有效的标准模型下格上基于身份的代理重加密

江明明 郭宇燕 余 磊* 宋万干 魏仕民

(淮北师范大学计算机科学与技术学院 淮北 235000)

摘 要：代理重加密在云计算环境下的密文共享等方面起着重要的作用。目前格上基于身份的代理重加密方案都是随机预言机模型的。针对这个问题，该文构造了一个高效的标准模型下格上基于身份的代理重加密方案。在方案中，用户身份仅仅被映射为一个向量，使得用户私钥的尺寸较短。该方案具有双向性，多次使用性等性质，并且在LWE困难假设下是适应性选择身份CPA安全的。

关键词：代理重加密；格密码；高斯抽样；基于身份的密码学

中图分类号：TN918.4 **文献标识码**：A **文章编号**：1009-5896(2019)01-0061-06

DOI: 10.11999/JEIT180146

Efficient Identity-based Proxy Re-encryption on Lattice in the Standard Model

JIANG Mingming GUO Yuyan YU Lei SONG Wangan WEI Shimin

(*School of Computer Science and Technology*, *Huaibei Normal University*, *Huaibei* 235000, *China*)

Abstract: Proxy re-encryption plays an important role for encrypted data sharing and so on in cloud computing. Currently, almost all of the constructions of identity-based proxy re-encryption over lattice are in the random oracle model. According to this problem, an efficient identity-based proxy re-encryption is constructed over lattice in the standard model, where the identity string is just mapped to one vector and getting a shorter secret key for users. The proposed scheme has the properties of bidirectional, multi-use, moreover, it is semantic secure against adaptive chosen identity and chosen plaintext attack based on Learning With Errors (LWE) problems in the standard mode.

Key words: Proxy re-encryption; Lattice cryptography; Gaussian sampling; Identity-based cryptography

1 引言

云存储可以为用户提供存储服务，而云计算可以通过整合用户上传到云中的资源来为用户提供各种计算服务。云计算在为用户提供服务的同时，也存在着各种安全风险，如用户的数据安全[1]。1998年，Blaze等人[2]提出了代理重加密的概念。代理重加密实现了非可信第3方在不解密的情况下，可以将一个用户的密文转化为其他用户的密文，保证了开放网络中数据的安全性和隐私性。这种特殊的转换性质使得代理重加密在云计算环境下的密文共享方面有着重要的应用。在一个代理重加密模型中，包含3个参与者，授权人，被授权人，代理人。授权人通过自己的私钥和被授权人的信息，产生一个秘密信息，作为代理人的代理私钥，代理人使用代理密钥把授权人的密文变换成被授权人的密文，而代理人并不能从代理密钥和用户密文中得到明文和用户的私钥的任何信息。文献[2]中提出了第1个代理重加密方案。Green等人[3]提出了第1个单向的基于身份的代理重加密方案。之后，一系列基于身份的代理重加密方案被设计出来[4,5]。然而，这些方案都是基于计算数论困难问题(如整数分解问题，离散对数问题)的，在量子计算环境下是不安全的。因此需要考虑抗量子计算能力的代理重加密方案的设计。格密码是设计抗量子攻击方案的一个很好的选择。Xagawa[6]提出了第1个基于格的多次使用的双向代理重加密方案。接着基于格的代理重加密方案与特殊性质的方案陆续被提出[7–12]。虽

收稿日期：2018-02-02；改回日期：2018-10-25；网络出版：2018-11-02
*通信作者： 余磊 yulei@chun.edu.com
基金项目：国家自然科学基金(60573026)，安徽省自然科学基金(1708085QF154)，安徽省高校自然科学基金(KJ2016A627, KJ2018A0398, KJ2017ZD32)，安徽省高校人才计划项目(gxyq2017154)
Foundation Items: The National Natural Science Foundations of China (60573026), Anhui Provincial Natural Science Foundation (1708085Q154), The Nature Science Foundation of Anhui Higher Education Institutions (KJ2016A627, KJ2018A398, KJ2017ZD32), The Talent Project of Anhui Higher Education Institutions (gxyq2017154)

然基于格公钥的代理重加密方案取得了一些结果，但基于身份的方案却很少，并且都是随机预言机模型下的。因此，本文的目标是构造一个格上高效的标准模型下基于身份的代理重加密方案。

