计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200700215

基于 R-SIS 和 R-LWE 构建的 IBE 加密方案

钱心缘[1,2]　吴文渊[1]
1 中国科学院重庆绿色智能技术研究院自动推理与认知重庆市重点实验室　重庆 400714
2 中国科学院大学　北京 101408
(979454883@qq.com)

摘　要　格上基于身份的加密机制(Identity-Based Encryption,IBE)能够有效抵抗量子攻击,并且该机制将每个人的身份信息作为公钥,能够简化公钥基础设施(Public Key Infrastructure,PKI)对海量用户的公钥管理,这种加密机制是对传统 PKI 的改进,能够解决 PKI 在物联网环境下暴露的众多问题。然而,目前国内外学者提出的基于格的 IBE 方案大多比较笨重,并且实现的方案很少。针对上述问题,提出了一种基于 R-SIS 以及 R-LWE 困难问题的 IND-sID-CPA 安全的 IBE 低膨胀率方案。首先,提出了分块复用技术,通过重用占存储空间较大的辅助解密密文块,极大地降低了密文膨胀率并提高了加密效率。然后,利用了 Kyber 提出的压缩算法并引入明文扩张参数,对以上两个参数指标进行进一步优化。通过严格的理论推导分析了所提方案的安全性、正确性和计算复杂度,利用数值实验给出了该方案在 3 种场景下的较优参数取值。最后,通过 C++程序实现新方案,对比了所提方案与 BFRS18 方案在 3 种场景下的性能。实验结果表明,该方案在保证正确性和安全性的同时,有效提高了原方案的加解密效率,降低了密文膨胀率。

关键词:基于身份加密;格密码;环小整数解问题;环容错学习问题;分块复用技术;压缩技术;高斯采样
中图法分类号　TP309

Identity-based Encryption Scheme Based on R-SIS/R-LWE

QIAN Xin-yuan[1,2] and WU Wen-yuan[1]
1 Chongqing Key Laboratory of Automated Reasoning and Cognition,Chongqing Institute of Green and Intelligent Technology,Chinese Academy of Sciences,Chongqing 400714,China
2 University of Chinese Academy of Sciences,Beijing 101408,China

Abstract　The identity-based encryption(IBE) by lattice can effectively resist quantum attacks,and this mechanism takes users' identity information as public keys,which can ease the management of public key infrastructure(PKI) with an extremely large number of users. The lattice-based IBE system is an improvement of the traditional PKI to solve some problems in the Internet of Things(IoT) environment. However,previous IBE schemes based on lattices are cumbersome,and there are few implementations of these schemes. Aiming at this problem,this paper proposes an IBE scheme based on R-SIS and R-LWE with advantages of low expansion rate,which is secure against IND-sID-CPA. Firstly,a block reusing technology is proposed to reuse a ciphertext block for auxiliary decryption which occupies a significant amount in storage so that the expansion rate of ciphertext decreases and the encryption efficiency improves in a large extent. Then,by using a compression algorithm and introducing a plaintext expansion parameter,the two indicators of the scheme have been further optimized. Next,the scheme's security,correctness,and computing complexity are analyzed through rigorous theoretical derivation,and numerical experiments with Maple give the optimal parameter values of this scheme under three scenarios. Finally,the new scheme is implemented with C++,and the performance of the scheme and the BFRS scheme in three scenarios are compared. Experiments and comparisons show that,while ensuring the correctness and security,this scheme improves the encryption and decryption efficiency of the original scheme and reduces the ciphertext expansion rate effectively.

Keywords　Identity-based encryption,Lattice,Ring small integer solution problem,Ring learning with errors problem,Block reusing technology,Compression technology,Gaussian sampling

到稿日期:2020-07-31　返修日期:2020-09-15　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:重庆市科委项目(cstc2018jcyj-yszxX0002,cstc2019yszx-jcyjX0003);中科院前沿科学重点项目(QYZDB-SSW-SYS026);贵州省科技计划项目([2020]4Y056)
This work was supported by the Chongqing Science and Technology Program(cstc2018jcyj-yszxX0002,cstc2019yszx-jcyjX0003), Key Research Program of Frontier Sciences of Chinese Academy of Sciences(QYZDB-SSW-SYS026) and Guizhou Science and Technology Program([2020]4Y056).
通信作者:吴文渊(wuwenyuan@cigit.ac.cn)

1 引言

5G 时代下，物联网(Internet of Things，IoT)蓬勃发展。随着 IoT 用户和设备的数量激增以及 IoT 环境对安全性的要求越来越高，传统公钥基础设施(Public Key Infrastructure，PKI)因其繁重的管理机制将无法适应 IoT 环境。基于身份的加密机制(Identity-Based Encryption，IBE) 是公钥密码的新方向，这种机制能够让加密方直接使用解密方的身份标识作为公钥，简化了 PKI 在多用户系统中密钥的产生和分配工作，从而解决了传统公钥机制因大量交换数字证书而导致系统效率低下的问题。IBE 的思想最初在 1984 年由 Shamir 提出[1]；2001 年，Boneh 首次提出了一种可实用的 IBE 构造[2]；此后，众多 IBE 方案被提出，使其形态呈多样化发展。

1994 年，Shor 算法[3]的提出意味着利用一台量子计算机可以极大地降低基于数论问题的困难性，进而破解了传统公钥密码体系[4]。当前已经出现了很多基于传统数学困难问题的高效 IBE 方案及实现[2,5]，因此这些方案在后量子时代下均无法抵抗量子攻击。格密码最显著的特征包括能够抵抗量子攻击、并行性以及在最困难情况的假设下无法求解的安全性，所以将格密码与 IBE 加密机制相结合有望替代传统的加密算法。格密码的研究最初是基于 Ajtai 的工作[6]，这种密码体制采用格困难问题作为格密码构造的安全性基础。到目前为止，被证明安全的基于格的困难问题主要有两种：1)小整数解问题(Small Integer Solution Problem，SIS)[6]；2)容错学习问题(Learning With Errors Problem，LWE)[7]。两个困难问题的实用变种 R-SIS[8]与 R-LWE[9]分别于 2006 年和 2009 年被相继提出，其优势在于：存储需求低、计算效率高，并且存在从最坏情况的理想格问题向这两个实用变种问题的归约。格的采样是大多数格上 IBE 方案不可或缺的技术，最初的原像采样算法[10-12]是顺序的(无法并行)且非常耗时，随后提出的众多并行可高效求解的格采样方案[13-16]极大地提高了采样效率。

2008 年，Gentry 等提出了第一种基于格困难问题的后量子 IBE 加密机制(Gentry-Peikert-Vaikuntanathan，GPV)[12]，此后密码学家又在此基础上进行了诸多改进[17-22]。2010 年，Cash 等[17]和 Agrawal 等[18]分别提出了两种不同的 IBE 框架。Cash 等所提方案的安全性证明撇开了常用的 Random Oracle 模型，但其公钥尺寸太大而无法实际应用；Agrawal 等利用两个特殊陷门构建了基于格的 IBE 标准模型(Agrawal-Boneh-Boyen，ABB)，后续很多 IBE 方案都是基于 ABB 框架构建的。2014 年，Ducas 等基于 GPV 加密机制，构造了一种基于 NTRU 格的 IBE 方案[19]，他们首次用程序实现了格上构造的 IBE 方案(Ducas-Lyubashevsky-Prest，DLP)。因 NTRU 基的特殊性质，该方案的加解密效率极高，Mccarthy 等在该方案的基础上进行了优化和改进[20]。与本文相关的近期工作是 Bert 等提出的一种基于 R-SIS 和 R-LWE 问题的 IBE 加密方案(Bert-Fouque-Roux-Sabt，BFRS)[21]，其采用 MP(Micciancio-Peikert)思想[14]构造陷门，采用 GM(Genise-Micciancio)算法[15]对原像采样进行了优化。该方案的加解密效率优于 DLP 方案，并且是基于更加一般的困难假设。近年来，针对格上 IBE 高效新方案的研究较少，大多数工作都是致力于对格上基于身份签名(Identity-Based Signature，IBS)的改进[23-25]、格上 IBE 的可撤销机制[26-27]以及 IBE 在工业中的应用[28-32]，然而很多方案只能满足特定的功能，其加解密效率以及存储性能无法满足实际需求。

