。$$

(3) 原像的存储大小上界变为

$$2n(1 + \lceil \log \bar{s} \rceil) + w(1 + \lceil \log \tilde{s} \rceil)。$$

为了保证算法的正确性与可模拟性,需要求 $\boldsymbol{\Sigma}_q \geqslant r^2$ 以及相关参数 $\bar{s}^2 \geqslant (\sigma^2 + r^2) \cdot S_1(R)^2 + 2\sigma^2 + 4r^2$,从而确定 $\bar{s} = \sigma' \cdot \tilde{s} \cdot s_1(R) / \sqrt{\tilde{s}^2 - \sigma'^2}$,其中,$\sigma'^2 = \sigma^2 + 5/4r^2$。模式一旨在尽可能提升算法的安全性,使原像范数上界的值最小,并且在确保算法的正确性与可模拟性的前提下,通过计算确定

$$\bar{s}^2 = (\sigma^2 + r^2) \cdot s_1(R)^2 + 2\sigma^2 + 4r^2,$$

$$\tilde{s}^2 = \frac{\bar{s}^2 \cdot \sigma^2}{\bar{s}^2 - s_1(R)^2 \cdot \sigma^2}。$$

接下来将给出环版本基于非球面高斯分布的近似陷门原像采样算法,用 *JHT-RingApproxSamPre*、*JHT-GMSampleP* 和 *RingGSAMPCUT* 分别表示运用非球面高斯的近似原像采样算法、搅扰向量采样算法和 g- 格采样算法。

算法 2 *JHT-RingApproxSamPre*($\boldsymbol{a}, \boldsymbol{R}, \boldsymbol{U}_l\boldsymbol{D}, \sigma, \bar{s}, \tilde{s}$)

输入:用户公钥 $\boldsymbol{a}$,主私钥 $\boldsymbol{R}$ 以及高斯参数 $\sigma, \bar{s}, \tilde{s}$

1. 搅扰采样:$\boldsymbol{p} \leftarrow$ *JHT-GMSampleP*($q, \sigma, \bar{s}, \tilde{s}, \boldsymbol{R}$)
2. 设置 $\boldsymbol{v} = U_{ID} - \boldsymbol{a}^{\mathrm{T}} \boldsymbol{p} \in \mathbb{R}_q$
3. G 格采样 $\boldsymbol{z} \leftarrow$ *RingGSAMPCUT*(v, σ)
4. 取 $\boldsymbol{y} = \boldsymbol{p} + \begin{bmatrix} \boldsymbol{R} \\ \boldsymbol{I} \end{bmatrix} \boldsymbol{z} \in \mathbb{R}^{2+k-l}$

输出:私钥 $sk_{ID} = \boldsymbol{y} \in \mathbb{R}^{2+k-l}$ 满足 $sk_{ID} \sim D_{\Lambda_q^{\perp}(a^{\mathrm{T}}), \sqrt{\Sigma}}$,其中,$\boldsymbol{\Sigma} = s^2 \boldsymbol{I}_{2n} \oplus \tilde{s}^2 \boldsymbol{I}_w$

上述表格中,算法 *JHT-GMSampleP* 是在搅扰向量下服从的协方差,修改为

$$\boldsymbol{\Sigma}_q = \begin{bmatrix} \bar{s}^2 \boldsymbol{I}_{2n} & \\ & \tilde{s}^2 \boldsymbol{I}_w \end{bmatrix} - \sigma^2 \begin{bmatrix} \boldsymbol{R} \\ \boldsymbol{I}_w \end{bmatrix} [\boldsymbol{R}^{\mathrm{T}} \quad \boldsymbol{I}_w],$$

其余部分与 Genise 等[30] 提出的 GM18 中的搅扰采样步骤一样。

2　基于非球形高斯的 RIBE 方案

在该部分,本文将描述一个新的 RIBE 方案。取 n, m, q 为正整数,且 q 为素数,$\sigma, \alpha, s, \tilde{s}, \tau$ 为正实数,令其作为本文的离散高斯参数,明文空间记为 M。用户身份空间记为 ID,由 $(k_{ID}+1)-bit$ 二进制字符串组成,它的第一位始终为 0。因此,$\| ID \| = 2^{k_{ID}}$。时间空间 T 由 $k_T - bit$ 二进制字符串组成,安全的哈希函数定义为 $H: \{0,1\}^{k_{ID}+k_T+1} \rightarrow \mathbb{R}_q$。特别地,在密钥更新步骤中,主要涉及一个特殊的算法 KUNode[31]。所谓的 KUNode 算法是将二叉树 BT 及其叶子集合 $RL_T = \{ID_1, \cdots, ID_R\}$ 作为输入,然后输出一组节点集合 $KU_T = \{\theta_1, \cdots, \theta_r\}$,它具有如下特征:

(1) 如果 $ID \in RL_T$,则存在唯一的 $ID[d] \in KU_T$,其中,$d \in [0, k_{ID}]$。

(2) 如果 $ID \notin RL_T$,则不存在 $ID[d] \in KU_T$,其中,$d \in [0, k_{ID}]$。

2.1　基于非球形高斯的 RIBE 方案

本文的 RIBE 方案主要是基于环版本对系统公钥生成算法,用户密钥生成算法和密钥更新算法运用非球面高斯的近似原像采样算法,因此,用 *New-Setup*、*New-GenSk* 和 *New-KeyUp* 来表示,其余部分都和方案[16] 描述一样。为了表示方便,取 $m = 2 + k - l$。