2 基础知识

2.1 格

设 $\boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\}\in\mathbb{Z}^{m\times m}$ 是一个 $m\times m$ 阶矩阵，且 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\in\mathbb{Z}^m$ 线性无关。则称向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 的所有整系数线性组合所构成的集合为一个 m 维格 $\varLambda$，即

$$\varLambda=\mathcal{L}(\boldsymbol{B})=\left\{\boldsymbol{y}\in\mathbb{Z}^m,\ \text{s.t. }\exists\boldsymbol{s}\in\mathbb{Z}^m,\ \boldsymbol{y}=\boldsymbol{B}\boldsymbol{s}=\sum_{i=1}^{m}s_i\boldsymbol{b}_i\right\}\tag{1}$$

这里，$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 构成了格 $\varLambda$ 的一组基。下面给出一类常用的整数格(正交格)。

定义 1 设 q 是一个素数，$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{u}\in\mathbb{Z}_q^n$，定义

$$\left.\begin{aligned}\varLambda_q^{\perp}(\boldsymbol{A})&:=\{\boldsymbol{e}\in\mathbb{Z}^m,\ \text{s.t. }\boldsymbol{A}\boldsymbol{e}=\boldsymbol{0}(\bmod q)\}\\ \varLambda_q^{u}(\boldsymbol{A})&:=\{\boldsymbol{e}\in\mathbb{Z}^m,\ \text{s.t. }\boldsymbol{A}\boldsymbol{e}=\boldsymbol{u}(\bmod q)\}\end{aligned}\right\}\tag{2}$$

引理 1[13] 设 $q\geq 3$ 是一个奇数且 $m=\lceil 6n\log_2 q\rceil$，则利用陷门生成算法 $\mathrm{TrapGen}(1^n)$，产生矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}\in\mathbb{Z}_q^{m\times m}$，其中 $\boldsymbol{A}$ 在 $\mathbb{Z}_q^{n\times m}$ 上的分布与均匀分布是不可区分的，$\boldsymbol{T}$ 是格 $\varLambda_q^{\perp}(\boldsymbol{A})$ 的一组基，且满足 $\|\widetilde{\boldsymbol{T}}\|\leq O\left(\sqrt{n\log_2 q}\right),\|\boldsymbol{T}\|\leq O(n\log_2 q)$，这里 $\widetilde{\boldsymbol{T}}$ 是 $\boldsymbol{T}$ 的施密特正交化矩阵，$\|\boldsymbol{T}\|$ 是矩阵 $\boldsymbol{T}$ 的欧几里得范数。

定义 2 $\mathrm{LWE}_{q,\chi}$ 判定问题：设 q 是一个素数，n 是一个正整数。$A_{s,\chi}$ 是变量为 $(\boldsymbol{a},\boldsymbol{a}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x})$ 的分布，这里 $\boldsymbol{a}\leftarrow\mathbb{Z}_q^n$，$\boldsymbol{s}\leftarrow\mathbb{Z}_q^n$ 是均匀随机选择的，$x\leftarrow\chi$，χ 是 $\mathbb{Z}_q$ 上的分布。$\mathrm{LWE}_{q,\chi}$ 判定问题是区分分布 $A_{s,\chi}$ 和 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的均匀分布。

2.2 离散高斯

离散高斯分布与高斯抽样算法是在随机格上设计方案的重要定义与算法，下面简单介绍离散高斯分布的定义以及关于高斯抽样算法的几个相关引理。

对于 $\boldsymbol{c}\in\mathbb{Z}^m$，$\sigma>0$，$m$ 维格 $\varLambda$ 上的离散高斯分布定义为

$$D_{\varLambda,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\varLambda)}=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\sum\limits_{x\in\varLambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})},\forall\boldsymbol{x}\in\mathbb{Z}^m\tag{3}$$

引理 2[14] 设 $q\geq 2$，矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$m>n$。$\boldsymbol{T}_{\boldsymbol{A}}$ 是格 $\varLambda_q^{\perp}(\boldsymbol{A})$ 的一组基，$\sigma\geq\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\cdot\omega\left(\sqrt{\log_2 m}\right)$。那么，对于 $\boldsymbol{c}\in\mathbb{Z}^m$，$\boldsymbol{u}\in\mathbb{Z}_q^n$ 有：

(1) $\Pr\left[\boldsymbol{x}\leftarrow D_{\varLambda_q^{\perp}(\boldsymbol{A}),\sigma}:\|\boldsymbol{x}\|>\sigma\sqrt{m}\right]\leq\mathrm{negl}(n)$；