从以上分析可以看出，利用格理论构造的 IBE 方案并不成熟，大多数仅停留在理论研究阶段，其加解密效率和存储性能并不能满足实际应用的需求，并且相关方案的具体性能分析也少之又少。因此，本文提出了一种基于 R-SIS 和 R-LWE 问题的高效 IBE 方案。本文的主要贡献有：1)基于 LWE 的多比特加密思想，提出了基于 R-LWE 的分块复用技术，并利用该技术优化 BFRS 方案。2)将 Kyber 的压缩技术、明文扩张参数与 BFRS 相结合，进一步降低密文膨胀率。3)利用安全游戏序列，在选择身份的 IBE 安全模型上对优势差公式进行严格推导，将新方案的安全性归约至 R-SIS 与 R-LWE 困难问题；分析噪声产生的误差分布，进而推导出特定出错概率下方案正确解密所应满足的公式，论证了方案的正确性；利用 Maple 程序进行数值实验，根据推导公式计算出了本文在 3 种不同场景下满足条件的较优参数取值。4)通过 C++编程测试本文方案性能，对比了所提方案与 BFRS 方案在 3 种场景下加解密操作的实验数据。实验结果表明，本文方案的加解密效率更高，密文膨胀率更低。

2 预备知识

2.1 记号表示

表 1 列出了本文使用的基本符号的简单定义。

表 1 基本符号表示

Table 1 Basic symbolic representation

Symbols	Descriptions
$\mathbb{Z}$	The set of integers.
$\mathbb{Z}_q$	$\mathbb{Z}$ mod q, usually q is a prime and $\mathbb{Z}_q$ is a field.
$\mathbb{Z}_q^n$	The N-dimensional vector space of $\mathbb{Z}_q$.
$\mathbb{R}$	The set of real numbers.
$\mathbb{Z}_q[x]$	$\mathbb{Z}[x]$ mod (x^n+1).
R	A set of polynomial ring with integer coefficients
R_q	For an integer q, $R_q=R/qR=\mathbb{Z}_q[x]$ mod (x^n+1)
R_q^k	The set of column vectors consisting of k polynomials of R_q.
$negl(\lambda)$	Negligible functions with safety parameter λ.
$\sigma,\gamma,\zeta,\alpha$	Gaussian parameters used in Gaussian sampling.
$D_{\Lambda,\sigma}$	Discrete Gaussian distribution on lattice Λ with gaussian parameter σ.
$U(Y)$	Uniform distribution of random variable Y.
$s\leftarrow X(Y)$	The value of the random variable Y sampled according to the X distribution is assigned to s.
a_j	$a=(a_0,a_1,\cdots,a_{n-1})\in R_q$, $a_i\in\mathbb{Z}_q$, and a_j is the coefficient of x^j.
$a_{i,j}$	$a=(a_0,a_1,\cdots,a_{m-1})\in R_q^m$, $a_i\in R_q$, and $a_{i,j}$ is the coefficient of x^j in a_i.

本文中，规定列向量以及矩阵分别用加粗的小写字体(例如，$\boldsymbol{x}$)和加粗的大写字体(例如，$\boldsymbol{T}$)表示。其中，向量 $\boldsymbol{x}$ 的欧几里得范数为 $\|\boldsymbol{x}\|$，矩阵 $\boldsymbol{T}$ 的范数为其列向量所有范数中的最大值，即 $\|\boldsymbol{T}\|=\max_i\|\boldsymbol{t}_i\|$。对于 $x\in\mathbb{R}$，符号 $\lfloor x\rfloor$ 表示对 x 向下取整，符号 $\lceil x\rceil$ 表示对 x 向上取整，符号 $\lceil x\rfloor$ 表示取 x 的四舍五入。

2.2 格及其相关表示

定义 1（格[33]） 给定一组 n 维线性无关的向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\in\mathbb{R}^m$，则由这些向量生成的格定义如下：

$$\Lambda=\mathcal{L}(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)=\{\sum_{i=1}^{n}z_i\boldsymbol{b}_i:z_i\in\mathbb{Z}\}$$

并且 $B=[\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n]$ 是 Λ 的一组基，n 为 Λ 的秩，m 为 Λ 的维数。

定义 2（取模运算与剩余系的表示） 假设 q 是一个正奇数，本文定义运算 $r'=r \bmod^{\pm} q$，并且 r' 表示完全剩余系 $\mathbb{Z}_q=\{-(q-1)/2,-(q-3)/2,\cdots,(q-1)/2\}$ 中与 r 唯一对应的元素，满足 $r'=r \bmod q$。同理，定义运算 $r'=r \bmod^{+} q$，r' 表示在完全剩余系 $\mathbb{Z}_q=\{0,1,\cdots,q-1\}$ 中与 r 唯一对应的元素，满足 $r'=r \bmod q$。

定义 3（多项式环的乘法[21]） 令 n 为 2 的幂次时，定义多项式环 $R_q=\mathbb{Z}_q[x]/(x^n+1)$，此时 R_q 与整数格 $\mathbb{Z}_q^n$ 同构。一个在环上的多项式 $f=\sum_{i=0}^{n-1}f_ix^i\in R_q$ 表示为一组系数为整数所组成的向量 $(f_0,f_1,\cdots,f_{n-1})\in\mathbb{Z}^n$。对于任意两个多项式 $a,b\in R_q$，令 c 为 a 和 b 在 $\mathbb{Z}[x]$ 中的乘积，则将 a 和 b 在 R_q 中的乘法定义为：$a\cdot b\equiv c \bmod (x^n+1)\bmod^{\pm} q$。

本文剩下篇幅基本都在多项式环 R_q 中进行讨论，其中模数 q 为质数。

定义 4（q-ary 格[34]） 对于一个质数 q，$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，并且 $\boldsymbol{u}\in\mathbb{Z}_q^n$，有如下定义：

$$\Lambda_q(\boldsymbol{A})=\{\boldsymbol{z}\in\mathbb{Z}^m,\text{ s. t. }\exists\boldsymbol{s}\in\mathbb{Z}_q^n,\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}=\boldsymbol{z}(\bmod q)\},\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{z}\in\mathbb{Z}^m,\text{ s. t. }\boldsymbol{A}^{\mathrm{T}}\boldsymbol{z}=0(\bmod q)\},\Lambda_q^{u}(\boldsymbol{A})=\{\boldsymbol{z}\in\mathbb{Z}^m,\text{ s. t. }\boldsymbol{A}^{\mathrm{T}}\boldsymbol{z}=\boldsymbol{u}(\bmod q)\}。$$

定义 5（离散高斯分布[21]） 对于所有 $\boldsymbol{x}\in\mathbb{R}^n$，中心是 $\boldsymbol{c}\in\mathbb{R}^n$、宽度参数为 $\sigma>0$ 的 n 维高斯函数定义为 $\rho_{\sigma,\boldsymbol{c}}(x)=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/\sigma^2)$。

利用可逆矩阵 $\boldsymbol{B}$ 对以上公式进行简单的线性映射，可以将这个定义拓展至以下满足以正定对称矩阵 $\sum=\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}$ 为协方差矩阵的高斯函数：

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

将一个格 Λ 上的离散高斯分布定义为：

$$D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\sum_{\boldsymbol{x}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}$$

本文用到两个格困难问题 R-SIS 和 R-LWE，两个理想格上的问题均可以归约至格上的最困难问题 GapSVP 和 Gap-SIVP。

定义 6（$R\text{-}SIS_{q,m,\beta}$ 问题[35-36]） 给定一个满足均匀分布的 m 维多项式 $\boldsymbol{a}=(a_1,a_2,\cdots,a_m)^{\mathrm{T}}\in R_q^m$，寻找一个每项系数取值较小的非零向量所表示的多项式 $\boldsymbol{x}=(x_1,\cdots,x_m)^{\mathrm{T}}\in R_q^m$，满足 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=\sum_{i=1}^{m}a_ix_i=0$，且 $0<\max_i(x_i)\leqslant t\beta$。

定义 7（$Decision\ R\text{-}LWE_{n,q,\chi}$ 问题[9,37]） 令 $\Delta=R_q^m$，$\chi=D_{\Delta,\sigma}$，给定一个满足均匀分布的 m 为多项式 $\boldsymbol{a}=(a_1,a_2,\cdots,a_m)^{\mathrm{T}}\in R_q^m$，以及 $\boldsymbol{b}=\boldsymbol{a}s+\boldsymbol{e}$，其中 $s\leftarrow U(R_q)$，$\boldsymbol{e}\leftarrow\chi$。$Decision\ R\text{-}LWE_{n,q,\chi}$ 问题即为区分按照以上构造得到的分布 $(\boldsymbol{a},\boldsymbol{b})$ 和在 $R_q^m\times R_q^m$ 上均匀选取的分布。