(1) *New-Setup*(1^{λ}) $\rightarrow$ (*MPK*, *MSK*)

运行算法 *RingApprox. TrapGen*(q, τ) $\rightarrow$ ($\boldsymbol{a}$, $\boldsymbol{R}$),其中,$\boldsymbol{R} \leftarrow D_{\mathbb{R}^{2\times(k-l)}, \lambda}$,$\boldsymbol{a} \in \mathbb{R}_q^m$。取 $MPK = \boldsymbol{a}$,$MSK = \boldsymbol{R}$。

(2) *Enc*(*MPK*, *ID*, *T*, *M*) $\rightarrow ct_{ID,T}$

1) 随机采样秘密 $\boldsymbol{s} \leftarrow U(\mathbb{R}_q)$,噪声向量 $\boldsymbol{x} \leftarrow D_{\mathbb{R}^m, \alpha}$,$\boldsymbol{x}_i \leftarrow D_{\mathbb{R}, \alpha}$,$i \in [0, k_{ID}]$。

2) 计算 $U_{ID} = H(ID \| 0)$,$U_{ID[i],T} = H(ID[i] \| T)$。

3) 计算密文:$\boldsymbol{c}=\boldsymbol{as}+\boldsymbol{x},\boldsymbol{c}_i=(U_{ID[i],T}+U_{ID})\boldsymbol{s}+\boldsymbol{x}_i+M\lfloor q/2\rfloor$, $i\in[0,k_{ID}]$,取

$ct_{ID,T}=(\boldsymbol{c},(\boldsymbol{c}_i)_{i\in[\boldsymbol{0},\boldsymbol{k}_{ID}]})\in\mathbb{R}_q^m\times\mathbb{R}_q^{k_{ID}+1}$。

(3) $New\text{-}GenSk(MPK,MSK,ID)\rightarrow sk_{ID}$

采样近似原像 ℓ_{ID}:运行 $\ell_{ID}\leftarrow JHT\text{-}Ring.ApproxSampPre(\boldsymbol{a},\boldsymbol{R},U_{ID},\sigma,\tilde{s},s)$。设置 $sk_{ID}=\ell_{ID}$ 作为用户的私钥。

(4) $New\text{-}KeyUp(MPK,T,MSK,RL_T)\rightarrow ku_T$

运行算法 $KUNode(RL_T)\rightarrow KU_T$,得到节点集合 KU_T,对任意的 $\theta_j\in KU_T$,运行 $JHT\text{-}Ring.ApproxSampPre(\boldsymbol{a},\boldsymbol{R},U_{\theta_j,T},\sigma,\tilde{s},s)\rightarrow\ell_{\boldsymbol{\theta}_j,\boldsymbol{T}}$,取 $ku_T=(\ell_{\boldsymbol{\theta}_j,\boldsymbol{T}})_{\theta_j\in KU_T}$ 得到更新密钥集合。

(5) $GenDk(MPK,sk_ID,ku_T)\rightarrow dk_{ID}$ 或 $\perp$(表示解密失败)

找出唯一的节点 $ID[d]\in KU_T$,如果不存在,则说明该用户ID被撤销,则算法输出 $\perp$。否则,取 $dk_{ID}=\ell_{ID}+\ell_{ID[d],T}$ 作为解密密钥。

(6) $Dec(MPK,dk_{ID,T},ct_{ID,T})\rightarrow M$

找出 $d\in[0,k_{ID}]$ 满足 $ID[d]\in KU_T$,计算 $\boldsymbol{c}=\boldsymbol{c}_d-\boldsymbol{c}^{\mathrm{T}}dk_{ID,T}\in\mathbb{R}_q$,得到的明文块 $\boldsymbol{c}$,其系数嵌入为 $\boldsymbol{c}_i$,若 $\boldsymbol{c}_i$ 与0的距离小于与 $\lfloor q/2\rfloor$ 的距离,则 $M_i=0$;否则 $M_i=1$,最后得到明文块 $M=(M_1,\cdots,M_n)$。

2.2 方案的正确性分析

由于加密算法与解密算法之间存在一定的误差,因此,本方案的解密正确性是由误差的 l_2 范数上界不能超过一定的值来保证[18]。得益于 $KUNode$ 算法[31],一个非撤销的用户可以使用一个有效的解密密钥 $dk_{ID}=\ell_{ID}+\ell_{ID[d],T}$ 得到:

$$\boldsymbol{c}'=\boldsymbol{c}_d-\boldsymbol{c}^{\mathrm{T}}dk_{ID[d],T}=(U_{ID[i],T}+U_{ID})\boldsymbol{s}+\boldsymbol{x}_d+M\lfloor\frac{q}{2}\rfloor-(\boldsymbol{as}+\boldsymbol{x})^{\mathrm{T}}(\ell_{ID}+\ell_{ID[d],T})=M\lfloor\frac{q}{2}\rfloor+\boldsymbol{x}_d-\boldsymbol{x}^{\mathrm{T}}(\ell_{ID}+\ell_{ID[d],T})+(\ell_1+\ell_2)\boldsymbol{s},$$