(2) 存在算法 $\mathrm{SamplePre}(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},\sigma)$，输出一个 $\varLambda_q^{u}(\boldsymbol{A})$ 中的向量 $\boldsymbol{x}$，且 $\boldsymbol{x}$ 的分布与分布 $D_{\varLambda_q^{u}(\boldsymbol{A}),\sigma,\boldsymbol{c}}$ 是不可区分的。

引理 3[14] 设 n 和 q 是正整数，且 q 是素数，$m\geq 2n\log_2 q$。那么对于 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m},\sigma\geq\omega\left(\sqrt{\log_2 m}\right)$，$\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,\sigma}$，则 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{e}\bmod q$ 的分布统计接近于 $\mathbb{Z}_q^n$ 上的均匀分布。

引理 4[15] 设 $\varLambda\subseteq\mathbb{Z}^m$ 是一个格，$\sigma\in\mathbb{R}$。对于 $i=1,2,\cdots,k,\boldsymbol{v}_i\in\mathbb{Z}^m$。$X_i$ 是从 $D_{\varLambda+\boldsymbol{v}_i,\sigma}$ 中抽取的两两线性无关的随机变量。设 $\boldsymbol{c}=(c_1,c_2,\cdots,c_k)\in\mathbb{Z}^k$，定义 $g:=\gcd(c_1,c_2,\cdots,c_k)$，$\boldsymbol{v}:=\sum_{i=1}^{k}c_i\boldsymbol{v}_i$。对于可忽略的 ε，$\sigma>\|\boldsymbol{c}\|\cdot\eta_{\varepsilon}(\varLambda)$，那么 $Z=\sum_{i=1}^{k}c_iX_i$ 的分布统计接近于 $D_{g\varLambda+\boldsymbol{v},\|\boldsymbol{c}\|\sigma}$。

上述3个引理用在方案的安全性证明中，来说明模拟的系统与真实的系统是不可区分的。

3 基于身份的代理重加密

3.1 方案介绍

(1)主密钥生成：输入安全参数 1^n，运行陷门生成算法 $\mathrm{TrapGen}(1^n)$ 产生一个随机的矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和格 $\varLambda_q^{\perp}(\boldsymbol{A})$ 的一个小范数矩阵 $\boldsymbol{T}\in\mathbb{Z}^{m\times m}$ 作为格的陷门基，且 $\|\widetilde{\boldsymbol{T}}\|\leq O\left(\sqrt{n\log_2 q}\right)$。函数 $f_{\boldsymbol{A}}(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}\bmod q(f:\mathbb{Z}^m\rightarrow\mathbb{Z}_q^n)$。随机选择 l+1个随机且线性无关的向量 $\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l\in\mathbb{Z}^n$。那么主公钥为 $\mathrm{MPK}=(\boldsymbol{A},\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l)$，主私钥为 $\mathrm{MSK}=\boldsymbol{T}$。

(2)用户私钥提取：输入主公钥MPK、主私钥MSK和用户的身份 $\mathbf{id}=(\mathrm{id}_1,\mathrm{id}_2,\cdots,\mathrm{id}_l)\in\{0,1\}^l$，提取用户私钥如下：(a)计算 $\boldsymbol{u}=\boldsymbol{u}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{u}_i$；(b)给定高斯参数 $\sigma\left(\left(1+\sum_{i=1}^{l}\mathrm{id}_i\right)\Big/(l+1)\right)$，利用原像抽样算法产生一个向量 $\boldsymbol{e}$ 满足 $\boldsymbol{A}\boldsymbol{e}=\boldsymbol{u}=\boldsymbol{u}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{u}_i$ 且 $\|\boldsymbol{e}\|\leq\sigma\left(\left(1+\sum_{i=1}^{l}\mathrm{id}_i\right)\Big/(l+1)\right)\sqrt{m}$。因此，用户 $\mathbf{id}$ 的私钥为 $\boldsymbol{e}$。

(3)代理重加密密钥生成：对于用户 $\mathbf{id}_1$ 与 $\mathbf{id}_2$，其对应的私钥为 $\boldsymbol{e}_{\mathbf{id}_1}$ 与 $\boldsymbol{e}_{\mathbf{id}_2}$，计算 $\mathrm{rk}_{\mathbf{id}_1\leftrightarrow\mathbf{id}_2}=\boldsymbol{e}_{\mathbf{id}_1}-\boldsymbol{e}_{\mathbf{id}_2}$ 作为代理重加密密钥。