2.3 随机多项式乘积分布

定理 1 假设 n 为整数，对于任意两个属于 R_q 的 n 维多项式 V 和 U，如果 V 和 U 的每项系数独立并且满足期望均为 0、方差分别为 η 和 ξ 的分布，则这两个多项式的乘积 $Y=VU$ 的分布近似于 $N(0,n\cdot\eta\xi)$ 分布。

将以上两个高斯分布的多项式分别写成 $V=v_0+v_1x+\cdots+v_{n-1}x^{n-1}$ 和 $U=u_0+u_1x+\cdots+u_{n-1}x^{n-1}$ 的形式。由定义 2 通过简单推导可以得到关于 V 和 U 的乘法：

$$(y_0,y_1,\cdots,y_{n-1})=(v_0,v_1,\cdots,v_{n-1})\cdot\begin{bmatrix}u_0 & u_1 & u_2 & \cdots & u_{n-1}\\ -u_{n-1} & u_0 & u_1 & \cdots & u_{n-2}\\ -u_{n-2} & -u_{n-1} & u_0 & \cdots & u_{n-3}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ -u_1 & -u_2 & -u_3 & \cdots & u_0\end{bmatrix}$$

因此，Y 可以表示成 $Y=VU=y_0+y_1x+\cdots+y_{n-1}x^{n-1}$。针对 Y 中每一项系数 $y_i=v_0u_i+v_1u_{i-1}+\cdots+v_iu_0-v_{i+1}u_{n-1}-v_{i+2}u_{n-2}-\cdots-v_{n-1}u_{i+1}$，由于 v_g 和 u_h 相互独立，y_i 是 n 个线性独立同分布 v_gu_h 的线性组合，因此 Y 的每项系数独立同分布。由 v_g 和 u_h 的独立性可以得到 v_gu_h 的期望和方差如下：

$$E(v_gu_h)=E(v_g)\cdot E(u_h)=0$$

$$D(v_gu_h)=\sum_{g=0}^{n-1}\sum_{h=0}^{n-1}(v_g\cdot u_h)^2\cdot\Pr[v_g]\Pr[u_h]-E^2(v_gu_h)=D(v_g)D(u_h)=\eta\cdot\xi$$

根据中心极限定理，可以得到 n 维多项式 Y 的分布近似高斯分布且满足 $N(0,n\cdot\eta\xi)$。

2.4 IBE 加密机制

图 1 给出了 IBE 的基本工作流程。PKG 在一定时间内根据系统安全参数生成相应的主公钥（Master Public Key，MPK）和主私钥（Master Secret Key，MSK）。如果 Alice 要给 Bob 发送加密信息，只需要知道 Bob 的身份信息（如邮件地址、电话号码等），就能生成属于 Bob 的公钥，进而对即将发送的密文进行加密；而 Bob 解密时所使用的私钥 $sk_{id_{\mathrm{Bob}}}$ 由系统的 Extract 算法生成，Bob 利用系统发送的 $sk_{id_{\mathrm{Bob}}}$ 对密文进行还原。通用 IBE 加密框架由 4 个多项式时间的概率算法组成：Setup，Extract，Encrypt 和 Decrypt，具体请参考文献[21]。

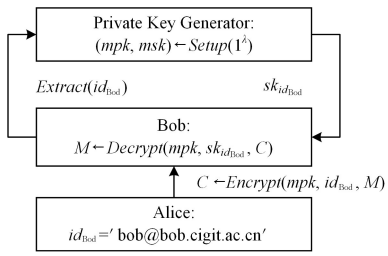

图 1 IBE 流程图

Fig. 1 Flow chart of IBE

2.5 G-格的陷门与采样

为了根据用户身份 id 生成其公私钥对，需要使用 G-格构造用户公钥，再采用原像采样算法求解其私钥。由于篇幅限制，本文只给出简单的原理与求解过程，详细请参见文献[21]。

2.5.1 基本原理

BFRS 中的 IBE 加密机制主要依靠由 Ajtai 引入的一种

陷门[6,38]，这种陷门采样技术在后续的工作中得到了改进[14-15]。BFRS 中使用陷门的主要思想如下：

对于任意 $\boldsymbol{a}\in R_q^k$，$u\in R_q$，定义陷门函数：$f_{\boldsymbol{a}}(\boldsymbol{x})=\boldsymbol{a}\boldsymbol{x}\in R_q$。这种陷门函数的安全性由 R-SIS 问题做支撑（详见定义 6），即已知 $\boldsymbol{a}$ 和 u，寻找一个足够小的非零多项式向量 $\boldsymbol{x}$ 满足 $\boldsymbol{a}\boldsymbol{x}=u\in R_q$ 困难。

上述困难问题中的 $\boldsymbol{x}$，可以通过构造 G-陷门并通过原像采样算法高效求解。结合 IBE 系统，假设用户公钥为 $\boldsymbol{a}$，公开参数为 u，上述方法对 $\boldsymbol{a}$ 的构造有特殊要求，需要利用 G-陷门进行构造。利用短基 $\boldsymbol{T}\in R^{(m-k)\times k}$ 在格 $\Lambda_q^{\perp}(\boldsymbol{a})$ 中以适当的高斯参数 σ 进行原像采样，可以快速得到用户私钥 $\boldsymbol{x}$；任何人在没有主私钥 $\boldsymbol{T}$ 的情况下无法求得私钥 $\boldsymbol{x}$，故此处的安全性由 R-SIS 问题保证。

2.5.2 G-陷门的构造

通常，将如下常量多项式组成的向量称作 $\boldsymbol{g}$-向量[21]：$\boldsymbol{g}=(1,2,2^2,\cdots,2^{k-1})^{\mathrm{T}}\in R_q^k$，其中 $k\geqslant\log_2(q)$。该向量的优势在于其计算具有可逆性，即对于函数 $f_{\boldsymbol{g}^{\mathrm{T}}}(\boldsymbol{z})=\boldsymbol{g}^{\mathrm{T}}\boldsymbol{z}\in R_q$，当 $f_{\boldsymbol{g}^{\mathrm{T}}}(\boldsymbol{z})=u\in R_q$ 时，已知 u 可以求得向量 $\boldsymbol{z}$。

本文在 BFRS 方案中用到的主要算法名称前加上方案名称，以此表示算法，如 *BFRS-TrapGen*，*BFRS-SamplePre*，*BFRS-SampleP* 以及 *BFRS-SamplePolyG*。本节主要利用 *BFRS-TrapGen* 陷门生成算法，该算法将环模数 q、高斯参数 σ、参数 $\boldsymbol{a}'$ 和身份标签 h_{id} 作为输入，采用散列函数进行身份映射 $h_{id}=\boldsymbol{H}(id)$[21] 得到用户身份标签。通过采样操作得到主私钥 $\boldsymbol{T}\leftarrow D_{R^{(m-k)\times k}}$ 后，计算用户公钥 $\boldsymbol{a}=(\boldsymbol{a}^{\mathrm{T}}|h_{id}\boldsymbol{g}-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{T})^{\mathrm{T}}$，陷门生成算法最终输出 $(\boldsymbol{a},\boldsymbol{T})$。得到的结果满足关系：

$$\boldsymbol{a}\,(\boldsymbol{T},\boldsymbol{I})^{\mathrm{T}}=h_{id}\boldsymbol{g}^{\mathrm{T}} \tag{1}$$