根据近似陷门的思想,$\boldsymbol{a}^{\mathrm{T}}\ell_{ID}\approx U_{ID}$,$\boldsymbol{a}^{\mathrm{T}}\ell_{ID[d],T}\approx U_{ID[d],T}$,且存在误差向量 $\ell_i\leftarrow D_{\mathbb{R},\eta}$,$i=\{1,2\}$,$\eta=\sigma\sqrt{(b^{2l}-1)/(b^2-1)}$,使得

$U_{ID}=\boldsymbol{a}^{\mathrm{T}}\ell_{ID}+\ell_1$, $U_{ID[d],T}=\boldsymbol{a}^{\mathrm{T}}\ell_{ID[d],T}+\ell_2$。

从而可观察到 $\boldsymbol{c}'=\boldsymbol{c}_d-\boldsymbol{c}^{\mathrm{T}}dk_{ID[d],T}$ 与 $M\lfloor q/2\rfloor$ 存在误差:

$$\boldsymbol{x}_d-\boldsymbol{x}^{\mathrm{T}}(\ell_{ID}+\ell_{ID[d],T})+(\ell_1+\ell_2)\boldsymbol{s},$$

只需保证该误差的 l_2 范数上界不超过 $\lfloor q/4\rfloor$ 即可。进一步分析,想要解密成功,单比特消息 c'_i 不能超过 $\lfloor q/4\rfloor$,即 $|\boldsymbol{ws}_i+\boldsymbol{sd}_i+\boldsymbol{st}_i-\boldsymbol{x}_{d_i}|<\lfloor q/4\rfloor$,其中,$\boldsymbol{ws}=(\boldsymbol{ws}_1,\cdots,\boldsymbol{ws}_n)\boldsymbol{s}$,$\boldsymbol{d}=(\boldsymbol{sd}_1,\cdots,\boldsymbol{sd}_n)$ 和 $\boldsymbol{st}=(\boldsymbol{st}_1,\cdots,\boldsymbol{st}_n)$ 分别为 $(\ell_1+\ell_2)\boldsymbol{s}$,$\sum_{i=1}^{2}\ell_i\boldsymbol{x}_i^{\mathrm{T}}$ 和 $\sum_{i=3}^{2+k-l}\ell_i\boldsymbol{x}_i^{\mathrm{T}}$ 的系数嵌入;$\ell=\ell_{ID}+\ell_{ID[d],T}$。根据相关引理可知,$\boldsymbol{ws}_i+\boldsymbol{sd}_i+\boldsymbol{st}_i-\boldsymbol{x}_{d_i}$ 的标准差为

$$n(2\sigma\sqrt{(b^{2l}-1)/(b^2-1)}+4s\alpha+2(k-l)\tilde{s}\alpha)+\alpha。$$

为了保证解密的正确性,根据 $|ws_i+sd_i+st_i-x_{d_i}|<\lfloor q/4\rfloor$ 可知,当

$$3|n(2\sigma\sqrt{(b^{2l}-1)/(b^2-1)}+4s\alpha+2(k-l)\tilde{s}\alpha)+\alpha|\leqslant\lfloor q/4\rfloor$$

时,可以保持较高的解密正确率。

2.3 方案的理论安全性分析

为了证明基于近似陷门的非球面高斯的RIBE方案是适应性身份匿名安全的,本节将通过安全游戏序列方式,由攻击者和挑战者进行8轮安全游戏,随着最后一轮游戏结束,若攻击者赢得游戏的优势是可忽略的,则说明本文的RIBE方案是适应性匿名安全的。安全性分析与文献[16]类似,为了简便,此处不进行过多叙述,详细证明过程参见附录A。

3 方案的实例化与分析

本方案运用基于近似陷门的非球面高斯采样技术,对方案[16]的公钥生成算法、用户秘钥提取算法以及更新秘钥提取算法进行了改进。在确保RIBE正确前提下,致力于缩减相关密钥的尺寸,以提升方案的空间效率。相比于模式二,模式一既能保证较高的安全性,又能一定程度上缩减密钥尺寸,因此,本文主要针对模式一进行比较,计算系统密钥尺寸、密文尺寸(单位为KB)以及评估LWE问题的安全性。

3.1 参数选取

本方案的参数主要包括安全参数 λ、多项式的阶 n、模数 q、维数 m、整数 b 以及高斯参数 $\sigma,\alpha,s,\tilde{s},\tau$。在参数选取方面,选取了 $n=1\ 024$ 以及 $n=2\ 048$ 两种取值进行分析。为了确保方案加解密的准确性,相关的参数需要满足

$$3\left|n\left(2\sigma\sqrt{\frac{(b^{2l}-1)}{(b^2-1)}}+4s\alpha+2(k-l)\tilde{s}\alpha\right)+\alpha\right|\leqslant\lfloor\frac{q}{4}\rfloor。$$

而又由于陷门 R 的标准差 τ 和噪声向量 x,x_i 的高

斯参数 α 需要保持相同才能够确保解密的低错误率,同时,为了保证误差项不能太大,环模 q 的值不能太小; 参数 α 的值受环模 q 和 n 取值的影响,也不能取太大,否则会使得解密错误率过高,导致无法成功解密。删减的维数 l 的值也不能取太高,否则也会导致误差太大,从而降低解密的成功率以及安全性。具体参数 n、q、l、b、σ、α、s、$\tilde{s}$ 和 τ 的选取如表 1 所示。

