NTRU 格上无证书加密

陈 虎* 胡予濮
(西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)

摘 要：为降低密钥尺寸，利用陷门抽样算法在优选的 NTRU 格上抽取部分私钥并使用多项式环上带误差的学习问题计算公钥等方法来构造格上无证书加密方案。它的安全性基于多项式环上带误差学习的判定问题和小多项式比判定问题等两个困难问题假设。为获取更好的效率，该文还提出一个无证书并行加密方案。该方案用中国剩余定理分解扩大后的明文空间为多个不同素理想之积来实现并行加密。它还用中国剩余定理分解加密运算所在的多项式环获取中国剩余基来优化算法，使算法只涉及整数间运算。结果显示该方案具有计算和通信复杂度低等特点。

关键词：无证书密码系统；格密码；环上带误差的学习问题；判定小多项式比问题
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2016)02-0347-07
DOI: 10.11999/JEIT150380

Certificateless Encryption over NTRU Lattices

CHEN Hu HU Yupu
(*State Key Laboratory of Integrated Service Networks*, *Xidian University, Xi'an* 710071, *China*)

Abstract: To lower the sizes of keys, a certificateless encryption scheme is put forward by using a trapdoor sampling algorithm over a selected NTRU lattice to extract partial private keys and using Ring Learning With Errors (RLWE) problem to generate public keys. Its security is based on both assumptions of the decisional ring learning with errors problem and the decisional Small Polynomial Ratio (SPR) problem. To further improve efficiency, a certificateless parallel encryption scheme with more efficient algorithms only using arithmetic in integers is also given by respectively using the Chinese Remainder Theorem (CRT) to decompose the enlarged plaintext space into the product of distinct prime ideals and to break down the ring, over which encryption operations work, for obtaining the Chinese Remainder basis. The given results show that the proposed schemes are characterized by low computation complexity and small communication complexity.

Key words: Certificateless cryptosystem; Lattice cryptography; Ring Learning With Errors (RLWE) problem; Decisional Small Polynomial Ratio (SPR) problem

1 引言

格公钥密码以具有抗量子计算攻击和存在从最差到平均情况的安全归约等特性成为竞相研究的热点。富含新颖独特应用场景的格密码方案[1–3]似春笋般涌现，尤其是从格上构造出全同态加密[4–6]以来格密码更是人们关注的焦点。然而格密码独特优势[7]仍难掩其空间开销大的弱点。致力于降低格公钥密码尺寸的成果[3,6–9]层出不穷，其中文献[3,8,9]不约而同地把目光聚焦在NTRU格上寻求突破口。特别是文献[3]选择在一类特殊的分圆多项式环中构造具有小尺寸陷门基的NTRU格，这在离散高斯抽样中具有重要意义。同时借助NTRU格的公开基和陷门基组成矩阵的结构特点极大地压缩了存储空间。而文献[10,11]在降低格密码存储空间时另辟蹊径地采用了在无证书体制[12–14]下构造格上的加密方案。遗憾地，他们只单方面地利用无证书体制不涉及证书管理和以身份作为公钥等优势来降低公钥尺寸。因为他们用文献[15]中陷门生成算法导致格的维数 $m > 6n\log_2 q$，所以公钥尺寸仍很大且方案效率不高。

本文在NTRU格上给出了一个无证书加密方案。它以多项式环上带误差学习(RLWE)[16]的判定问题和小多项式比(SPR)[17]判定问题为基础，并在随机预言模型下证明是语义安全的。受文献[14]的启发，加强了攻击者的能力[13](见第3节)。为缩小用户

收稿日期：2015-04-01；改回日期：2015-11-13；网络出版：2016-01-04
通信作者：陈虎 chenhuchh@163.com
基金项目：国家自然科学基金(61472309, 61173151)，安徽省自然科学基金(1208085MF108, KJ2012B157)
Foundation Items: The National Natural Science Foundation of China (61472309, 61173151), The Natural Science Foundation of Anhui Province (1208085MF108, KJ2012B157)

公私钥尺寸，本文采用四轮驱动的方式来实现。首先，部分地依托无证书体制的优势，部分地依靠文献[3]中小尺寸陷门生成方法来降低高斯抽样中的偏差和部分地凭借NTRU格的公开基和陷门基自身的结构特点进一步压缩了它们的存储空间。其次，本文中用户秘密值和公钥生成算法简单自然。用户的秘密值就作为RLWE问题的秘密多项式，公钥仅为该秘密值下的1个RLWE对。此外，本文还使用中国剩余定理进一步强化方案在密文扩展比和计算效率等方面的优势并给出方案。

2 背景知识

2.1 符号

设 n,m,q 为正整数，记 $[n]=\{0,1,\cdots,n-1\}$，$[m]_q=m \bmod q \in (-q/2,q/2]$，$\mathrm{poly}(n)$ 是 n 的任意多项式函数，$\mathrm{negl}(n)=o(1/\mathrm{poly}(n))$ 是一个可忽略的函数。$x \leftarrow X$ 是通配符，需按上下文来确定含义。若 X 为一个集合中的元素，则 $x \leftarrow X$ 表示把 X 赋值给 x；若 X 为一个集合，则 $x \leftarrow X$ 表示 x 是从 X 中均匀随机抽取；若 X 为随机变量的概率分布，则 $x \leftarrow X$ 表示 x 是以概率分布 X 抽取；若 X 为一个多项式时间的算法，则 $x \leftarrow X$ 表示 x 是算法 X 的输出。$\boldsymbol{a} \odot \boldsymbol{b}$ 表示两 n 维向量 $\boldsymbol{a},\boldsymbol{b}$ 对应分量相乘所得的 n 维向量。环 $\mathcal{R}=\mathbb{Z}[x]/(x^n+1)$，$\mathcal{R}_q=\mathcal{R}/q\mathcal{R}$，$q$ 为素数，$n=2^\kappa$，κ 为正整数。如下可逆函数可进行 $\mathcal{R}_q$ 与 $\mathbb{Z}_q^n$ 间元素互化。

定义 1 设 $a=\sum_{i\in[n]}a_i x^i \in \mathcal{R}_q$ 且 $a_i \in \mathbb{Z}_q$，定义 $\tau:\mathcal{R}_q \to \mathbb{Z}_q^n, a \mapsto \boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})^{\mathrm{T}}$。

令 $a=\sum_{j\in[n]}a_j x^j$，$\forall i \in [n]$，则有 $\tau(x^i a)=(-a_{n-i},-a_{n-i+1},\cdots,-a_{n-1},a_0,a_1,\cdots,a_{n-i-1})^{\mathrm{T}}$。用它可方便地表示反循环矩阵[3]，即 $\boldsymbol{M}_n(a)=(\tau(a),\tau(xa),\cdots,\tau(x^{n-1}a))^{\mathrm{T}}$。