2.5.3 原像采样算法

使用原像采样算法的目的是利用陷门参数 $\boldsymbol{T}$ 快速求解私钥 $\boldsymbol{x}$。原像采样算法的具体定义请参见文献[12]。BFRS 中调用原像采样算法 *BFRS-SamplePre* 计算 $\boldsymbol{x}$，使得 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=u\in R_q$ 成立，该算法同时调用了辅助算法 *BFRS-SampleP* 和 *BFRS-SamplePolyG*。*BFRS-SamplePre* 的大致思路如下：将用户公钥 $\boldsymbol{a}\in R_q^m$、陷门 $\boldsymbol{T}\in R^{(m-k)\times k}$、陷门标签 $h_{id}\in R_q$、随机多项式 $u\in R_q$ 以及高斯噪声参数 ζ、σ 和 α 作为输入。首先利用 *BFRS-SampleP* 产生满足 $\sum\limits_{p}=\zeta^2\boldsymbol{I}_m-\alpha^2(\boldsymbol{T},\boldsymbol{I}_k)^{\mathrm{T}}(\boldsymbol{T}^{\mathrm{T}}\boldsymbol{I}_k)$ 分布的扰动量 $\boldsymbol{p}$。然后计算：

$$v\leftarrow h_{id}^{-1}\cdot(u-\boldsymbol{a}^{\mathrm{T}}\boldsymbol{p}) \tag{2}$$

利用 *BFRS-SamplePolyG* 算法在 $\Lambda_q^{\perp}(\boldsymbol{g}^{\mathrm{T}})$ 中进行 G-格的采样，得到满足条件的 $\boldsymbol{z}$：

$$\boldsymbol{g}^{\mathrm{T}}\boldsymbol{z}=v\in R_q \tag{3}$$

最后计算 $\boldsymbol{x}$：

$$\boldsymbol{x}\leftarrow\boldsymbol{p}+(\boldsymbol{T},\boldsymbol{I}_k)^{\mathrm{T}}\boldsymbol{z} \tag{4}$$

这样的 $\boldsymbol{x}$ 满足分布 $\sum\limits_{x}=\sum\limits_{p}+\alpha^2(\boldsymbol{T},\boldsymbol{I}_k)^{\mathrm{T}}(\boldsymbol{T}^{\mathrm{T}}\ \boldsymbol{I}_k)=\zeta^2\boldsymbol{I}_m$，这种球状高斯分布不会泄露私钥的任何信息[18]。

由式(1)—式(4)联立得到 $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{x}=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{p}+\boldsymbol{a}^{\mathrm{T}}(\boldsymbol{T},\boldsymbol{I}_k)^{\mathrm{T}}\boldsymbol{z}=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{p}+h_{id}\boldsymbol{g}^{\mathrm{T}}\boldsymbol{z}=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{p}+h_{id}\cdot h_{id}^{-1}(u-\boldsymbol{a}^{\mathrm{T}})\boldsymbol{p}=u$，原像采样算法的正确性得证。

2.6 压缩技术

为了降低密文膨胀率，本文使用 Kyber 提出的压缩(compress)与解压(decompress)技术[39]，具体的函数定义如下。

$Compress(x,d,q)\rightarrow y=\lceil x\cdot(2^d/q)\rfloor\bmod^{+}2^d$：输入 $x\in\mathbb{Z}_q$，压缩参数 $d\leqslant\lfloor\log_2(q)\rfloor$（$d$ 需要根据噪声对解密正确性的影响进行取值），输出一个属于 $\mathbb{Z}_q$ 的整数 y。

$Decompress(y,d,q)\rightarrow x'=\lceil(q/2^d)\cdot y\rfloor$：输入 $y=Compress(x,d,q)$，输出 $x'=\lceil(q/2^d)\cdot y\rfloor$。

当对整数 $x\in\mathbb{Z}_q$ 分别调用压缩和解压算法后将产生误差：$|x'-x|\bmod q\leqslant\lceil q/2^{d+1}\rfloor$。

引入压缩和解压技术后，可以对密文进行一定程度的压缩。将这种技术应用在多项式环 $x\in R_q$ 或 $\boldsymbol{x}\in R_q^k$ 上，则可以逐次对每一项的相应参数进行压缩和解压。进行压缩和解压会对方案的误差造成一定影响，3.4 节将会对本文方案进行误差推导，并证明其正确性。

3 基于格的高效实用 IBE 方案

BFRS 算法是基于 R-SIS 和 R-LWE 问题构建的 IBE 加密机制，其效率甚至优于基于 NTRU 格所构建的 IBE 的方案。然而，BFRS 算法的效率还有待提高，并且 BFRS 算法的明文空间较小，仅有 $\{0,1\}^n$，该算法在最低安全环境下仅能达到 1∶1696 的密文膨胀率，即每加密 1 kB 的明文就会产生约 1.656 MB 的密文，对于传统的加解密而言不具有实用性。针对以上问题，本文对 BFRS 算法进行了改进。

3.1 分块复用技术

本节基于 LWE 的多比特加密思想[18]，提出适用于 R-LWE 的分块加密技术。在一般的基于 LWE 问题的加密方案中，密文形式为 $(\boldsymbol{b},c)\in\mathbb{Z}_q^m\times\mathbb{Z}_q$，包含明文信息的密文形式为 $c=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+e'+M\cdot\lceil q/2\rfloor$，而辅助解密的密文 $\boldsymbol{b}=\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}$ 为一个向量。密文 $(\boldsymbol{b},\boldsymbol{c})$ 是一个 $m+1$ 维的向量，仅能对单个明文块 M 进行加密。为了降低密文膨胀率，可以利用同一个密文占比较大的 $\boldsymbol{b}$，一次同时对多个明文块进行加密：假设有明文组 $(M_1,\cdots,M_l)$，在产生公钥时随机采样一个矩阵 $\boldsymbol{U}=(\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l)\in\mathbb{Z}_q^{n\times l}$，对第 j 个明文信息加密 $c_j=\boldsymbol{u}_j^{\mathrm{T}}\boldsymbol{s}+e_j'+M_j\cdot q/2$，密文形式变为 $(\boldsymbol{b},c_1,\cdots,c_l)$，由此得到多比特加密方案。上述方案在公钥生成阶段采样 $\boldsymbol{U}$（具体安全性证明见第 3.3 小节）而非 $\boldsymbol{u}\in\mathbb{Z}_q^n$，是因为利用密文块作差后得到 $c_i-c_j=e_i'-e_j'+\lceil q/2\rfloor\cdot(M_i-M_j)$，由于 $e_i'-e_j'$ 很小，因此会泄露明文信息。在采样得到 $\boldsymbol{U}$ 后，针对每个 $\boldsymbol{u}_i\in\boldsymbol{U}$，都会相应产生一个私钥块 $\boldsymbol{x}_i$，满足 $\boldsymbol{A}\boldsymbol{x}_i=\boldsymbol{u}_i$。随着参数 l 的增大，密文膨胀率将降低，但是私钥尺寸会膨胀 l 倍。

类似地，LWE 的多比特加密思想可以向 R-LWE 推广：BFRS 方案中密文形式为 $(\boldsymbol{b},c)\in R_q^m\times R_q$，为了降低密文膨胀率，基于多比特加密思想，利用分块复用技术重用向量 $\boldsymbol{b}$，牺牲较小的私钥尺寸，在不泄露更多信息的情况下尽量还原出更多的密文。分块复用技术在本方案运用的安全性将在 3.3 节的 Game 3 中进行分析。本文中分块复用参数为 l，其大小取值详见第 3.6 节。

3.2 方案构造

本节直接将压缩技术与分块复用技术与 BFRS 算法结合，同时引入明文扩张参数 dp[40]，形成新方案。基于格的高

效实用 IBE 方案中系统基本参数 n,m,k,q，压缩参数 d_b 和 d_c，以及分块复用参数 l 为整数；σ,α,τ,ζ 为实数。

(1) $NEW\text{-}Setup(1^n)\rightarrow(mpk,msk)$

输入：初始化参数 1^n。

1) 调用 $(\boldsymbol{a},\boldsymbol{T})\leftarrow BFRS\text{-}TrapGen(q,\sigma,h=0)$ 算法，首先对陷门和随机多项式进行采样 $\boldsymbol{T}\leftarrow D_{R_q^{(m-k)k},\sigma}$，$\boldsymbol{a}''\leftarrow U(R_q^{m-k-1})$，令 $\boldsymbol{a}'=(1,\boldsymbol{a}'')\in R_q^{m-k}$，再计算出 $\boldsymbol{a}=(\boldsymbol{a}'|-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{T})^{\mathrm{T}}\in R_q^m$。

2) 根据密文分块参数 l，进行 l 次随机采样 $u_i\leftarrow U(R_q)$，$i=1,\cdots,l$，得到 $\boldsymbol{u}=(u_1,\cdots,u_l)$。