(4)加密：输入主公钥MPK，用户身份 $\mathbf{id}_1=(\mathrm{id}_{11},\mathrm{id}_{12},\cdots,\mathrm{id}_{1l})$ 和一个消息比特 $\mu\in\{0,1\}$，加密如下：(a)计算 $\boldsymbol{u}=\boldsymbol{u}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{u}_i$；(b)选择

一个随机的向量$\boldsymbol{s}$，计算$\boldsymbol{y}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}$, $c=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+\mu\lfloor q/2\rfloor$，这里$\boldsymbol{x}\leftarrow\Phi_{\alpha}^{m}$, $x\leftarrow\Phi_{\alpha}$。(c)输出密文$(\boldsymbol{y},c)$。

(5)重加密：输入重加密密钥$\mathrm{rk}_{\mathbf{id}_1\leftrightarrow\mathbf{id}_2}=\boldsymbol{e}_{\mathbf{id}_1}-\boldsymbol{e}_{\mathbf{id}_2}$，用户$\mathbf{id}_1=(\mathrm{id}_{11},\mathrm{id}_{12},\cdots,\mathrm{id}_{1l})$的密文$(\boldsymbol{y},c_{\mathbf{id}_1})$，代理者利用代理重加密密钥计算$c_{\mathbf{id}_2}=c_{\mathbf{id}_1}-\mathrm{rk}_{\mathbf{id}_1\leftrightarrow\mathbf{id}_2}^{\mathrm{T}}\boldsymbol{y}$，输出用户$\mathbf{id}_2=(\mathrm{id}_{21},\mathrm{id}_{22},\cdots,\mathrm{id}_{2l})$的密文$(\boldsymbol{y},c_{\mathbf{id}_2})$。

(6)解密：输入用户$\mathbf{id}_2=(\mathrm{id}_{21},\mathrm{id}_{22},\cdots,\mathrm{id}_{2l})$的私钥$\boldsymbol{e}_{\mathbf{id}_2}$，计算$c_{\mathbf{id}_2}-\boldsymbol{e}_{\mathbf{id}_2}^{\mathrm{T}}\boldsymbol{y}$，若结果接近0，则输出0，若结果接近$\lfloor q/2\rfloor$，则输出1。

3.2 正确性与参数设置

对于一个密文$(\boldsymbol{y},c)$，解密过程为

$$\begin{aligned}t&=c-\boldsymbol{e}^{\mathrm{T}}\boldsymbol{y}=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+\mu\lfloor q/2\rfloor-\boldsymbol{e}^{\mathrm{T}}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x})\\&=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+\mu\lfloor q/2\rfloor-(\boldsymbol{A}\boldsymbol{e})^{\mathrm{T}}\boldsymbol{s}-\boldsymbol{e}^{\mathrm{T}}\boldsymbol{x}\\&=x-\boldsymbol{e}^{\mathrm{T}}\boldsymbol{x}+\mu\lfloor q/2\rfloor\end{aligned}\tag{4}$$