2.2 NTRU 格及陷门基生成算法

定义 2[3] 设 $f,g \in \mathcal{R}$ 且 $h=g\cdot f^{-1} \in \mathcal{R}_q$，由 (h,q) 所确定的 $2n$ 维满秩格称为 NTRU 格，记为 $\Lambda_{h,q}=\{(u,v)\in\mathcal{R}^2 \mid u+vh=0 \bmod q\} \subseteq \mathbb{Z}^{2n}$，其一组公开基按行组成的矩阵为

$$\boldsymbol{A}_{h,q}=\begin{pmatrix}-\boldsymbol{M}_n(h) & \boldsymbol{I}_n \\ q\boldsymbol{I}_n & \boldsymbol{O}_n\end{pmatrix} \tag{1}$$

生成 NTRU 格陷门基的有效算法 $\mathrm{Trapdoor}_{\mathrm{NTRU}}(n,q)$ 详见文献[3]。设计方案时，要在 NTRU 格上进行离散高斯抽样[1]，并有如下结论。

引理 1[2] 设 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 的列向量生成 $\mathbb{Z}_q^n$，$\boldsymbol{T}$ 是格 $\Lambda^{\perp}(\boldsymbol{A})$ 的任一组基，对任意的 $\boldsymbol{y}\in\mathbb{Z}_q^n$ 和 $s \geq \|\widetilde{\boldsymbol{T}}\|\omega(\sqrt{\log_2 n})$，有

(1) $\Pr_{\boldsymbol{x}\leftarrow D_{\Lambda_{\boldsymbol{y}}^{\perp}(\boldsymbol{A}),s}}(\|\boldsymbol{x}\|>s\sqrt{m}) \leq \mathrm{negl}(n)$，其中 $D_{\Lambda_{\boldsymbol{y}}^{\perp}(\boldsymbol{A}),s}$ 表示给定 $\boldsymbol{y}\in\mathbb{Z}_q^n$ 并由式子 $\boldsymbol{y}=\boldsymbol{A}\boldsymbol{x} \bmod q$ 所确定的陪集 $\Lambda_{\boldsymbol{y}}^{\perp}(\boldsymbol{A})=\boldsymbol{x}+\Lambda^{\perp}(\boldsymbol{A})$ 上且以 s 为偏差的离散高斯概率分布。

(2)存在一个有效的算法 $\mathrm{SampleD}(\boldsymbol{A},\boldsymbol{T},\boldsymbol{y},s)$，样本 $\boldsymbol{x}\leftarrow\mathrm{SampleD}(\boldsymbol{A},\boldsymbol{T},\boldsymbol{y},s)$ 的分布与分布 $D_{\Lambda_{\boldsymbol{y}}^{\perp}(\boldsymbol{A}),s}$ 是计算不可区分的且满足 $\boldsymbol{y}=\boldsymbol{A}\boldsymbol{x} \bmod q$。

我们把上述算法应用到 NTRU 格 $\Lambda_{h,q}$ 上进行抽样，即抽取 $(\boldsymbol{e},\boldsymbol{d})\leftarrow\mathrm{SampleD}(h,\boldsymbol{T},(\boldsymbol{u},\boldsymbol{0}),\sigma)$，其中 $\boldsymbol{e},\boldsymbol{d}\in\mathbb{Z}_q^n$，输出 $(e,d)=(\tau^{-1}(\boldsymbol{e}),\tau^{-1}(\boldsymbol{d}))\in\mathcal{R}_q^2$，则有 $hd+e=u=\tau^{-1}(\boldsymbol{u})\in\mathcal{R}_q$ 且 $\|\tau(e)\|,\|\tau(d)\| \leq \sigma\sqrt{n}$。

下面说明 $hd+e=u=\tau^{-1}(\boldsymbol{u})$。由文献[1]中引理5.1知，对随机生成的 NTRU 格 $\Lambda_{h,q}$ 和任意给定的 $(\boldsymbol{u},\boldsymbol{0})\in\mathbb{Z}_q^{2n}$，存在 $(s,t)\in\mathcal{R}^2$ 满足 $s+th=\tau^{-1}(\boldsymbol{u}) \bmod q$ 以概率 $1-\mathrm{negl}(n)$ 成立。先求一组解 (s_0,t_0) 并记 $(\boldsymbol{s}_0,\boldsymbol{t}_0)=(\tau(s_0),\tau(t_0))$，则有 $s_0+t_0h=\tau^{-1}(\boldsymbol{u}) \bmod q$，再调用格上高斯抽样算法[1]获得 $(\boldsymbol{s}_1,\boldsymbol{t}_1)\in\mathbb{Z}_q^{2n}$，则有 $(\tau^{-1}(\boldsymbol{s}_1),\tau^{-1}(\boldsymbol{t}_1))\in\Lambda_{h,q}$，即 $\tau^{-1}(\boldsymbol{s}_1)+\tau^{-1}(\boldsymbol{t}_1)\cdot h=0 \bmod q$。把两式相加，则上述结论成立。

2.3 困难问题假设

判定 RLWE 问题假设就是该问题是不可区分的，并有从最差到平均情况的规约。

引理 2[4,5,16] 若 $\mathcal{R}_q=\mathbb{Z}_q[x]/(x^n+1)$，$n$ 为 2 的幂，素数 $q=\mathrm{poly}(n)$，$q\equiv 1 \bmod (2n)$，$r\geq\omega(\sqrt{\log_2 n})$，误差分布 $\chi=D_{\Lambda,r}$（其中 $\Lambda=\mathbb{Z}^n$），则存在一个从 $\mathcal{R}$ 中理想格的 SIVP (Shortest Independent Vectors Problem) 或 SVP (Shortest Vector Problem)问题到判定 RLWE 的随机化规约，其中近似因子为 $2^{\omega(\log_2 n)}(q/r)$。

存在一个从文献[16] 加密方案(Lyubashersky-Peikert-Regev Encryption，记为 LPR.E)到我们方案的规约。LPR.E 在判定RLWE问题假设下是语义安全的(INDistinguishable Chosen-Plaintext Attack, IND-CPA)，具体方案请参考文献[16]。

定义 3[17] 判定小多项式比(SPR)问题就是区分在 $\mathcal{R}_q$ 上的两种分布：

(1)均匀分布 $\mathcal{U}$：$h\leftarrow\mathcal{R}_q$；(2) 小多项式比分布 SPR：$h=g\cdot f^{-1}\in\mathcal{R}_q$，其中小多项式 $f,g\leftarrow\vartheta$ 且 f 在 $\mathcal{R}_q$ 上可逆，ϑ 为 $\mathcal{R}$ 的分布。

判定 SPR 问题假设就是两种分布是计算不可区分的。当 $\vartheta=D_{\mathbb{Z}^n,r}$ 且 $r>\mathrm{poly}(n)\sqrt{q}$ 时，判定 SPR 问题甚至对计算能力无界的区分算法都是不可区分的[5]。

2.4 中国剩余定理与中国剩余基

中国剩余定理[16] (CRT)可实现明文空间的分

解与聚合。它还可构造 $\mathcal{R}_q$ 的中国剩余基[18]($\mathbb{Z}_q-\mathrm{CRT}$)。因此，它对提高理想格上的方案效率很有帮助。