输出：主公钥 $mpk=(\boldsymbol{a},\boldsymbol{u})\in R_q^{m+l}$ 和主私钥 $msk=\boldsymbol{T}\in R_q^{(m-k)k}$。

(2) $NEW\text{-}Extract(mpk,msk,id\in\boldsymbol{ID})\rightarrow sk_{id}$

输入：主公钥 mpk、主私钥 msk、身份 $id\in\boldsymbol{ID}$。

1) 计算出用户的身份标签 $h_{id}=\boldsymbol{H}(id)$。

2) 计算 $\boldsymbol{a}_{id}=\boldsymbol{a}^{\mathrm{T}}+(0|h_{id}\boldsymbol{g})^{\mathrm{T}}=(\boldsymbol{a}'|h_{id}\boldsymbol{g}-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{T})^{\mathrm{T}}$。

3) 利用 $\boldsymbol{x}_i\leftarrow BFRS\text{-}SamplePre(\boldsymbol{T},\boldsymbol{a}_{id},h_{id},\zeta,\sigma,\alpha,u_i)$ 算法依次对 l 维的用户私钥采样，满足条件 $\boldsymbol{a}_{id}^{\mathrm{T}}\boldsymbol{x}_i=u_i$。

输出：私钥 $sk_{id}=\boldsymbol{x}=(\boldsymbol{x}_1,\cdots,\boldsymbol{x}_m)$。

(3) $NEW\text{-}Encrypt(mpk,id,(M_1,\cdots,M_l)\in R_{2^{dp}}^l)\rightarrow C$

输入：主公钥 mpk、用户身份 id、明文。

1) 如 $NEW\text{-}Extract$ 算法所示，计算用户标签 h_{id} 和 $\boldsymbol{a}_{id}$。

2) 采样 $s\leftarrow U(R_q)$，$\boldsymbol{e}\leftarrow D_{R_q^m,\tau}$ 和 $e_i\leftarrow D_{R_q,\tau}$，$i=1,\cdots,l$。

3) 分别计算 $\boldsymbol{b}=\boldsymbol{a}_{id}s+\boldsymbol{e}\in R_q^m$ 和 $c_i=u_i\cdot s+e_i+\lceil q/2^{dp}\rfloor M_i$，$i=1,\cdots,l$。

4) 利用压缩算法对密文进行压缩 $\boldsymbol{b}=Compress(\boldsymbol{b},d_b,q)$，$c_i=Compress(c_i,d_c,q)$，得到 $\boldsymbol{c}=(c_1,\cdots,c_l)$。

输出：密文 $C=(\boldsymbol{b},\boldsymbol{c})\in R_q^{m+l}$。

(4) $NEW\text{-}Decrypt(sk_{id},C)\rightarrow(M_1',\cdots,M_l')$

输入：私钥 sk_{id}、密文 C。

1) 对密文参数进行解压：$\boldsymbol{b}'=Decompress(\boldsymbol{b},d_b,q)$ 和 $c_i'=Decompress(c_i,d_c,q)$。

2) 逐块计算解密结果：$res_i=c_i'-\boldsymbol{b}'^{\mathrm{T}}\boldsymbol{x}_i\in R_q$，得到 $M_i'=Compress(res_i,dp,q)$。

输出：$(M_1',\cdots,M_l')$。

3.3 安全性分析

本节将证明本文方案在 R-SIS 和 R-LWE 假设下是 IND-sID-CPA 安全的。其中用 $Adv_{\mathrm{NEW.CPA}}^{\mathrm{IND\text{-}sID\text{-}CPA}}[\mathcal{A}]$ 表示本方案中敌手所具有的优势。

定理 2 令 $\Delta=R_q^m$，如果 $R\text{-}SIS_{q,m,\zeta}$ 与 $Decision\text{-}RLWE_{n,q,D_{\Delta,\tau}}$ 困难问题成立，新方案在选择敌手的选择明文攻击下是 IND-sID-CPA 安全的，并且本方案敌手的优势满足：$Adv_{\mathrm{NEW.CPA}}^{\mathrm{IND\text{-}sID\text{-}CPA}}[\mathcal{A}]\leqslant Adv_{q,m,\zeta}^{\mathrm{R\text{-}SIS}}[\mathcal{A}]+Adv_{n,q,D_{\Delta,\tau}}^{\mathrm{R\text{-}LWE}}[\mathcal{A}]+negl(\lambda)$。

证明：本文将通过一组游戏序列证明定理 2，总共进行 4 轮游戏。由于前 3 轮游戏已经有详细的论证过程[21]，本文只给出简单证明。在第 4 个游戏中，主要证明了采用分块复用技术后，不会因增加带明文信息的密文参数而降低方案的安全性。

Game 0 敌手与具有 IND-sID-CPA 能力的挑战者进行一轮 IND-sID-CPA 的 IBE 安全游戏。其中主公钥 $mpk=(\boldsymbol{a},\boldsymbol{u})$、主私钥 $msk=\boldsymbol{T}$ 由算法 $BFRS\text{-}TrapGen(q,\sigma,h=0)$ 产生，因此 $\boldsymbol{a}=(\boldsymbol{a}'^{\mathrm{T}}|-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{T})^{\mathrm{T}}$，$\boldsymbol{u}\in R_q^l$ 为一个均匀随机的多项式向量。在 Game 0 中敌手具有的优势为 $Adv_{\mathrm{Game\ 0}}[\mathcal{A}]=Adv_{\mathrm{IBE}}^{\mathrm{IND\text{-}sID\text{-}CPA}}[\mathcal{A}]=\left|\Pr[b=b^*]-\frac{1}{2}\right|$[21]。

Game 1 在第 2 轮游戏中，通过添加挑战身份 id^* 生成主公、私钥对。公钥参数 A 通过调用算法 $BFRS\text{-}TrapGen(q,\sigma,h=-h_{id^*})$ 生成，因此 $\boldsymbol{a}=(\boldsymbol{a}'^{\mathrm{T}}|-h_{id^*}\boldsymbol{g}-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{T})^{\mathrm{T}}$。当 $\mathcal{A}$ 询问身份 $id\neq id^*$ 时，挑战者必须回应敌手 $\mathcal{A}$ 的询问：$\boldsymbol{a}_{id}=\boldsymbol{a}^{\mathrm{T}}+(0|h_{id}\boldsymbol{g})=(\boldsymbol{a}'^{\mathrm{T}}|(h_{id}-h_{id^*})\boldsymbol{g}-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{T})^{\mathrm{T}}$。因为 $h_{id}-h_{id^*}$ 可逆，调用算法 $BFRS\text{-}SamplePre(\boldsymbol{T},\boldsymbol{a}_{id},h_{id}-h_{id^*},\zeta,\sigma,\alpha,u_i)$ 依次生成私钥 $\boldsymbol{x}_i$，满足 $\boldsymbol{a}_{id}^{\mathrm{T}}\boldsymbol{x}_i=u_i$，其中 $i=1,\cdots,l$。当 $id=id^*$ 时，$\boldsymbol{a}=(\boldsymbol{a}'^{\mathrm{T}}|-\boldsymbol{a}'^{\mathrm{T}}\boldsymbol{T})^{\mathrm{T}}$ 由 RLWE 假设保证其与从随机分布选取的多项式向量 $\boldsymbol{d}\sim R_q^m$ 计算不可区分，即证明了 A 不能通过 G-陷门得到任何关于指定身份的私钥信息，只能转而求解 $R\text{-}SIS_{q,m,\zeta}$ 问题。因此得到 Game 0 与 Game 1 的优势差为 $|Adv_{\mathrm{Game\ 1}}[\mathcal{A}]-Adv_{\mathrm{IBE}}^{\mathrm{IND\text{-}sID\text{-}CPA}}[\mathcal{A}]|\leqslant Adv_{q,m,\zeta}^{\mathrm{R\text{-}SIS}}[\mathcal{A}]$。