若t接近0，则输出0，若结果接近$\lfloor q/2\rfloor$，则输出1。

对于一个重加密密文$(\boldsymbol{y},c_{\mathbf{id}_2})$，解密过程为

$$\begin{aligned}t&=c_{\mathbf{id}_2}-\boldsymbol{e}_{\mathbf{id}_2}^{\mathrm{T}}\boldsymbol{y}=c_{\mathbf{id}_1}-\mathrm{rk}_{\mathbf{id}_1\leftrightarrow\mathbf{id}_2}^{\mathrm{T}}\boldsymbol{y}-\boldsymbol{e}_{\mathbf{id}_2}^{\mathrm{T}}\left(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}\right)\\&=\boldsymbol{u}_{\mathbf{id}_1}^{\mathrm{T}}\boldsymbol{s}+x+\mu\lfloor q/2\rfloor-\left(\boldsymbol{e}_{\mathbf{id}_1}-\boldsymbol{e}_{\mathbf{id}_2}\right)^{\mathrm{T}}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x})\\&\quad-\boldsymbol{e}_{\mathbf{id}_2}^{\mathrm{T}}\left(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}\right)\\&=\boldsymbol{u}_{\mathbf{id}_1}^{\mathrm{T}}\boldsymbol{s}+x+\mu\lfloor q/2\rfloor-\boldsymbol{u}_{\mathbf{id}_1}^{\mathrm{T}}\boldsymbol{s}-\boldsymbol{e}_{\mathbf{id}_1}^{\mathrm{T}}\boldsymbol{x}+\boldsymbol{u}_{\mathbf{id}_2}^{\mathrm{T}}\boldsymbol{s}\\&\quad+\boldsymbol{e}_{\mathbf{id}_2}^{\mathrm{T}}\boldsymbol{x}-\boldsymbol{u}_{\mathbf{id}_2}^{\mathrm{T}}\boldsymbol{s}-\boldsymbol{e}_{\mathbf{id}_2}^{\mathrm{T}}\boldsymbol{x}\\&=x-\boldsymbol{e}_{\mathbf{id}_1}^{\mathrm{T}}\boldsymbol{x}+\mu\lfloor q/2\rfloor\\&=x-\boldsymbol{e}_{\mathbf{id}_1}^{\mathrm{T}}\boldsymbol{x}+\mu\lfloor q/2\rfloor\end{aligned}\tag{5}$$

因此，若t接近0，则输出0，若结果接近$\lfloor q/2\rfloor$，则输出1。

对于方案的正确性，参数应该满足如下条件：

(1)为了满足陷门生成算法TrapGen的需要，我们设置$m>6n\log_2 q$，并且$q=\mathrm{ploy}(n)$，这里$\mathrm{ploy}(n)$表示n的多项式；

(2)为了满足私钥提取算法的需要，要求$\sigma\geq\|\widetilde{\boldsymbol{T}}\|\cdot\omega(\sqrt{\log_2 n})$；

(3)为满足文献[14]中对偶加密算法的正确性，要求$q>5\sigma(m+1)$且$\alpha<1/\sigma\sqrt{m}\omega(\log_2 m)$；

(4)在陷门生成算法中，要求$\left\|\tilde{\boldsymbol{T}}\right\|\leq O\left(\sqrt{n\log_2 q}\right)$；

因此，设置参数如下：$m=6n\lceil\log_2 q\rceil$, $q=n^3$, $\sigma=m\cdot\omega(\log_2 n)$, $\alpha=1/(l+1)\sigma m\omega(\log_2 m)$，这里$l<n$是用户身份的长度。

3.3 安全性分析

定理1(多次使用性)　该方案满足多次使用性。

证明　考虑k个用户$1,2,\cdots,k$，假设$(\boldsymbol{y},c_1)$是用户1的密文，从$1-k$的重加密过程为

$$\begin{aligned}c_k&=c_{k-1}-\mathrm{rk}_{k-1\leftrightarrow k}^{\mathrm{T}}\boldsymbol{y}\\&=c_{k-2}-\mathrm{rk}_{k-2\leftrightarrow k-1}^{\mathrm{T}}\boldsymbol{y}-\mathrm{rk}_{k-1\leftrightarrow k}^{\mathrm{T}}\boldsymbol{y}=\cdots\\&=c_1-\sum_{i=1}^{k-1}\mathrm{rk}_{i\leftrightarrow i+1}^{\mathrm{T}}\boldsymbol{y}=c_1-\sum_{i=1}^{k-1}\left(\boldsymbol{e}_i-\boldsymbol{e}_{i+1}\right)\boldsymbol{y}\\&=c_1-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{y}+\boldsymbol{e}_k^{\mathrm{T}}\boldsymbol{y}\\&=\boldsymbol{u}_1^{\mathrm{T}}\boldsymbol{s}+x+\mu\lfloor q/2\rfloor-\boldsymbol{e}_1^{\mathrm{T}}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x})\\&\quad+\boldsymbol{e}_k^{\mathrm{T}}\left(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}\right)\\&=\boldsymbol{u}_k^{\mathrm{T}}\boldsymbol{s}+\left(x-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{x}+\boldsymbol{e}_k^{\mathrm{T}}\boldsymbol{x}\right)+\mu\lfloor q/2\rfloor\\&=\boldsymbol{u}_k^{\mathrm{T}}\boldsymbol{s}+x'+\mu\lfloor q/2\rfloor\end{aligned}\tag{6}$$