设分圆域 $K=\mathbb{Q}(x)/(\Phi_m(x))$，$p$ 为素数。对整环 $\mathcal{O}_K=\mathbb{Z}[x]/(\Phi_m(x))$ 中的理想 $\langle p\rangle=p\mathcal{O}_K$ 进行素理想分解。特别地，假设 $(p,m)=1$，$p^d\equiv 1 \bmod m$，则有

$$\Phi_m(x)=\prod_{i\in[\ell]} f_i(x) \bmod p \tag{2}$$

$f_i(x)$ 是 $\mathbb{Z}_p[x]$ 中 d 次不可约多项式。

据式(2)知：理想 $\langle p\rangle$ 具有如下分解式：

$\langle p\rangle=\prod_{i\in[\ell]}\boldsymbol{p}_i$，$\boldsymbol{p}_i=\langle p, f_i(\zeta)\rangle$ 是 $\mathcal{O}_K$ 中的素理想，其中 $\zeta=\exp(2\pi\sqrt{-1}/m)$。

据文献[16]中引理 2.12 知：

$$\mathbb{Z}_p[x]/(\Phi_m(x))\overset{\varphi}{\cong}\mathbb{Z}_p[x]/f_0(x)\times\cdots\times\mathbb{Z}_p[x]/f_{\ell-1}(x)\overset{\psi}{\cong}\left(\mathbb{F}_{p^d}\right) \tag{3}$$

定义 4 据式(3)中的同构映射设 ψ,φ，定义复合映射 $\mathrm{CRT}_p=\varphi\circ\psi$。

定义 5[18] 若 $\tilde{\boldsymbol{c}}=(c_i)_{i\in\mathbb{Z}_{2n}^*}$ 满足：当 $i=j$ 时，$c_i=1 \bmod \boldsymbol{p}_j$；否则，$c_i=0 \bmod \boldsymbol{p}_j$。称 $\tilde{\boldsymbol{c}}$ 为 $\mathcal{R}_q$ 的一组 $\mathbb{Z}_q-\mathrm{CRT}$。

引理 3[18] $c_ic_i=c_i\in\mathcal{R}_q$，$c_ic_j=0\in\mathcal{R}_q$，其中 $i,j\in\mathbb{Z}_{2n}^*$。

引入中国剩余基可更有效地实现 $\mathcal{R}_q$ 中的运算。如 $a,b\in\mathcal{R}_q$，它们在基 $\tilde{\boldsymbol{c}}$ 下的坐标分别为 $\boldsymbol{a},\boldsymbol{b}\in\mathbb{Z}_q^n$，即 $a=\langle\tilde{\boldsymbol{c}},\boldsymbol{a}\rangle$，$b=\langle\tilde{\boldsymbol{c}},\boldsymbol{b}\rangle$。据引理 3 知：$[ab]_q=\langle\tilde{\boldsymbol{c}},\boldsymbol{a}\odot\boldsymbol{b}\rangle \bmod q$。

3　安全模型

无证书加密方案由系统参数生成(Setup)，部分私钥提取(ExtractPPK)，设置公/私钥(Setkey)，加密(Enc)和解密(Dec)等 5 个算法组成[13]。在无证书系统中，令(主公钥，主私钥，身份，公钥，部分私钥，私钥，秘密值)=(MPK, MSK, ID, PK, PPK, SK, SV)且(公开参数，第 1 类攻击者，第 2 类攻击者)=(params, A_{I}, A_{II})。A_{I} 不能获知 MSK，但可替换任何用户的 PK。A_{II} 可拥有 MSK，可向 A_{I} 那样替换除了目标身份之外任何用户的 PK。用攻击者 $A\in\{A_{\mathrm{I}},A_{\mathrm{II}}\}$ 与挑战者 $\mathcal{B}$ 交互的游戏来刻画无证书加密的 IND-CPA 安全。

设置参数　$\mathcal{B}$ 输入安全参数 n，运行 (pramas, MSK, MPK) $\leftarrow$ Setup(1^n)。$\mathcal{B}$ 将 (pramas, MPK) 送给 A。若 $A=A_{\mathrm{II}}$，则需把 MSK 也给 A_{II}，导致 A_{II} 不用部分私钥询问。

问答交互　A 可访问如下的预言器(包括 hash 函数，若必要)但有次数限制。这些预言器都由 $\mathcal{B}$ 控制。为提供完美的攻击环境，$\mathcal{B}$ 必须及时记录与 A 每次问答中发生的数据。受文献[14]的启发：本文允许攻击者询问用户的秘密值，导致 A 不必做用户私钥询问(因为他完全可以自己有效地生成)。A 可适用性地做生成用户，部分私钥，公钥替换及秘密值等询问(部分私钥询问只对 A_{I} 有效)。

挑战　只要 A 宣布结束询问，他输出挑战明文 $m_0,m_1\in\mathcal{M}$ 和挑战身份 ID^* 给 $\mathcal{B}$。$\mathcal{B}$ 回应：

(1)当 $A=A_{\mathrm{I}}$ 时，若 ID^* 现在的公钥没被换掉，或 ID^* 现在的公钥被换为合法的公钥(公钥来自公钥空间并有正确公钥之形式)且部分私钥未被询问过。则执行(3)；若 ID^* 现在的公钥被换为合法的公钥且部分私钥已被询问过，则终止游戏；若 ID^* 现在的公钥被换为非法的公钥，则判定 A 失败[12]。

(2)当 $A=A_{\mathrm{II}}$ 时，ID^* 应满足公钥没被换掉且秘密值没被询问过；否则，终止游戏。

(3) 随机选择 $b\in\{0,1\}$，计算 $c^*\leftarrow\mathrm{Enc}(\mathrm{params}, \mathrm{ID}^*, \mathrm{PK}_{\mathrm{ID}^*}, m_b)$，输出 c^* 给 A。

猜测　A 传猜测值 $b'\in\{0,1\}$ 给 $\mathcal{B}$。

A 获胜的充分必要条件为 $b=b'$ 和优势为 $\varepsilon=2\left|P(b=b')-1/2\right|$。

定义 6　称无证书加密是自适应选择消息和身份攻击下语义安全的，若任何概率多项式时间(PPT)算法 $A\in\{A_{\mathrm{I}},A_{\mathrm{II}}\}$，在游戏中胜出的优势为 $\mathrm{negl}(n)$。

4　方案构造

借鉴文献[3,16]中思想，本节先给出明文空间 $\mathcal{R}_2$ 上的方案。后用中国剩余定理优化它为并行加密方案。

4.1 无证书加密(CertificateLess Encryption, CL.E)

(1) Setup(1^λ)：设 λ 为安全参数，$n=n(\lambda)$ 为 2 的幂，素数 $q=\mathrm{poly}(n)$，$q\equiv 1 \bmod 2n$。$\mathcal{R}=\mathbb{Z}[x]/(x^n+1)$，$\mathcal{R}_q=\mathcal{R}q\mathcal{R}$，误差分布 χ，其中 $\sigma_1=\omega(\sqrt{\log_2 n})$。$H$:$\{0,1\}^*\rightarrow\mathbb{Z}_q^n$ 是抗碰撞的哈希函数。密钥生成中心(KGC)运行 $(h,\boldsymbol{T})\leftarrow\mathrm{Trapdoor}_{\mathrm{NTRU}}(n,q)$，其中 $\sigma_2=1.17\sqrt{q}\omega(\sqrt{\log_2 n})\geq\|\tilde{\boldsymbol{T}}\|\omega(\sqrt{\log_2 n})$。设置 (MPK, MSK)$=(h,\boldsymbol{T})$，消息空间 $\mathcal{R}_2$，公开参数 params $=\{\lambda,n,q,\sigma_1,\sigma_2,h,H,\mathcal{R}_2\}$。这里取 $\chi=D_{\mathbb{Z}^n,\sigma_1}$。