表 1　方案[16]与本方案在空间效率以及安全性上的具体数值比较

Table 1　Comparision of specific values of space efficiency as well as safety between scheme [16] and the present scheme

参数选取	$n=1\,024, b=2, \tau=\alpha=0.85$		$n=2\,048, b=2, \tau=\alpha=0.93$	
	方案[16]	本方案	方案[16]	本方案
q	2^{29}	2^{27}	2^{31}	2^{29}
l	0	9	0	10
$\bar{s}$	1 280.79	1 198.90	2 034.91	1 889.76
$\tilde{s}$		15.00		15.15
$\|sk_{ID}\|$	228 195.59	54 294.24	529 013.65	120 981.48
sk_{ID}	46.5	14.25	99.0	29.75
$dk_{ID,T}$	46.5	14.25	99.0	29.75
MPK	116.25	67.5	264.0	157.5
MSK	14.5	9.0	31.0	19.0
$ct_{ID,T}$	116.33	67.57	264.08	157.58
AISIS	332	349	741	759
LWE	82	91	195	311
ξ	$2^{-13.247}$	$2^{-13.072}$	$2^{-15.177}$	$2^{-15.241}$
参数选取	$n=1\,024, b=4, \tau=\alpha=1.9$		$n=2\,048, b=4, \tau=\alpha=1.2$	
	方案[16]	本方案	方案[16]	本方案
q	416	415	416	415
l	0	5	0	4
$\bar{s}$	4 595.75	4 032.74	4 097.77	3 705
$\tilde{s}$		55.32		55.85
$\|sk_{ID}\|$	623 940.18	182 586.76	786 771.25	237 307.31
sk_{ID}	31.5	12.0	63.0	25.75
$dk_{ID,T}$	31.5	12.0	63.0	25.75
MPK	72.0	45.0	144.0	97.5
MSK	8.0	5.0	16.0	11.0
$ct_{ID,T}$	72.08	45.77	144.08	97.58
AISIS	308	329	715	805
LWE	80	88	193	209
ξ	$2^{-35.20}$	$2^{-34.30}$	$2^{-28.24}$	$2^{-30.96}$

注:表中,τ 和 α 分别为陷门 R 的标准差和噪音向量服从的高斯参数,l 为近似陷门删减的维数,$\bar{s}$ 和 $\tilde{s}$ 为密钥服从的高斯参数,密钥的存储单位为 KB,ξ 为解密错误率。

3.2　安全性评估

本文主要采用 BKZ 算法对方案的安全性进行评估。具体来说,BKZ 算法主要是通过格上 SVP Oracles 的时间复杂度来评估相关问题的安全性。对于本方案的安全性分析主要分为两种情形: ①评估求解 ApproxISIS 问题的困难性(签名伪造的困难性);②评估公钥的随机性,即评估 LWE 问题的安全性(密钥恢复的困难性)。其中,LWE 问题的安全性主要由参数 n、q 以及陷门 R 的标准差 τ 来决定,固定 n 和 q 时,陷门 R 的标准差 τ 越大,

LWE 问题的安全性就越高。根据文献[21]可知,求解 *Approx ISIS*$_{m,n,q,\beta,\alpha}$ 问题的困难程度与求解 *ISIS*$_{n,q,m,\beta+\alpha}$ 问题的困难程度一样,因此,评估 *ApproxISIS* 问题的安全性可以转换为与之对应的 *ISIS* 问题的安全性。进一步而言,对于 *ISIS*$_{n,q,m,\beta+\alpha}$ 安全性评估,通过衡量要运行多少次 *BKZ* 算法才能在格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 找到一个短向量 $\boldsymbol{x}(\|\boldsymbol{x}\|=\beta+\alpha)$。*BKZ* 算法的时间复杂度计算过程如下:通过等式 $\beta+\alpha=\delta^{2n}\sqrt{q}$ 求出 δ,然后根据

$$\delta\approx(c/2\pi e(\pi c)^{1/c})^{1/2(c-1)}$$

求出 c 的值,最后取 $8\cdot 2n\cdot 2^{0.292c+16.4}$ 为其时间复杂度。

3.3 对比分析

如表2所示,本文与文献[16]在存储主私钥以及密钥所需的比特数方面进行对比。显然,仅从式子上看,无法直观凸显本 RIBE 在存储空间以及安全性上的优势。因此,本文通过选取合适的参数,使得方案[16]与本方案在同等解密错误率下,对 LWE 问题安全性、密钥尺寸等相关具体数据进行比较。特别地,从表2可知,更新密钥的存储尺寸与用户私钥密钥尺寸有着倍数关系,因此,仅对比解密密钥和用户密钥的存储尺寸,得到相关数值。具体如表1以及图1和图2所示,其中,用户数量 $ID=2^{20}$。

在同一解密错误率水平(表1和图1所示),可以看出,取定 $b=2$ 时,对于 $n=1\ 024$ 还是 $n=2\ 048$ 而言,LWE 的安全性至少提高了 9 - bit,主公钥 *MPK* 尺寸缩减了 40.34% ~41.93%,主私钥 *MSK* 尺寸缩减了 37.93% ~38.70%,用户私钥 sk_{ID} 以及解密密钥 $dk_{ID,T}$ 尺寸缩减了 69.35% ~69.95%,密文 $ct_{ID,T}$ 尺寸缩减了 40.33% ~41.91%。