Game 2 第 3 轮游戏中，在 Game 1 的基础上改变 A 需要辨识的密文的生成方式。在采用分块复用技术前的构造中，密文形式为 $C^*\leftarrow R_q^m\times R_q$ 或 $C^*=(\boldsymbol{b}=\boldsymbol{a}_{id}s+\boldsymbol{e},\boldsymbol{c})$，其中 $C^*=(\boldsymbol{b}=\boldsymbol{a}_{id}\cdot s+\boldsymbol{e},\boldsymbol{c})$ 是一个满足近似均匀分布的样本[15]，挑战密文从直观上来说也是均匀的。因此 $\mathcal{A}$ 最后要么输出一个猜想 $\boldsymbol{b}\in\{0,1\}$，则仅有二分之一的概率猜测成功，要么 $\mathcal{A}$ 转而求解 $Decision\text{-}RLWE_{n,q,D_{\Delta,\tau}}$ 问题。因此得出 Game 2 与 Game 1 的优势差为 $|Adv_{\mathrm{Game\ 2}}[\mathcal{A}]-Adv_{\mathrm{Game\ 1}}[\mathcal{A}]|\leqslant Adv_{n,q,D_{\Delta,\tau}}^{\mathrm{R\text{-}LWE}}[\mathcal{A}]$。

Game 3 在 Game 2 中已经证明了生成密文 $(\boldsymbol{b}^*,c^*)$ 在 $\mathcal{A}$ 攻击下的安全性。在 Game 3 中，考虑将 Game 2 中生成的密文块进行更改 $(\boldsymbol{b}^*,c_1^*,\cdots,c_l^*)$，即完全与本文提出的新方案一致，因此 $Adv_{\mathrm{NEW.CPA}}^{\mathrm{IND\text{-}sID\text{-}CPA}}[\mathcal{A}]=Adv_{\mathrm{Game\ 3}}[\mathcal{A}]$，其中：

$$c_1^*=u_i\cdot s+e_1+\lfloor q/2\rfloor M_1$$

$$\cdots$$

$$c_l^*=u_l\cdot s+e_l+\lfloor q/2\rfloor M_l$$

将其中任意两个密文块 c_i^* 与 c_j^* 作差得到：$c_i^*-c_j^*=(u_i-u_j)\cdot s+(e_i-e_j)+\lfloor q/2\rfloor(M_i-M_j)$。

已知 u_i 和 u_j 独立同分布、e_i 和 e_j 独立同分布，由各个分量的独立性可以得到其任意线性组合 (u_i-u_j) 和 (e_i-e_j) 仍然是独立同分布的。因此，敌手不可能从多出的密文参数中得到任何关于明文的信息，进而得到优势差：$|Adv_{\mathrm{Game\ 3}}[\mathcal{A}]-Adv_{\mathrm{Game\ 2}}[\mathcal{A}]|\leqslant negl(\lambda)$。

综上，可以得到 $Adv_{\mathrm{NEW.CPA}}^{\mathrm{IND\text{-}sID\text{-}CPA}}[\mathcal{A}]\leqslant Adv_{q,m,\zeta}^{\mathrm{R\text{-}SIS}}[\mathcal{A}]+Adv_{n,q,D_{\Delta,\tau}}^{\mathrm{R\text{-}LWE}}[\mathcal{A}]+negl(\lambda)$。因此，在 $R\text{-}SIS_{q,m,\zeta}$ 和 $Decision\text{-}RLWE_{n,q,D_{\Delta,\tau}}$ 问题是困难的前提下，本文的公钥加密方案可证明是 IND-sID-CPA 安全的。

3.4 正确性分析

本节参数与第 3.2 节所示方案参数一致，设对密文 $\boldsymbol{b}$ 以及第 i 个密文块 c_i 调用 $Compress$ 和 $Decompress$ 后，产生的误差分别为：$\boldsymbol{c}_b=\boldsymbol{b}'-\boldsymbol{b}$，$c_c=c_i'-c_i$。

定理 3 1) 解密密文块 c_i 时产生的误差为 $\varepsilon=(c_c+e_i)-$

$(\boldsymbol{c}_b+\boldsymbol{e}^{\mathrm{T}})\cdot\boldsymbol{x}_i$；2)当误差的范数$\|\varepsilon\|$与本文算法中的模数$q$和明文扩张参数$dp$满足以下关系时，则能够保证本文算法的正确性。

$$\Pr\left(\|\varepsilon\|<\frac{q}{2^{dp+1}}\right)>1-negl(\lambda) \tag{5}$$

证明：结合本文算法，利用压缩技术先压缩再解压得到：

$$\boldsymbol{b}'=Decompress(\boldsymbol{b},q,d_b)=\boldsymbol{a}_{id}\cdot s+\boldsymbol{e}+\boldsymbol{c}_b$$

$$c_i'=Decompress(c_i,q,d_c)=u_i\cdot s+e_i+\left\lceil\frac{q}{2^{dp}}\right\rfloor\cdot M_i+c_c$$

因此在解密时，得到：

$$\begin{aligned}res_i&=c_i'-\boldsymbol{b}'^{\mathrm{T}}\boldsymbol{x}_i\\&=u_i\cdot s+e_i+\left\lceil\frac{q}{2^{dp}}\right\rfloor\cdot M_i+c_c-\boldsymbol{a}_{id}^{\mathrm{T}}\boldsymbol{x}_i\cdot s-(\boldsymbol{e}^{\mathrm{T}}+\boldsymbol{c}_b^{\mathrm{T}})\boldsymbol{x}_i\\&=\left\lceil\frac{q}{2^{dp}}\right\rfloor\cdot M_i+(e_i+c_c)-(\boldsymbol{e}^{\mathrm{T}}+\boldsymbol{c}_b^{\mathrm{T}})\boldsymbol{x}_i\end{aligned}$$

由此，定理3的1)得证。

又有$M'=Compress(res_i,q,dp)$，如果要解密得到$M_i'=M_i$，必须满足条件：$\|M_i'-M_i\|=\|\varepsilon\|\cdot\lceil 2^{dp}/q\rfloor<\frac{1}{2}$，即做相应变换后满足式(5)，由此定理3的2)得证，定理3证毕。

3.5 复杂度分析

本节分析了新方案在加解密时的时间复杂度和空间复杂度，以下描述的所有参数均与前文保持一致。假设对一个多项式的明文进行加密，总共的比特位数为$n\times dp\times l$。在整个加解密过程中主要消耗的计算量是在噪声的产生以及多项式乘法，其他计算的计算复杂度可以忽略不计。由于在格点上高斯采样得到一个噪声多项式的时间复杂度为$O(n)$，一次多项式乘法的时间复杂度为$O(n\log n)$，本文空间复杂度为调用一次多项式乘法所消耗的空间$O(n)$。因此，结合本文算法可以得到复杂度分析表，如表2所列。

表2 新算法的计算复杂度分析

Table 2 Analysis of computational complexity of our scheme

Algorithm stages	Time complexity	Space complexity
Encryption operation	$O((m+l)\cdot(n\log n+2n))$	$O(n)$
Decryption operation	$O(m\cdot l\cdot n\log n)$	$O(n)$

3.6 参数取值

本文将综合考虑误差大小、密文膨胀率以及加解密效率，以得到较优的参数组合。

(1)密文膨胀率

定理4 设密文膨胀率为ρ，压缩参数和明文扩张参数分别为d_b，d_c和dp(同第3.2节所示参数)，则密文膨胀率的计算公式为：

$$\rho\approx\frac{d_b\cdot m+d_c\cdot l}{dp\cdot l} \tag{6}$$

证明：$M\in R_2^{dp}$，因此明文多项式M由n个小于2^{dp}的整数组成，密文$\boldsymbol{b}=Compress(\boldsymbol{b},d_b,q)$由$m\cdot n$个小于$2^{d_b}$的整数组成，每个密文块$c_i=Compress(c_i,d_c,q)$是由$n$个小于$2^{d_c}$的整数组成，总共有$l$个密文块，将$d_b$，$d_c$和$dp$看成比特位数，可以得到以下推导式：

$$\rho\approx\frac{d_b\cdot n\cdot m+d_c\cdot n\cdot l}{dp\cdot n\cdot l}=\frac{d_b\cdot m+d_c\cdot l}{dp\cdot l}$$

由此定理4得证。

(2)误差分析

为了保证解密的正确性，要对本文误差进行分析，必须先计算误差的各个分量分布。

首先在R上定义分布ψ_d：随机选取$y\leftarrow R_q$，计算压缩与解压后产生的误差$err=(y-Decompress(Compress(y,d,q),d,q))\bmod^{\pm}q$，满足分布$\psi_d$。根据Kyber的工作，$|err|\leqslant B_q=\lceil q/2^{d+1}\rfloor$，且$\psi_d$近似均匀分布。因此，满足分布$\psi_d$的多项式的各项系数满足期望为0，方差为$\frac{B_q^2}{3}$。