(2) ExtractPPK(ID, params)：用户注册并提交身份 $\mathrm{ID}\in\{0,1\}^*$。KGC 执行下列程序输出 $(e,d)\in\mathcal{R}_q^2$，并安全地传 (e,d) 给该用户。用户验证所获的数据是否满足 $hd+e=u=\tau^{-1}(H(\mathrm{ID}))\in\mathcal{R}_q$ 且 $\|\tau(e)\|,\|\tau(d)\|\leq\sigma_2\sqrt{n}$。若满足，则用户置 d 为部分私钥并销毁 e；否则，要求 KGC 重新生成。

(a)若系统中已存在该ID，则拒绝并退出程序；否则，执行(b)。

(b)计算 $\boldsymbol{u}=H(\mathrm{ID})\in\mathbb{Z}_q^n$，置 $(\boldsymbol{u}\,|\,\boldsymbol{0})\in\mathbb{Z}_q^{2n}$。

(c)抽取 $(\boldsymbol{e},\boldsymbol{d})\leftarrow\mathrm{SampleD}(h,\boldsymbol{T},(\boldsymbol{u},\boldsymbol{0}),\sigma_2)$，其中 $\boldsymbol{e},\boldsymbol{d}\in\mathbb{Z}_q^n$，输出 $(e,d)=(\tau^{-1}(\boldsymbol{e}),\tau^{-1}(\boldsymbol{d}))\in\mathcal{R}_q^2$。

(3) Setkey(ID,params)：身份为ID的用户选取秘密值 $s\leftarrow\chi$。设置私钥 $\mathrm{SK}=(s,d)\in\mathcal{R}_q^2$。设置公钥PK如下：任选 $b\leftarrow\mathcal{R}_q$，$e_1\leftarrow\chi$，计算 $\bar{b}=bs+e_1\in\mathcal{R}_q$，设置 $\mathrm{PK}=(b,\bar{b})\in\mathcal{R}_q^2$。

(4) Enc(m,ID,PK,params)：在身份ID，公钥 $\mathrm{PK}=(b,\bar{b})$ 下加密 $m\in\mathcal{R}_2$。

(a)任选 $r,\bar{s},e_2,e_3,e_4,e_5\leftarrow\chi$，计算 $c_1=br+e_2\in\mathcal{R}_q$，$c_2=h\bar{s}+e_3\in\mathcal{R}_q$。

(b)计算 $c_3=m\lfloor q/2\rfloor+\bar{b}r+e_4+u\bar{s}+e_5\in\mathcal{R}_q$，这里 $u=\tau^{-1}(H(\mathrm{ID}))\in\mathcal{R}_q$。

(c)输出密文 $\boldsymbol{c}=(c_1,c_2,c_3)\in\mathcal{R}_q^3$。

(5) Dec($\boldsymbol{c}$,SK,params)：用私钥 $\mathrm{SK}=(s,d)$ 解密 $\boldsymbol{c}=(c_1,c_2,c_3)$：$m=\lfloor(2/q)[c_3-dc_2-sc_1]_q\rceil\bmod 2$。

把上述方案的明文空间由 $\mathcal{R}_2$ 扩大到 $\mathcal{R}_p$，借助中国剩余定理来实现下面的并行加密和优化算法(加解密不必做 $\bmod(x^n+1)$ 运算)[16]。

4.2 无证书并行加密

(1) Setup(1^λ)：参数 $\lambda,n,q,\sigma_1,\sigma_2,\chi,H,\mathcal{R},(h,\boldsymbol{T})$ 与4.1节Setup(1^λ)算法中的相同。不同是这里增加了：$\tilde{\boldsymbol{c}}$ 为 $\mathcal{R}_q=\mathcal{R}/q\mathcal{R}$ 上一组 $\mathbb{Z}_q-\mathrm{CRT}$，选择小素数 $p\ll q$，满足 $p^d\equiv 1\bmod 2n$。令 $\ell=n/d$，设置嵌入(或聚合)明文空间为 $\mathbb{F}_{p^d}$(或 $\mathcal{R}_p$)，CRT_p 为 $(\mathbb{F}_{p^d})^\ell\to\mathcal{R}_p$ 的同构映射。然后，计算 $h=\langle\tilde{\boldsymbol{c}},\boldsymbol{h}\rangle$。设置 $(\mathrm{MPK},\mathrm{MSK})=(\boldsymbol{h},\boldsymbol{T})$，其中 $\boldsymbol{h}\in\mathbb{Z}_q^n$，$\boldsymbol{T}\in\mathbb{Z}_q^{2n\times 2n}$。公开参数 $\mathrm{params}=\{\lambda,n,p,q,d,\ell,\sigma_1,\sigma_2,\tilde{\boldsymbol{c}},\boldsymbol{h},H,\mathbb{F}_{p^d}\}$，这里 $\tilde{\boldsymbol{c}}=(c_i)_{i\in\mathbb{Z}_{2n}^*}$。

(2) ExtractPPK(ID,params)：类似4.1节相应的算法，用户注册并验证KGC发送是数据 $(\boldsymbol{e},\boldsymbol{d})$ 是否满足 $\|\tau(\langle\tilde{\boldsymbol{c}},\boldsymbol{e}\rangle)\|,\|\tau(\langle\tilde{\boldsymbol{c}},\boldsymbol{d}\rangle)\|\le\sigma_2\sqrt{n}$ 和 $\boldsymbol{h}\odot\boldsymbol{d}+\boldsymbol{e}=\boldsymbol{u}\bmod q$，这里 $\boldsymbol{u}$ 来自 $\tau^{-1}(H(\mathrm{ID}))=\langle\tilde{\boldsymbol{c}},\boldsymbol{u}\rangle$。

(a)若系统中已存在该ID，则拒绝并退出程序；否则，执行步骤(b)。

(b)计算 $\overline{\boldsymbol{u}}=H(\mathrm{ID})\in\mathbb{Z}_q^n$，设置 $(\overline{\boldsymbol{u}}\,|\,\boldsymbol{0})\in\mathbb{Z}_q^{2n}$。

(c)抽取 $(\overline{\boldsymbol{e}},\overline{\boldsymbol{d}})\leftarrow\mathrm{SampleD}(h,\boldsymbol{T},(\overline{\boldsymbol{u}},\boldsymbol{0}),\sigma_2)$，计算 $(\tau^{-1}(\overline{\boldsymbol{e}}),\tau^{-1}(\overline{\boldsymbol{d}}))=(\langle\tilde{\boldsymbol{c}},\boldsymbol{e}\rangle,\langle\tilde{\boldsymbol{c}},\boldsymbol{d}\rangle)\in\mathcal{R}_q^2$，输出 $(\boldsymbol{e},\boldsymbol{d})\in\mathbb{Z}_q^{n\times 2}$。