表2 方案[16]与本方案的密钥在空间内存上的比较

Table 2 Comparison of keys in space memory between scheme [16] and the present scheme

参数	方案[16]	本方案
主私钥 R	$4kn$	$4(k-l)n$
主公钥 a	$(2+k)n\lceil\log q\rceil$	$(2+k-l)n\lceil\log q\rceil$
用户私钥 sk_{ID}	$(2+k)n(\lceil\log s\rceil+1)$	$2n(1+\lceil\log\bar{s}\rceil)+w(1+\lceil\log\bar{s}\rceil)$
更新密钥 ku_T	$(2+k)n(\lceil\log s\rceil+1)O(\lvert RL_t\rvert(k_{id}-\log\lvert RL_t\rvert))$	$(2n(1+\lceil\log\bar{s}\rceil)+w(1+\lceil\log\bar{s}\rceil))O(\lvert RL_T\rvert(k_{id}-\log\lvert RL_t\rvert)$
解密密钥 $dk_{ID,T}$	$(2+k)n(\lceil\log s\rceil+1)$	$2n(1+\lceil\log\bar{s}\rceil)+w(1+\lceil\log\bar{s}\rceil)$

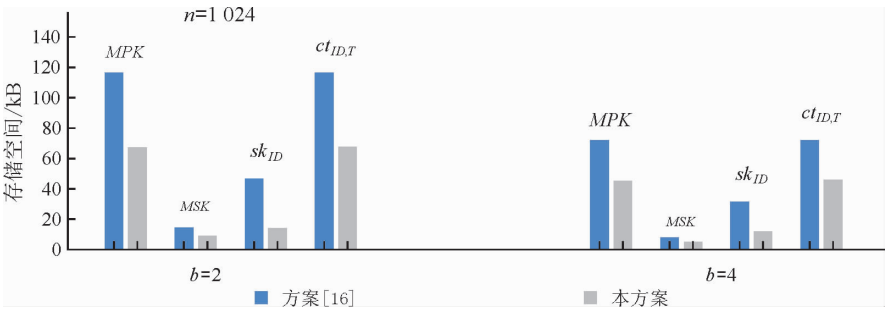

图1 同一解密错误率下,方案[16]与本方案数据存储尺寸对比

Fig. 1 Comparison of data storage size between scheme [16] and the present scheme for the same decryption error rate

同样地,对于取定 $b=4$ 时(如表2,图2所示),无论对于 $n=1\ 024$ 还是 $n=2\ 048$ 而言,LWE 的安全性至少提高了 8 - bit,主公钥 *MPK* 尺寸缩减了 32.29% ~37.50%,主私钥 *MSK* 尺寸缩减了 31.25% ~37.50%,用户私钥 sk_{ID} 以及解密密钥 $dk_{ID,T}$ 尺寸缩减了将近 59.13% ~61.90%,密文 $ct_{ID,T}$ 尺寸缩减了 32.27% ~36.50%。

从数据对比可以发现,在同一解密错误率水平下,主公钥和主私钥以及用户私钥的存储尺寸都至少缩减了30%以上。特别地,用户秘钥的缩减尺寸甚至高达60%,减少了内存的开销,提高了方案的空间效率。并且本文的 RIBE 方案的安全性也比方案[16]的安全性要高。

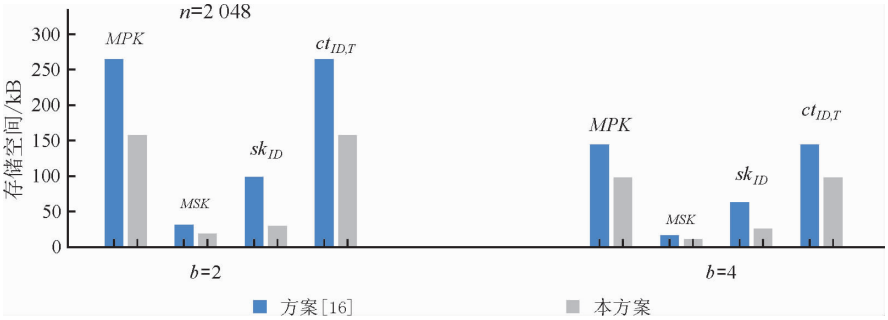

图 2　同一解密错误率下,方案[16]与本方案数据存储尺寸对比

Fig. 2　Comparison of data storage size between scheme [16] and this scheme for the same decryption error rate

4　结　论

综上所述,从以上几组数据分析可知,在同等解密错误率水平下,相比于原方案,本文基于近似陷门以及非球面高斯采样技术的 RIBE 方案在缩减密钥的存储空间方面比原方案更优,同时,方案的安全性也得到了一定的提升。

参考文献:

[1] Shamir A. Workshop on the Theory and Application of Cryptographic Techniques. April 09-11, 1984[C]. Berlin: Springer, 1984.

[2] Boneh D, Franklin M. Indentity-Based Encryption from the Weil pairing[J]. SIAM Journal on Computing, 2000, 32(3): 586-615.

[3] Paterson K G, Schuldt J C N. Proceedings of the 11th Australasian Conference on Information Security and Privacy (ACISP). July 03-05, 2006[C]. Berlin: Springer, 2006.