设解密c_i密文块的误差$\varepsilon=(c_c+e_i)-(\boldsymbol{c}_b^{\mathrm{T}}+\boldsymbol{e}^{\mathrm{T}})\cdot\boldsymbol{x}_i$(见定理3)。$\varepsilon$由满足两种不同类型的分布的多项式计算得到，分别为：

$$(\boldsymbol{e},e_i,\boldsymbol{x}_i)\leftarrow D_{R_q^m,\tau}\times D_{R_q,\tau}\times D_{R_q^m,\zeta}$$

$$(c_c,\boldsymbol{c}_b)\leftarrow\psi_{d_c}\times\psi_{d_b}^m$$

令$B_{q,c}=\left\lceil\frac{q}{2^{d_c+1}}\right\rfloor$与$B_{q,b}=\left\lceil\frac{q}{2^{d_b+1}}\right\rfloor$，得到$(c_c+e_i)$和$(\boldsymbol{c}_b+\boldsymbol{e})$，计算结果的各项系数满足期望为0，方差分别为$\frac{B_{q,c}^2}{3}+\tau$和$\frac{B_{q,b}^2}{3}+\tau$。结合定理1，可得$(\boldsymbol{c}_b^{\mathrm{T}}+\boldsymbol{e}^{\mathrm{T}})\cdot\boldsymbol{x}_i$的系数满足$N\left(0,m\cdot n\cdot\zeta\cdot\left(\frac{B_{q,b}^2}{3}+\tau\right)\right)$的近似高斯分布。

根据定理3，为了保证算法的正确性，误差的范数必须满足$\|\varepsilon\|=\|(c_c+e_i)-(\boldsymbol{c}_b^{\mathrm{T}}+\boldsymbol{e}^{\mathrm{T}})\cdot\boldsymbol{x}_i\|<\lceil q/2^{dp+1}\rfloor$，由此可得本方案各个参数应满足的关系：

$$t\cdot\sqrt{m\cdot n\cdot\zeta\cdot\left(\frac{B_{q,b}^2}{3}+\tau\right)}+\left(\frac{B_{q,c}^2}{3}+\tau\right)<\frac{q}{2^{dp+1}} \tag{7}$$

(3)参数设置

为了保证方案的安全性，本文选取的参数与BFRS方案一致，参数的设置分为3个安全等级，如表3所列。其中，λ为安全参数，m为多项式向量的维数，参数$k=m-2$，σ和τ分别为BFRS-TrapGen和噪声采样的高斯参数，ζ为私钥的高斯参数。

表3 本文方案的基础参数设置

Table 3 Basic parametersset for our scheme

λ	n	m	k	σ	ζ	τ
40	512	52	50	3.3	1935.7	3.3
80	1024	53	51	5	6360.5	5
195	2048	64	62	6.7	19898.5	6.7

在标准正态分布中，随机变量大于8倍标准差的概率为$2^{-49.6}$，可以忽略不计。同时经过测试参数l取值为7时较优，再由上文给出的式(7)，结合Maple数值实验得到本文新增压缩参数和明文扩张参数d_b，d_c和dp的优化取值以及本文密文膨胀率ρ(由式(6)计算得到)，具体取值如表4所列。

表4 本文方案的压缩参数取值

Table 4 New parametersset for our scheme

(λ,n)	dp	d_b	d_c	ρ
(40,512)	15	25	25	14.1
(80,1024)	13	27	27	17.8
(195,2048)	12	30	30	23.7

4 实验结果及分析

4.1 实验环境

本文方案的所有测试结果均在具有 6 核 Intel Core i7-8850H CPU 且频率为 2.6GHz 的 Macbook Pro 上运行得到，内存为 32GB，操作系统为 macOS Catalina 10.15.3。另外，采用的系统编译器 GCC 版本是 Apple clang 11.0.0（clang-1100.0.33.16）。为了方便对文件进行操作，本文程序是在具有标准文件库的 C++17 标准下实现的。整个实验使用了“-O2”参数进行编译优化，对时钟周期的测量采用的是 C++11 标准中的“high_resolution_clock”类。由于 GM 中采样算法对系统扰动可以并行求解得到，因此本文在实现 NEW-Extract 算法时使用了 C++标准库的〈thread〉模块优化，其他加密解密部分均采用单线程实现并测试。虽然 NTL 库中多项式乘法的效率不高，但本文仍选择其作为核心算法库进行测试，原因有两点：

(1)其针对大整数运算有很高的优化，支持任意大数的运算。

(2)NTL::ZZ_pX 类型具有足够的函数支持本方案环上的算数运算，如对多项式求模以及多项式乘法。在多项式乘法上，NTL 采用的是针对系数为大整数的 NTT 快速精确求解算法。

4.2 性能对比

测试的加密对象均为一个大小为 569 kB 的 pdf 文件，分别记录下加解密的时间后，取稳定的时间（多次测量，去掉偏差较大的数据后取平均值得到的结果）计算出实际速率。将加解密速率、密文膨胀率、明文大小、密文大小、加密平均时间、解密平均时间分别用 v_+，v_-，ρ，c_{ptxt}，c_{ctxt}，$\bar{t}_e$ 和 $\bar{t}_d$ 表示，计算公式如下：

$$v_+=\frac{c_{ptxt}}{\bar{t}_e},v_-=\frac{c_{ptxt}}{\bar{t}_d},\rho=\frac{c_{ctxt}}{c_{ptxt}}$$

本节将测试本文方案在第 3.6 节中给出的 3 种不同安全参数下的性能，主要包括加密速率、解密速率以及密文膨胀率，并与 BFRS 在相同参数下的测试结果进行对比。由于以下 4 点，本文重新实现 BFRS 算法并进行测试对比，对比结果如表 5 所列。1)BFRS 在程序实现的正确性上存在问题，解出的密文与原明文不一致；2)BFRS 采用 NFLib 库（针对环上的算数运算实现的高效算法库），该库对其参数 k 的取值有限制，测试时并非按照原表进行参数设置；3)BFRS 的程序实现并没有考虑实际加解密中的读写时间以及数据类型转化的时间等；4)两者的计算平台和环境存在差异。

BFRS 是基于 R-SIS 和 R-LWE 的 IBE 公钥加密方案，该方案的加解密效率虽然可以与基于 NTRU 格的 DLP[19] 和 MSO[20] 方案的效率相当，但是在实际加密中仍然无法达到实用标准，并且近千倍的密文膨胀率会消耗大量的空间资源。3 种安全场景下的对比测试中，本文方案在加密效率和解密效率上均远远优于 BFRS，其中本文方案对加密算法的优化程度更大，这是因为分块复用技术仅能在加密阶段复用解密辅助参数 $\boldsymbol{b}$，而在解密阶段 $\boldsymbol{b}$ 需要与相应的私钥 $\boldsymbol{x}_i$ 相乘，没有减少多项式的乘法次数。另外，本文在密文膨胀率方面也得到了极大提升。采用分块复用技术后，私钥尺寸成倍增大，然而，由于原本私钥存储开销小，因此牺牲私钥存储空间提升加密速率，并降低密文膨胀率是一种行之有效的方法。本文方案在测试时的密文膨胀率较表 4 所列的理论膨胀率偏大，是因为实现程序 IO 时是按照每个系数使用 int 类型大小存储数据，而实际系数所需内存均小于该大小，对 IO 接口改进后，基本能够达到理论计算的密文膨胀率大小。

表 5 3 种安全场景下本文算法与 BFRS 的性能对比

Table 5 Performance comparison between our scheme and BFRS in three different scenarios

(a)Encryption algorithm performance comparison

(λ,n)	v_+	
	Ours/(kB/s)	BFRS/(kB/s)
(40,512)	263.80	3.73
(80,1024)	217.97	3.57
(195,2048)	166.95	2.90

(b)Decryption algorithm performance comparison

(λ,n)	v_-	
	Ours/(kB/s)	BFRS/(kB/s)
(40,512)	80.16	3.58
(80,1024)	65.91	3.43
(195,2048)	48.94	2.77

(c)Ciphertext expansion rate comparison

(λ,n)	ρ	
	Ours	BFRS
(40,512)	18.10	1696.08
(80,1024)	21.20	1728.08
(195,2048)	27.60	2080.57