(3) Setkey(ID,params)：身份为ID的用户选取秘密值 $s\leftarrow\chi$ 在基 $\tilde{\boldsymbol{c}}$ 下的坐标为 $\boldsymbol{s}$，设置私钥 $\mathrm{SK}=(\boldsymbol{s},\boldsymbol{d})\in\mathbb{Z}_q^{n\times 2}$。设置公钥PK如下：

(a)任选 $b\leftarrow\mathcal{R}_q$，$e_1\leftarrow\chi$，它们在基 $\tilde{\boldsymbol{c}}$ 下的坐标分别为 $\boldsymbol{b},\boldsymbol{e}_1$。

(b)计算 $\overline{\boldsymbol{b}}=\boldsymbol{b}\odot\boldsymbol{s}+\boldsymbol{e}_1\in\mathbb{Z}_q^n$，设置 $\mathrm{PK}=(\boldsymbol{b},\overline{\boldsymbol{b}})\in\mathbb{Z}_q^{n\times 2}$。

(4) Enc($(h_0,h_1,\cdots,h_{\ell-1})$,ID,PK,params)：在ID和 $\mathrm{PK}=(\boldsymbol{b},\overline{\boldsymbol{b}})$ 下对 $(h_0,h_1,\cdots,h_{\ell-1})\in(\mathbb{F}_{p^d})^\ell$ 加密。

(a)计算聚合明文 $m\leftarrow\mathrm{CRT}_p(h_0,h_1,\cdots,h_{\ell-1})\in\mathcal{R}_p$ 和 $u=\tau^{-1}(H(\mathrm{ID}))$ 在基 $\tilde{\boldsymbol{c}}$ 下的坐标分别为 $\boldsymbol{m}$ 和 $\boldsymbol{u}$。

(b)任选 $r,\bar{s},e_2,e_3,e_4,e_5\leftarrow\chi$，它们在基 $\tilde{\boldsymbol{c}}$ 下的坐标分别为 $\boldsymbol{r},\overline{\boldsymbol{s}},\boldsymbol{e}_2,\boldsymbol{e}_3,\boldsymbol{e}_4,\boldsymbol{e}_5$。

(c)计算 $\boldsymbol{v}_1=\boldsymbol{b}\odot\boldsymbol{r}+\boldsymbol{e}_2\in\mathbb{Z}_q^n$，$\boldsymbol{v}_2=\boldsymbol{h}\odot\overline{\boldsymbol{s}}+\boldsymbol{e}_3\in\mathbb{Z}_q^n$。

(d)计算 $\boldsymbol{v}_3=\boldsymbol{m}\lfloor q/2\rfloor+\overline{\boldsymbol{b}}\odot\boldsymbol{r}+\boldsymbol{e}_4+\boldsymbol{u}\odot\overline{\boldsymbol{s}}+\boldsymbol{e}_5\bmod q$。

(e)输出密文 $\boldsymbol{c}=(\boldsymbol{v}_1,\boldsymbol{v}_2,\boldsymbol{v}_3)\in\mathbb{Z}_q^{n\times 3}$。

(5) Dec($\boldsymbol{c}$,SK,params)：用私钥 $\mathrm{SK}=(\boldsymbol{s},\boldsymbol{d})$ 解密 $\boldsymbol{c}=(\boldsymbol{v}_1,\boldsymbol{v}_2,\boldsymbol{v}_3)$。

(a)计算聚合明文 $m=\lfloor(p/q)[\langle\tilde{\boldsymbol{c}},\boldsymbol{v}_3-\boldsymbol{d}\odot\boldsymbol{v}_2-\boldsymbol{s}\odot\boldsymbol{v}_1\rangle]_q\rceil\bmod p$。

(b)输出 $(h_0,h_1,\cdots,h_{\ell-1})\leftarrow\mathrm{CRT}_p^{-1}(m)$。

5 方案分析

易见，若4.1节中方案(CL.E)是正确安全的，则4.2节方案也如此。故只分析CL.E的性质。

5.1 正确性

下面的定理给出CL.E方案的正确性的刻画。

定理 1 在CL.E中，若 $\boldsymbol{c}\leftarrow\mathrm{Enc}(m,\mathrm{ID},\mathrm{PK},\mathrm{params})$，则 $c_3-dc_2-sc_1=m\lfloor q/2\rfloor+\Delta\bmod q$。其中 $\Delta=\bar{s}\,e+re_1-se_2-de_3+e_4+e_5$。只要 $\|\Delta\|_\infty<((q-3)/4)$，总有 $m=\lfloor(2/q)[c_3-dc_2-sc_1]_q\rceil\bmod 2$。

根据解密公式，定理1不难证明，限于篇幅，证明从略。

5.2 安全性

设定理中 $A\in\{A_{\mathrm{I}},A_{\mathrm{II}}\}$ 是自适应选择消息和身份的攻击者。A 做生成用户，部分私钥，公钥替换和秘密值等询问的最大次数依次组成向量 (q_1,q_2,q_3,q_4)，并把具有这种询问能力的攻击者记为 $A(q_1,q_2,q_3,q_4)$。上述每种询问中一次问答过程耗时依次组成向量 (t_1,t_2,t_3,t_4)。证明中用到的符号 $\perp$ 表示一个未知的值。

定理 2 设判定RLWE和判定SPR困难问题假设成立。在随机预言模型下，若在时间 T 内，$A_I(q_1,q_2,q_3,q_4)$ 以不可忽略的概率 ε 攻破CL.E，则存在一个PPT算法 $\mathcal{B}$ 以概率 $\bar{\varepsilon}\ge(1-1/q_1)^{q_2}\cdot 1/q_1\cdot\varepsilon$，在不大于 $T+q_1t_1+q_2t_2+q_3t_3+q_4t_4$ 时间内攻破LPR.E的CPA安全性。

证明 在攻击LPR.E的游戏中，设算法 $\mathcal{F}$ 是挑战者，$\mathcal{B}$ 为攻击者。在攻击CL.E的游戏中，$\mathcal{B}$ 是挑

战者，A_{I} 为攻击者。因此据 A_{I} 和 $\mathcal{F}$ 去构造 $\mathcal{B}$。

设置参数　$\mathcal{F}$ 传给 $\overline{\mathcal{B}}$ 关于 LPR.E 的参数 $(\lambda,n,q,\sigma_1,\mathcal{R}_2)$ 和公钥 $(h^*,u^*)\in\mathcal{R}_q^2$。 $\mathcal{B}$ 据它们设置 CL.E 的参数。 首先，设置主公钥 $h=h^*$，选择哈希函数 H，选择 σ_2=1.17$\sqrt{q}\omega(\sqrt{\log_2 n})$，其它参数同 LPR.E 中。 设置 $\mathrm{params}=\{\lambda,n,q,\sigma_1,\sigma_2,h,H,\mathcal{R}_2\}$。 $\mathcal{B}$ 传 params 给 A_{I}。