[4] Boneh D, Raghunathan A, Segev G. 33rd Annual Cryptology Conference Santa Barbara. August 18-22, 2013[C]. Berlin: Springer, 2013.

[5] Tessaro S, Wilson D A. 17th International Conference on Practice and Theory in Public-Key Cryptography. March 26-28, 2014[C]. Berlin: Springer, 2014.

[6] Boldyreva A, Goyal V, Kumar V. Proceedings of the 15th ACM Conference on Computer and Communications Security. October 27-31, 2008[C]. Berlin: Springer, 2008.

[7] Emura K, Takayasu A, Watanabe Y. Adaptively secure revocable hierarchical IBE from k-linear assumption[J]. Designs Codes Cryptography, 2021, 89(7): 1535-1574.

[8] Emura K, Takayasu A, Watanabe Y. Generic constructions of revocable hierarchical identity-based encryption[J]. Information Security and Cryptology, 2021, 12020: 381-396.

[9] Ge A J, Wei P W. 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography. April 14-17, 2019[C]. Berlin: Springer, 2019.

[10] Shor P. Polynomial-time algorithm for prime factorization and discrete logarithm on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[11] Chen J, Lim H W, Ling S, et al. 17th Australasian Conference on Information Security and Privacy. July 03-05, 2012 [C]. Berlin: Springer, 2012.

[12] Ma X C, Lin D D. Information Security and Cryptology-15th International Conference. December 04-06, 2019[C]. Berlin: Springer, 2019.

[13] Wang S X, Zhang J Y, He J N, et al. Cryptology and Network Security-18th International Conference. September 30—October 03, 2019[C]. Berlin: Springer, 2019.

[14] Agrawal S, Boneh D, Boyen X. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. May 30—June 03, 2010[C]. Berlin: Springer, 2010.

[15] Gentry G, Peikert C, Vaikuntanathan V. Proceedings of the 40th Annual ACM Symposium on Theory of Computing. May

17-20, 2008[C]. New York: ACM, 2008.
[16] Takayasu A. Adaptively secure lattice-based revocable IBE in the QROM: Compact parameters, tight security, and anonymity[J]. Designs, Codes and Cryptography, 2021, 89(8): 1-28.
[17] Micciancio D, Peikert C. 31th Annual International Conference on the Theory and Applications of Cryptographic Techniques. April 06-09, 2010[C]. Berlin: Springer, 2010.
[18] Jia H, Hu Y, Tang C. Lattice-based hash-and-sign signatures using approximate trapdoor, revisited[J]. IET Information Security, 2022, 16(1): 41-50.
[19] Lyubashevsky V, Micciancio D, Peikert C. 31th Annual International Conference on the Theory and Applications of Cryptographic Techniques. April 06-09, 2012[C]. Berlin: Springer, 2012.
[20] Micciancio D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions[J]. Computer Complexity, 2007, 16(4): 365-411.
[21] Chen Y, Genise N, Mukherjee P. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. May 30—June 03, 2010[C]. Berlin: Springer, 2010.
[22] Lyubashevsky V, Peikert C, Regev O. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. May 30—June 03, 2010[C]. Berlin: Springer, 2010.
[23] Bert P, Fouque P, Roux A, et al. 9th International Conference. April 09-11, 2018[C]. Berlin: Springer, 2018.
[24] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures[J]. SIAM Journal on Computing, 2007, 37(1): 267-302.
[25] Peikert C, Rosen A. Theory of Cryptography Conference. March 04-07, 2006[C]. Berlin: Springer, 2006.
[26] Bansarkhani R E, Buchmann J. 14th IMA International Conference. December 17-19, 2013[C]. Berlin: Springer, 2013.
[27] 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.
[28] Katsumata S C, Yamada S. 22nd International Conference on the Theory and Application of Cryptology and Information Security. December 04-08, 2016[C]. Berlin: Springer, 2016.
[29] Katsumata S C, Matsuda T, Takayasu A. 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography. April 14-17, 2019[C]. Berlin: Springer, 2019.
[30] Genise N, Micciancio D. 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques. April 29—May 03, 2018[C]. Berlin: Springer, 2018.
[31] Naor D, Naor M, Lotspiech J. 21st Annual International Cryptology Conference. August 19-23, 2001[C]. Berlin: Springer, 2001.

【责任编辑: 陈 钢】

附录

• 附录 A

本文所使用方案的安全性分析如下:

在 game－1 中,攻击者对$(ID \| 0)$进行随机询问,挑战者返回 $U_{ID}=H(ID \| 0)$。同样地,攻击者对$(ID[i] \| T)$进行随机询问,挑战者返回 $U_{ID}=H(ID[i] \| T)$。随后,攻击者对 ID 进行用户密钥生成询问,挑战者返回 $\ell_{ID}\leftarrow JHT\text{-}RingApproxSampPre(\boldsymbol{a},\boldsymbol{R},\boldsymbol{U}_{ID},\tau,\tilde{s})$。在撤销与密钥更新询问阶段,挑战者运行

$$\ell_{\theta_j,T}\leftarrow JHT\text{-}Ring.\ ApproxSampPre(a,\boldsymbol{R},\boldsymbol{U}_{\theta_j,T},\tau,\tilde{s},s)。$$