另外需要说明的是，本文得到的时间均考虑了实际的加密状态，即加密时间包括对公钥的读取、方案的加密算法、数据类型转化以及写入密文的时间，而解密时间则包括私钥的读取、解密算法、数据类型转化以及写入明文的时间。

结束语 本文针对一种基于 R-SIS 和 R-LWE 问题的 IBE 加密方案进行了改进，提出了分块复用技术，再结合 Kyber 的压缩算法，同时引入明文扩张参数，构建了能够用于一般物联网加密的 IBE 新方案。本文通过理论分析论证了本文方案的正确性、安全性，得到了计算复杂度，利用数值实验给出了优化参数取值。本文通过 NTL 库实现了所提方案，将其性能与原方案进行对比，结果表明所提方案提高了加解密效率，同时有效降低了密文膨胀率，体现出较好的实用性。然而，分块复用技术带来的性能提升会导致私钥尺寸膨胀。本文的分块复用技术以及对压缩算法的运用可以为其他类似的格加密算法优化提供参考思路。

本文方案达到了轻量级要求。以 $\lambda=80$ 为例，明文空间为 $\{0,1,\cdots,2^{13}-1\}$，多项式的每一项系数可以放入 13 位的二进制明文信息，一个多项式能放入 1664 字节的明文，能够保证一个多项式装入物联网设备必要的密钥交换内容。假设使用 AES-128 对称加密算法加密，密钥交换内容的大小为 16 字节，仅用一个明文多项式便可装入，则生成的密文仅占 284.8 字节，密文膨胀率控制在 20 倍以内，加密耗时 375.47 ms，解密耗时 1379.71 ms，符合轻量级密码的实用性

需求。5G 的数据传输速率是 4G 的 100 倍，因此 20 倍膨胀率在 5G 的传输速率下是能够容忍的。

后续研究工作如下：1)将进一步提升本文方案的安全性，达到自适应安全；2)有望构建一个基于模容错学习问题(M-LWE)的 IBE 方案，以大幅提高加解密效率。

参 考 文 献

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

[2] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C]// Proceedings of CRYPTO 2001. Berlin: Springer, 2001: 213-229.

[3] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. Siam Journal on Computing, 1997, 26(5): 1484-1509.

[4] YOU I, HORI Y, SAKURAI K. Enhancing SVO Logic for Mobile IPv6 Security Protocols [J]. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2011, 2(3): 26-52.

[5] COCKS C. An identity based encryption scheme based on quadratic residues[C]// Proc of Cryptography and Coding. Berlin: Springer, 2001: 360-363.

[6] AJTAI M. Generating hard instances of lattice problems[C]// Proceedings of STOC. 1996: 99-108.

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

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

[9] STEHLE D, STEINFELD R, TANAKA K, et al. Efficient public key encryption based on ideal lattices[C]// Proceedings of ASIACRYPT. Berlin, Heidelberg: Springer, 2009: 617-635.

[10] BABAI L. On Lovász' lattice reduction and the nearest lattice point problem [J]. Combinatorica, 1986, 6(1): 1-13.

[11] KLEIN P. Finding the closest lattice vector when it's unusually close[C]// Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms. 2000: 937-941.

[12] 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.

[13] PEIKERT C. An efficient and parallel Gaussian sampler for lattices[C]// Annual Cryptology Conference. Berlin, Heidelberg: Springer, 2010: 80-97.

[14] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: Simpler, tighter, faster, smaller [C] // Proceedings of EUROCRYPT 2012. Berlin: Springer, 2012: 700-718.

[15] GENISE N, MICCIANCIO D. Faster gaussian sampling for trapdoor lattices with arbitrary modulus[C]// Proceedings of EUROCRYPT. Cham: Springer, 2018: 174-203.

[16] GENISE N, MICCIANCIO D, POLYAKOV Y. Building an efficient lattice gadget toolkit: Subgaussian sampling and more [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2019: 655-684.

[17] CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate a lattice basis[C]// Proceedings of EUROCRYPT 2010. Berlin: Springer, 2010: 523-552.

[18] AGRAWAL S, BONEH D, BOYEN X. Efficient lattice(H) IBE in the standard model[C]// Proceedings of EUROCRYPT 2010. Berlin: Springer, 2010: 553-572.

[19] DUCAS L, LYUBASHEVSKY V, PREST T. Efficient identity-based encryption over NTRU lattices[C]// Proceedings of ASIACRYPT 2014. Berlin: Springer, 2014: 22-41.

[20] MCCARTHY S, SMYTH N, O'SULLIVAN E. A practical implementation of identity-based encryption over NTRU lattices [C]// Proceedings of IMACC. Cham: Springer, 2017: 227-246.

[21] BERT P, FOUQAUE P A, ROUX-LANGLOIS A, et al. Practical implementation of ring-SIS/LWE based signature and IBE [C]// Proceedings of PQCrypto. Cham: Springer, 2018: 271-291.

[22] YAMADA S. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters[C]// Proceedings of EUROCRYPT 2016. Berlin: Springer, 2016: 32-62.

[23] SINGH S, PADHYE S. Identity based blind signature scheme over NTRU lattices [J]. Information Processing Letters, 2020, 155: 105898.

[24] LU X, WEN Q, YIN W, et al. Quantum-Resistant Identity-Based Signature with Message Recovery and Proxy Delegation [J]. Symmetry, 2019, 11(2): 272.

[25] ZHANG Y, GAN Y, YIN Y, et al. Fuzzy Identity-Based Signature from Lattices for Identities in a Large Universe [C]// International Conference on Cloud Computing and Security. Cham: Springer, 2018: 573-584.

[26] KATSUMATA S, MATSUDA T, TAKAYASU A. Lattice-based revocable(hierarchical) IBE with decryption key exposure resistance [J]. Theoretical Computer Science, 2020, 809: 103-136.

[27] ZHANG Y, WANG S, DU Q. Revocable identity-based encryption scheme under LWE assumption in the standard model [J]. IEEE Access, 2018, 6: 65298-65307.

[28] SRIVASTAVA G, AGRAWALG R, SINGH K, et al. A hierarchical identity-based security for delay tolerant networks using lattice-based cryptography [J]. Peer-to-Peer Networking and Applications, 2020, 13(1): 348-367.

[29] DONG C, YANG K, QIU J, et al. Outsourced revocable identity-based encryption from lattices [J]. Transactions on Emerging Telecommunications Technologies, 2019, 30(11): e3529.

[30] ZHANG X, TANG Y, WANG H, et al. Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage [J]. Information Sciences, 2019, 494: 193-207.

[31] ZHANG X，XU C，MU L，et al. Identity-based encryption with keyword search from lattice assumption [J]. China Communications，2018，15(4)：164-178.

[32] ZHU H，TAN Y，ZHU L，et al. An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks [J]. Sensors，2018，18(5)：1663.

[33] REGEV O. Lecture 1 Intriduction [EB/OL]. Tel Aviv University，2004 [2020-03-28]. https：//cims. nyu. edu/～regev/teaching/lattices_fall_2004/ln/introduction. pdf.

[34] LIU Y，WANG L C，LI L X，et al. Secure and Efficient Multi-Authority Attribute-Based Encryption Scheme From Lattices [J]. IEEE Access，2019，7：3665-3674.

[35] LYUBASHEVSKY V，MICCIANCIO D. Generalized compact knapsacks are collision resistant [C]// Proceedings of ICALP. Berlin，Heidelberg：Springer，2006：144-155.

[36] PEIKERT C，ROSEN A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices [C]// Proceedings of TCC. Berlin，Heidelberg：Springer，2006：145-166.

[37] 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，Heidelberg：Springer，2010：1-23.

[38] AJTAI M. Generating hard instances of the short basis problem [C]// Proceedings of Int Colloquium on Automata，Languages and Programming. Berlin：Springer，1999：1-9.

[39] BOS J，DUCAS L，KILTZ E，et al. CRYSTALS-Kyber：a CCA-secure module-lattice-based KEM [C] // Proceedings of EuroS&P. IEEE，2018：353-367.

[40] KE C S，WU W Y，FENG Y. Low expension rate of encryption algorithm based on MLWE [J]. Computer Science，2019，46(4)：144-150.

QIAN Xin-yuan，born in 1995，postgraduate. His main research interests include information security，lattice cryptography，IBE and ABE.

WU Wen-yuan，born in 1976，Ph.D，professor. His main research interests include automated reasoning，hybrid computing and lattice cryptography.