问答交互　$\mathcal{B}$ 选择 $t\leftarrow[q_1]$，初始化空表 L 按格式 $(\mathrm{ID},\tau(u),d,e,s,b,\bar{b})$ 添加记录。 $\mathcal{B}$ 掌控随机预言器 H。 A_{I} 适应地做下列询问且每次询问都各异。

(1)生成用户询问：当 A_{I} 输入 ID_i 时， $\mathcal{B}$ 回应：

(a) 若 $i=t$，则置 $H(\mathrm{ID}_t)$=$\tau(u^*)$，$d_t=\perp$，$e_t=\perp$。若 $i\neq t$，计算 $u_i=h\tau^{-1}(\boldsymbol{d}_i)+\tau^{-1}(\boldsymbol{e}_i)$ 满足 $(*,\tau(u_i),*,*,*,*,*)$ 在 L 中唯一，其中 $(\boldsymbol{e}_i,\boldsymbol{d}_i)\leftarrow D_{\mathbb{Z}^n,\sigma_2}$；若不唯一，则重新抽取再计算。

(b) 选择 $b_i\leftarrow\mathcal{R}_q$，$s_i\leftarrow\chi$，$e_i\leftarrow\chi$，计算 $\bar{b}_i=b_is_i+e_i \bmod q$。

(c) 添 $(\mathrm{ID}_i,\tau(u_i),d_i,e_i,s_i,b_i,\bar{b}_i)$ 入 L，传 $(\mathrm{ID}_i,\tau(u_i),b_i,\bar{b}_i)$ 给 A_I。

不失一般性，假设 A_{I} 下面询问所涉及的身份 ID_{i} 已存在。

(2)部分私钥询问：当 A_{I} 输入 ID_i 时，$\mathcal{B}$ 回应。当 $i\neq t$ 时，按 ID_i 在 L 中匹配 $(\mathrm{ID}_i,\tau(u_i),d_i,e_i,s_i,b_i,\bar{b}_i)$，传 d_i 给 A_{I}。当 $i=t$ 时，终止协议。

(3)公钥替换询问：当输入 ID_i 时，A_{I} 同时提供新公钥 $(b_i',\bar{b}_i')$ 给 $\mathcal{B}$。 $\mathcal{B}$ 据 ID_i 匹配 L，换 $(\mathrm{ID}_i,\tau(u_i),d_i,e_i,s_i,b_i,\bar{b}_i)$ 为 $(\mathrm{ID}_i,\tau(u_i),d_i,e_i,\perp,b_i',\bar{b}_i')$。

(4)秘密值询问：当 A_{I} 输入 ID_i 时，$\mathcal{B}$ 据 ID_i 索引 L 并回应。若 $s_i\neq\perp$，则传 s_i 给 A_{I}；否则，输出 $\perp$。

挑战　只要 A_{I} 宣布结束询问，他输出挑战身份 ID_i 和挑战明文 $m_0,m_1\in\mathcal{R}_2$ 给 $\mathcal{B}$。 $\mathcal{B}$ 回应。

(1)若 $\mathrm{ID}^*\neq\mathrm{ID}_t$，则 $\mathcal{B}$ 终止协议。若 ID^*=ID_t，$\mathcal{B}$ 据 ID_t 匹配 L 得到 $(\mathrm{ID}_t,\tau(u^*),\perp,\perp,s_t,b_t,\bar{b}_t)$ 或 $(\mathrm{ID}_t,\tau(u^*),\perp,\perp,\perp,b_i',\bar{b}_i')$，它们分别对应于 ID^* 的公钥没被换或已被换了。

(2)若 ID^* 的公钥没有被换，则令 $(b^*,\bar{b}^*)=(b_t,\bar{b}_t)$ 并执行(4)；否则，执行(3)。

(3)对已换的公钥 $(b_t',\bar{b}_t')$ 进行合法性测试，若非法，则以 A_{I} 失败而告终；若合法，$\mathcal{B}$ 设置 $(b^*,\bar{b}^*)=(b_t',\bar{b}_t')$ 并转入(4)。公钥 $(b_t',\bar{b}_t')$ 合法性测试过程如下：$\mathcal{B}$ 选择 $r,e_1,e_2\leftarrow\chi$ 和 $y_1,y_2\leftarrow\mathcal{R}_q$，设置 $((b_t',b_t'),(y_1,y_2))$ 和 $((b_t',\bar{b}_t'),(b_t'r+e_1,\bar{b}_t'r+e_2))$。然后，$\mathcal{B}$ 随机选择 $k\leftarrow\{0,1\}$，若 $k=0$，则输出 $c^*=(b_t',b_t',(y_1,y_2))$；否则，输出 $c^*=(b_t',\bar{b}_t',(b_t'r+e_1,\bar{b}_t'r+e_2))$。 A_{I} 据 c^* 输出猜测值 $k'\in\{0,1\}$。 若 A_{I} 能以 $1-\mathrm{negl}(n)$ 概率满足 $k=k'$，则称 $(b_t',\bar{b}_t')$ 为合法的公钥。

(4) $\mathcal{B}$ 传 m_0,m_1 给 $\mathcal{F}$，并从 $\mathcal{F}$ 那里获得挑战密文 $(c_2,c_{3,1})$。 于是，$\mathcal{B}$ 为 A_{I} 设计有效的挑战密文为 (c_1^*,c_2^*,c_3^*)=$(e_2+rb^*,c_2,c_{3,1}+\bar{e}_4+r\bar{b}^*)$，其中 $r,e_2,\bar{e}_4\leftarrow\chi$。

猜测　据 (c_1^*,c_2^*,c_3^*)，A_{I} 给出猜测 b。 $\mathcal{B}$ 把该结果 b 作为自己的猜测值传给 $\mathcal{F}$。

获胜概率　据 RLWE 假设和安全模型关于 A_{I} 胜负的规定，假定 A_{I} 必定输出合法的替换公钥是合理的。 $\mathcal{B}$ 攻击 LPR.E 获胜概率 $\bar{\varepsilon}=P(\mathrm{S}_1\cap\mathrm{S}_2\cap\mathrm{S}_3)=P(\mathrm{S}_1)P(\mathrm{S}_2\mid\mathrm{S}_1)P(\mathrm{S}_3\mid\mathrm{S}_2\cap\mathrm{S}_1)$，其中事件 S_1：在部分私钥询问时，协议未终止；事件 S_2：满足 $\mathrm{ID}^*=\mathrm{ID}_t$；事件 S_3：A_{I} 成功区分挑战密文。协议没有终止，从而挑战身份被完美隐藏。其次，从生成用户询问数据获取的方法知：回应的部分私钥分布和身份的 hash 输出分布与真实分布是不可区分的且不依赖于 u^*。此外，公钥替换、秘密值询问同真实攻击，挑战密文合法。 A_{I} 可正常发挥能力，即 $P(\mathrm{S}_3|\mathrm{S}_2\cap\mathrm{S}_1)\geq\varepsilon$。 又 $P(\mathrm{S}_1)\geq(1-1/q_1)^{q_2}$，$P(\mathrm{S}_2|\mathrm{S}_1)\geq1/q_1$，所以有 $\bar{\varepsilon}\geq(1-1/q_1)^{q_2}\cdot1/q_1\cdot\varepsilon$。