在攻击者挑战阶段,挑战者运行 $ct^{*}_{ID,T}\leftarrow Enc(MPK,MSK,ID^{*},T^{*},M^{*})$。若 coin = 0,则在$\mathbb{R}_q^{m+k_{ID}+1}$中随机采样一个发送给攻击者; 若 coin = 1,则将 $ct^{*}_{ID,T}$发送给攻击者。下面用 $Adv_j(\lambda)$表示攻击者在游戏 game－i 中的优势。

在 game－2 中,与上一轮游戏的不同点在于攻击者对$(ID,0)$进行密钥询问时,挑战者首先运行 $SampleZ(\sigma)$算法得到 $\ell_{ID},\boldsymbol{\omega}_1$,再令 $\boldsymbol{U}_{ID}=\boldsymbol{a}^{\mathrm{T}}\ell_{ID}+\boldsymbol{\omega}_1$。类似地,对$(\theta_j,T)$进行密钥询问时,挑战者首先运行 $SampleZ(\sigma)$算法得到 $\ell_{\theta_j,T},\omega_{\theta_j,T}$,再取 $\boldsymbol{U}_{\theta_j,T}=\boldsymbol{a}^{\mathrm{T}}\ell_{\theta_j,T}+\boldsymbol{\omega}_{\theta_j,T}$。挑战者将 $\boldsymbol{U}_{ID},\boldsymbol{U}_{\theta_j,T}$发送给攻击者,并且存储

$(ID,O,\boldsymbol{U}_{ID},\boldsymbol{\ell}_{ID},\boldsymbol{\omega}_1)$与$(ID,O,\boldsymbol{U}_{\theta_j,T},\boldsymbol{\ell}_{\theta_j,T},\boldsymbol{\omega}_{\theta_j,T})$。在合适的参数选取下,由引理 7 可知,$\boldsymbol{U}_{ID}$和$\boldsymbol{U}_{\theta_j,T}$与随机均匀中选取的数值是统计不可区分的,即攻击者在 game－2 和 game－1 的优势是统计不可区分的。

在 game－3 中,与 game－2 不同的地方在于挑战者并不利用主私钥 R 去创造用户私钥 $\boldsymbol{\ell}_{ID}$和 $\boldsymbol{\ell}_{\theta_j,T}$。具体来说,当攻击者对$(ID,0)$进行密钥询问时,并不运行算法

$$JHT\text{-}RingApproxSampPre,$$

而是直接令 $\boldsymbol{\ell}_{ID}=\boldsymbol{\ell}_{ID}$。同样地,挑战者也直接令 $\boldsymbol{\ell}_{\theta_j,T}=\boldsymbol{\ell}_{\theta_j,T}$来回应攻击者的询问。在合适的参数选取下,由引理7 可知,第二轮游戏中的 $\boldsymbol{\ell}_{ID}$与 $\boldsymbol{\ell}_{\theta_j,T}$在统计上靠近 $D^{U_{ID}}_{\Lambda_q^{(\boldsymbol{a}^{\mathrm{T}})},\sqrt{\Sigma}}$与 $D^{U_{\theta_j,T}}_{\Lambda_q^{(\boldsymbol{a}^{\mathrm{T}})},\sqrt{\Sigma}}$,则 $\boldsymbol{\ell}_{ID}$与 $\boldsymbol{\ell}_{\theta_j,T}$的统计也接近于 $D^{U_{ID}}_{\Lambda_q^{(a^{\mathrm{T}})},\sqrt{\Sigma}}$与 $D^{U_{\theta_j,T}}_{\Lambda_q^{(a^{\mathrm{T}})},\sqrt{\Sigma}}$,即攻击者在 game－2 和 game－3 的优势是统计不可区分的。

在 game－4 中,与 game－3 不同的地方在于挑战者并不运用 *RingApproxTrapGen* 算法生成主公钥,而是在$\mathbb{R}_q^m$上随机采样一个 $\boldsymbol{a}$,并且挑战者也不会使用主私钥 $\boldsymbol{R}$ 去回答攻击者的询问,但可以回应其他询问。在合适的参数选取下,可以确保 $\boldsymbol{a}$ 是统计上接近$\mathbb{R}_q^m$上的均匀分布,因此第三轮游戏与第四轮游戏中攻击者的优势是统计上不可区分的。

在 game－5 中,与前一轮游戏不同的地方在于密文的生成方式。在 game－4 中,取 $\boldsymbol{s}\leftarrow U(\mathbb{R}_q)$,$\boldsymbol{x}\leftarrow D_{\mathbb{R}^m,\alpha}$,$\boldsymbol{x}_i\leftarrow D_{\mathbb{R},\alpha}$,计算 $\boldsymbol{c}=\boldsymbol{a}\boldsymbol{s}+\boldsymbol{x}$,$\boldsymbol{c}_i=(\boldsymbol{U}_{ID^*[i],T}+\boldsymbol{U}_{ID^*})\boldsymbol{s}+\boldsymbol{x}_i+M^*\lfloor\frac{q}{2}\rfloor$。而在该轮游戏中,令 $\boldsymbol{s}\leftarrow U(\mathbb{R}_q)$,$\boldsymbol{x}\leftarrow D_{\mathbb{R}^m,\beta}$计算 $\boldsymbol{c}=\boldsymbol{a}\boldsymbol{s}+\boldsymbol{x}$,挑战者将$(ID^*,O,\boldsymbol{U}_{ID},\boldsymbol{\ell}_{ID^*})$与$(ID^*[i],T^*,\boldsymbol{U}_{ID^*[i],T},\boldsymbol{\ell}_{ID^*[i],T})$存储起来。再运行

$$ReRand([\boldsymbol{I}_m|\boldsymbol{\ell}_{ID^*[0],T^*}+\boldsymbol{\ell}_{ID^*}|\cdots|\boldsymbol{\ell}_{ID^*[k_{ID}],T^*}+\boldsymbol{\ell}_{ID^*}|],\boldsymbol{c},\beta),$$