因此，若 A_{I} 能在时间 T 内以不可忽略的概率 ε 攻破 CL.E，则 $\mathcal{B}$ 可以在不大于 $T+q_1t_1+q_2t_2+q_3t_3+q_4t_4$ 时间内以概率 $\bar{\varepsilon}\geq(1-1/q_1)^{q_2}\cdot1/q_1\cdot\varepsilon$ 攻破 LPR.E。　　证毕

定理 3　设判定 RLWE 和判定 SPR 困难问题假设成立。在随机预言模型下，若在时间 T 内，$A_{\mathrm{II}}(q_1,0,q_3,q_4)$ 以不可忽略的概率 ε 攻破 CL.E，则存在一个 PPT 算法 $\mathcal{B}$ 以概率 $\bar{\varepsilon}\geq(1-1/q_1)^{q_3+q_4}\cdot1/q_1\cdot\varepsilon$，在不大于 $T+q_1t_1+q_3t_3+q_4t_4$ 时间内攻破 LPR.E 的 CPA 安全性。

类似定理2的证明，不再赘述。

5.3 参数选取

方案中参数 n，q,σ_1,σ_2 都是 λ 的函数。从安全角度看，要满足下面 2 个困难问题假设。

(1)判定 RLWE 问题： 据文献[4]，要使方案具有 2^{λ} 的安全性就需要 $n=\Omega(\lambda\log_2(q/B))$，其中 B 为误差分布的界。由引理 1 知：$B=\omega(\sqrt{n\log_2 n})$。再据引理 2 有

$$\left.\begin{array}{l} q=\mathrm{poly}(n),\sigma_1=\omega\left(\sqrt{\log_2 n}\right)\\ n=\Omega\left(\lambda\log_2\left(q/\omega\left(\sqrt{n\log_2 n}\right)\right)\right)\end{array}\right\}\tag{4}$$

(2)判定 SPR 问题： 据文献[5]知，当 $\vartheta=D_{\mathbb{Z}^n,r}$ 且 $r>\mathrm{poly}(n)\sqrt{q}$ 时，判定 SPR 问题是困难的。而 $\mathrm{Trapdoor}_{\mathrm{NTRU}}(n,q)$ 中误差分布 $\vartheta=D_{\mathbb{Z}^n,\sigma_f}$ 中 $\sigma_f=1.17\sqrt{q/(2n)}<\mathrm{poly}(n)\sqrt{q}$，这意味着该算法生成的公钥 h 分布不是均匀的。 但是，文献[3]显示：目前最好的区分 h 的算法就是求出 NTRU 格中的 f,g 满

足它们的模是异乎寻常的短，且 $h\cdot f-g=0 \bmod q$。而求解小模 f,g 的困难性取决于参数 $\gamma=(\sqrt{n}/1.368)^{1/(2n)}$ (越小，安全性越高)。文献[19]给出 γ 和安全水平 λ 之间保守关系 $\log_2\gamma=1.8/(\lambda+110)$，如当 $\gamma\le 1.00485$ 时，求解短向量的困难性至少是 2^{148}。据上述保守关系知，本方案要达到 $\gamma\le 1.00485$，则需满足 $n\ge 256$。

其次，从方案的正确性考虑。由 5.1 节中定理 1 并经简单地计算知：

$$\begin{aligned}\|\Delta\|_\infty &= \|\bar{s}e+re_1-se_2-de_3+e_4+e_5\|_\infty \\ &\le 6\|de_3\|_\infty \le 6\delta_{\mathcal{R}}\|d\|_\infty\|e_3\|_\infty \end{aligned}\tag{5}$$

据文献[5]知，式(5)中的 $\delta_{\mathcal{R}}=n$。由文献[6]中命题 2.2 知：因为 $e_3\leftarrow D_{\mathbb{Z}^n,\sigma_1}$，所以 $\|e_3\|_\infty\le\sigma_1\cdot\omega(\sqrt{\log_2 n})$。由 $\mathrm{Trapdoor}_{\mathrm{NTRU}}(n,q)$ 算法知：

$$\sigma_2=1.17\sqrt{q}\cdot\omega(\sqrt{\log_2 n})\ge\|\tilde{\boldsymbol{T}}\|\omega(\sqrt{\log_2 n})$$

若 $(\boldsymbol{e},\boldsymbol{d})\leftarrow \mathrm{SampleD}(h,\boldsymbol{T},(\boldsymbol{u},\boldsymbol{0}),\sigma_2)$，$d=\tau^{-1}(\boldsymbol{d})$，则由引理1知：

$$\|d\|_\infty\le\sigma_2\omega(\sqrt{\log_2 n})=1.17\sqrt{q}\omega(\sqrt{\log_2 n})^2$$

把上面所得的结果代入式(5)中，得

$$\|\Delta\|_\infty\le 7.02n\sqrt{q}\omega\left(\sqrt{\log_2 n}\right)^4\tag{6}$$

为同时满足定理1和式(6)，我们有 $\|\Delta\|_\infty\le 7.02n\sqrt{q}\omega(\sqrt{\log_2 n})^4<(q-3)/4$。取该式成立的充分条件：

$$29n\omega\left(\sqrt{\log_2 n}\right)^4<\sqrt{q}\tag{7}$$

由式(4)和结论 $n\ge 256$，限定 $256\le n\le \mathrm{poly}(\lambda)$，即 $\log_2 n\le O(\log_2\lambda)$。又因为 $4\le\log_2 n\le\sqrt{n}$，所以满足式(7)的充分条件：$q=O(n^6)$。于是，$q/\omega(\sqrt{n\log_2 n})\le q/\sqrt{n}\le O(n^{5.5})$。推出 $\log_2(q/\omega(\sqrt{n\log_2 n}))\le O(\log_2 n)$。从而 $\log_2(q/\omega(\sqrt{n\log_2 n}))\le O(\log_2\lambda)$。由式(4)，式(7)和 $n\ge 256$ 知：

$$\left.\begin{aligned} &n=\Omega(\lambda\log_2\lambda)\ge 256\\ &q=O\left(n^2\right)\omega\left(\sqrt{\log_2 n}\right)^8\\ &\sigma_1=\omega\left(\sqrt{\log_2 n}\right)\end{aligned}\right\}\tag{8}$$

由 $\sigma_2=1.17\sqrt{q}\cdot\omega(\sqrt{\log_2 n})\ge\|\tilde{\boldsymbol{T}}\|\omega(\sqrt{\log_2 n})$，式(8)，定理2和定理3，我们有定理4。

定理 4 设 λ 为安全参数，若 $n=\Omega(\lambda\log_2\lambda)\ge 256$ 且 n 为 2 的幂，素数 $q\equiv 1 \bmod 2n$ 且 $q=O(n^2)\cdot\omega(\sqrt{\log_2 n})^8$，$\sigma_1=\omega(\sqrt{\log_2 n})$，$\sigma_2=1.17\sqrt{q}\omega(\sqrt{\log_2 n})$，则 CL.E 存在且是 IND-CPA 安全的。

证明略。

5.4 效率

目前可公开获取的格上无证书加密方案[10,11]是基于标准 LWE 问题的困难性假设，而本文方案 CL.E 是以 RLWE 问题为基础。又因为文献[10]是标准模型下的方案，效率必然低于文献[11]和本文在随机预言模型下的方案，所以只需在文献[11]和本文之间作比较。典型地取 $\omega(\sqrt{\log_2 n})=\log_2 n$。类似 5.3 节中的计算，可以得到给定参数 n 下，文献[11]与本文方案的计算结果如表 1 所示，从表 1 可看出，本文方案每个指标都占优。

表 1 效率对比

方案	文献[11]	本文方案
模数 q	$O(n^4\log_2^{3.5}n)\omega(\log_2 n)^3$	$O(n^2)\omega(\sqrt{\log_2 n})^8$
主公钥尺寸	$6n^2\log_2^2 q$	$n\log_2 q$
主私钥尺寸	$36n^2\log_2^2 q\cdot\log_2(\sqrt{n\log_2 q})$	$2.9n\log_2 q$
用户公钥尺寸	$(6n^2\log_2 q+n)\log_2 q$	$2n\log_2 q$
用户私钥尺寸	$15n\log_2 q\cdot\log_2(6n\log_2 q)$	$n\log_2(1.17n^2\sqrt{q})$
密文尺寸	$(12n\log_2 q+1)\log_2 q$	$3n\log_2 q$
生成用户公钥计算量	$O(n^2\log_2^2 q\cdot\log_2 n)$	$O(n\log_2^2 n\cdot\log_2 q)$
生成用户私钥计算量	$O(n^2\log_2^2 q\cdot\log_2^2 n)$	不用计算
加密计算量	$O(n^2\log_2^3 q)$	$O(n\log_2^2 n\cdot\log_2 q)$
解密计算量	$O(n\log_2^2 q\cdot\log_2 n)$	$O(n\log_2^2 n\cdot\log_2^2 q)$

6 结论

本文提出一个无证书加密方案。它比文献[11]中方案有更小的存储开销，更低的计算和通信代价。本文方案可根据效率和安全做权衡。其一，如文献[3]那样把抽取误差多项式的系数限制在集 $\{-1,0,1\}$ 中，以获得更好的效率。其二，在生成 NTRU 格的陷门基时，适当放大高斯抽样偏差抽取 f 和 g 来取消小多项式比问题假设，以获得更强的安全。

参 考 文 献

[1] GENTRY C, PEIKERT C, and VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]. Proceedings of the 40th ACM Symposium on Theory of Computing (STOC08), Victoria, Canada, 2008: 197–206. doi: 10.1145/1374376.1374407.

[2] AGRAWAL S, BONEH D, and BOYEN X. Lattice basis

delegation in fixed dimension and shorter-ciphertext hierarchical IBE[J]. *LNCS*, 2010, 6223: 98–115. doi: 10.1007/978-3-642-14623-7_6.

[3] DUCAS L, LYUBASHEVSKY V, and PREST T. Efficient identity-based encryption over NTRU lattices[J]. *LNCS*, 2014, 8874: 22–41. doi: 10.1007/978-3-662-45608-8_2.

[4] BRAKERSKI Z, GENTRY C, and VAIKUNTANATHAN V. Fully homomorphic encryption without Bootstrapping[C]. Proceedings of the 3rd Innovations in Theoretical Computer Science (ITCS) Conference, Cambridge, Massachusetts, 2012: 309–325.

[5] LOPEZ-ALT A, TROMER E, and VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]. Proceedings of the 44th ACM Symposium on Theory of Computing (STOC12), New York, USA, 2012: 1219–1234. doi: 10.1145/2213977.2214086.

[6] BRAKERSKI Z and VAIKUNTANATHAN V. Lattice-based FHE as secure as PKE[C]. Proceedings of the 5rd Innovations in Theoretical Computer Science (ITCS) Conference, Princeton, New Jersey, 2014: 1–12.

[7] MICCIANCIO D and PEIKERT C. Trapdoor for lattices: simpler, tighter, faster, smaller[J]. *LNCS*, 2012, 7237: 738–755.

[8] JARVIS K and NEVINS M. ETRU: NTRU over the Eisenstein integers[J]. *Designs, Codes and Cryptography*, 2015, 74(1): 219–242.

[9] BI J G and CHENG Q. Lower bounds of shortest vector lengths in random NTRU lattices[J]. *Theoretical Computer Science*, 2014, 560(2): 121–130. doi: 10.1007/978-3-642-29952-0_18.

[10] SEPAHI R, STEINFELD R, and PIEPRZYK J. Lattice-based certificateless public-key encryption in the standard model[J]. *International Journal of Information Security*, 2014, 13(4): 315–333. doi: 10.1007/s10207-013-0215-8.

[11] JIANG Mingming, HU Yupu, LEI Hao, *et al*. Lattice-based certificateless encryption scheme[J]. *Frontiers of Computer Science*, 2014, 8(5): 828–836. doi: 10.1007/s11704-014-3187-6.

[12] AL-RIYAMI S S and PATERSON K G. Certificateless public key cryptography[J]. *LNCS*, 2003, 2894: 452–473.

[13] DENT A. A survey of Certificateless encryption schemes and security models[J]. *International Journal of Information Security*, 2008, 7(5): 347–377. doi: 10.1007/s10207-008-0055-0.

[14] 陈虎, 张福泰, 宋如顺. 可证安全的无证书代理签名方案[J]. 软件学报, 2009, 20(3): 692–701. doi: 10.3724/SP.J.1001.2009.00574.

CHEN Hu, ZHANG Futai, and SONG Rushun. Certificateless proxy signature scheme with provable security[J]. *Journal of Software*, 2009, 20(3): 692–701. doi: 10.3724/SP.J.1001.2009.00574.

[15] ALWEN J and PEIKERT C. Generating shorter bases for hard random lattices[J]. *Theory of Computing Systems*, 2011, 48(3): 535–553.

[16] LYUBASHEVSKY V, PEIKERT C, and REGEV O. On ideal lattices and learning with errors over rings[J]. *Journal of the ACM*, 2013, 60(6): 43:1–43:35.

[17] STEHLE D and STEINFELD R. Making NTRU as secure as worst-case problems over ideal lattices[J]. *LNCS*, 2011, 6632: 27–47.

[18] LYUBASHEVSKY V, PEIKERT C, and REGEV O. A toolkit for ring-LWE cryptography[J]. *LNCS*, 2013, 7881: 35–54.

[19] LINDNER R and PEIKERT C. Better key sizes (and attacks) for LWE-based encryption[J]. *LNCS*, 2011, 6558: 319–339. doi: 10.1007/978-3-642-19074-2_21.

陈　虎：　男，1975 年生，博士生，副教授，研究方向为格密码和无证书加密与签名.

胡予濮：　男，1955 年生，教授，博士生导师，研究方向为格密码和流密码.