见算法[28],从而可以得到$[\boldsymbol{c}\parallel\boldsymbol{c}_0\parallel\cdots\parallel\boldsymbol{c}_{k_{ID}}]$,挑战者再计算:$\boldsymbol{c}_i=\boldsymbol{c}_i+M^*\lfloor\frac{q}{2}\rfloor$,然后返回 $ct^*=(\boldsymbol{c},(\boldsymbol{c}_i)_{i\in[0,k_{ID}]})$。由引理6 可知,game－5 与 game－4 中攻击者的优势是统计上不可区分的。

在 game－6 中,对等式 $\boldsymbol{c}=\boldsymbol{a}\boldsymbol{s}+\boldsymbol{x}$ 上进行修改,即 $\boldsymbol{c}=\boldsymbol{v}+\boldsymbol{x}$,其中,$\boldsymbol{v}\leftarrow U(\mathbb{R}_q^m)$,$\boldsymbol{x}\leftarrow D_{\mathbb{R}^m,\beta}$。而 $LWE_{n,m,q,D_{\mathbb{R},\beta}}$问题的困难性,确保了 game－5 与 game－6 是计算无法区分的。具体来说,对于传统的多项式时间攻击者,存在一个传统的归约算法 B 满足$|Adv_5(\lambda)-Adv_6(\lambda)|\leqslant Adv_B^{LWE_{n,m,q,D_{\mathbb{R},\beta}}}$。

在 Game－7 中,挑战者并不会运行 *ReRand* 算法,而是直接采样 $\boldsymbol{c}\leftarrow U(\mathbb{R}_q^m)$,$\boldsymbol{x}'\leftarrow D_{\mathbb{R}^{m+k_{ID}+1},\alpha}$,计算

$$[\boldsymbol{c}\parallel\boldsymbol{c}_0\parallel\cdots\parallel\boldsymbol{c}_{k_{ID}}]=[\boldsymbol{I}_m|\boldsymbol{\ell}_{ID^*[0],T^*}+\boldsymbol{\ell}_{ID^*}|\cdots|\boldsymbol{\ell}_{ID^*[k\_ID],T^*}+\boldsymbol{\ell}_{ID^*}|]^{\mathrm{T}}\boldsymbol{c}+\boldsymbol{x}',$$

由引理6 可知,上述操作与 *ReRand* 算法得到的统计不可区分。从而在 game－7 与 game－6 中攻击者的优势是统计不可区分的。

Game－8 相比于 game－7 而言,无论 coin 取何值,挑战者都随机均匀采样 $ct^*\leftarrow U(\mathbb{R}_q\times\mathbb{R}^{k_{ID}+1})$。因此,在该轮游戏中,攻击者的优势为0; 要证明该轮游戏与上一轮游戏是统计不可区分的,即只需证明

$$[\boldsymbol{I}_m|\boldsymbol{\ell}_{ID^*[0],T^*}+\boldsymbol{\ell}_{ID^*}|\cdots|\boldsymbol{\ell}_{ID^*[k_{ID}],T^*}+\boldsymbol{\ell}_{ID^*}|]^{\mathrm{T}}\boldsymbol{c},$$

与$\mathbb{R}^{m+k_{ID}+1}$上的均匀分布是统计不可区分。由引理 4 以及剩余哈希引理可知,$[\boldsymbol{\ell}_m|\boldsymbol{\ell}_{ID^*[0],T^*}|\cdots|\boldsymbol{\ell}_{ID^*[k_{ID}],T^*}|]^{\mathrm{T}}\boldsymbol{c}$ 是以$(k_{ID}+1)\sqrt{q/2^{m-1}}$接近$\mathbb{R}^{m+k_{ID}+1}$上的均匀分布,从而有

$$[\boldsymbol{I}_m|\boldsymbol{\ell}_{ID^*[0],T^*}+\boldsymbol{\ell}_{ID^*}|\cdots|\boldsymbol{\ell}_{ID^*[k_{ID}],T^*}+\boldsymbol{\ell}_{ID^*}|]^{\mathrm{T}}\boldsymbol{c},$$

其以$(k_{ID}+1)\sqrt{q/2^{m-1}}$统计接近$\mathbb{R}^{m+k_{ID}+1}$上的均匀分布。则攻击者在 game－8 与 game－7 的优势是统计不可区分的。具体来说,$|Adv_7(\lambda)-Adv_8(\lambda)|\leqslant 2^{-\Omega(n)}$。

综上所述,由以上 8 轮安全游戏可知,第一轮游戏与第八轮游戏是统计不可区分的,即攻击者在第一轮游戏中的优势接近于0,从而可知该方案满足适应性匿名安全。