其中，$x'=x-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{x}+\boldsymbol{e}_k^{\mathrm{T}}\boldsymbol{x}$。显然$(\boldsymbol{y},c_k)$是用户$k$的密文。由于$\boldsymbol{e}_1$, $\boldsymbol{e}_k$, $\boldsymbol{x}$是小范数向量，x是较小的整数，因此x'也是一个较小的整数，所以$(\boldsymbol{y},c_k)$可以正确解密。　　证毕

定理2 (安全性)　假设参数设置为3.2节所示，并且LWE问题是困难的，则该代理重加密方案在标准模型下是IND-aID-CPA安全的。

证明　在证明过程中，需要使用游戏的方式来证明一个多项式时间敌手攻击该方案的优势是可忽略的。下面需要证明3个游戏(Game)对于多项式时间敌手来说是不可区分的。

游戏1　该游戏是标准的适应性选择身份的选择明文攻击安全(IND-aID-CPA)的方案。

初始阶段：输入安全参数1^n，运行陷门生成算法$\mathrm{TrapGen}\left(1^n\right)$产生一个随机的矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和格$\Lambda_q^{\perp}(\boldsymbol{A})$的一个小范数矩阵$\boldsymbol{T}\in\mathbb{Z}^{m\times m}$作为格的陷门基，且$\|\widetilde{\boldsymbol{T}}\|\leq O\left(\sqrt{n\log_2 q}\right)$。函数$f_{\boldsymbol{A}}(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}\bmod q(f:\mathbb{Z}^m\rightarrow\mathbb{Z}_q^n)$。随机选择$l$+1个随机且线性无关的向量$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l\in\mathbb{Z}^n$。最后把公开参数$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$, $\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l\in\mathbb{Z}^n$发送给敌手$\mathcal{A}$。

阶段1：在这个阶段，敌手$\mathcal{A}$在得到公开参数后，可以进行密钥提取询问、重加密密钥询问(敌手询问到重加密密钥后可自行进行重加密操作，因此不需要进行重加密询问)，真实系统回答提问如下：

密钥提取询问：敌手询问用户$\mathbf{id}$的密钥，真实系统计算$\boldsymbol{u}=\boldsymbol{u}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{u}_i$；给定高斯参数$\sigma\left(\left(1+\sum_{i=1}^{l}\mathrm{id}_i\right)\Big/(l+1)\right)$，利用原像抽样算法产生一个向量$\boldsymbol{e}$满足$\boldsymbol{A}\boldsymbol{e}=\boldsymbol{u}=\boldsymbol{u}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{u}_i$且$\|\boldsymbol{e}\|\leq\sigma\left(\left(1+\sum_{i=1}^{l}\mathrm{id}_i\right)\Big/(l+1)\right)\sqrt{m}$。发送$\boldsymbol{e}$给敌手$\mathcal{A}$作为用户$\mathbf{id}$的私钥。

重加密密钥询问：敌手$\mathcal{A}$询问用户$\mathbf{id}_1$与$\mathbf{id}_2$之间的代理重加密密钥，系统查询其对应的私钥为

$\boldsymbol{e}_{\mathbf{id}_1}$与$\boldsymbol{e}_{\mathbf{id}_2}$，计算$\mathrm{rk}_{\mathbf{id}_1\leftrightarrow\mathbf{id}_2}=\boldsymbol{e}_{\mathbf{id}_1}-\boldsymbol{e}_{\mathbf{id}_2}$作为代理重加密密钥发送给敌手$\mathcal{A}$。

挑战阶段：当挑战者收到$(\mathbf{id}^*,\mu_0,\mu_1)$，挑战者选择一个随机的$b\in\{0,1\}$，计算$\boldsymbol{y}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}$，$c^*=\boldsymbol{u}_{\mathbf{id}^*}^{\mathrm{T}}\boldsymbol{s}+x+\mu_b\lfloor q/2\rfloor$，并发送$\boldsymbol{c}^*=(\boldsymbol{y},c^*)$给敌手$\mathcal{A}$。最后$\mathcal{A}$给出猜测$b'$，若$b'=b$，则挑战者输出1，否则输出0。

游戏2 在这个游戏中，游戏2与游戏1的区别是矩阵$\boldsymbol{A}$与向量$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l$的生成方法。在游戏2中挑战者$\mathcal{C}$要模拟真实的方案，并且需要回答攻击者$\mathcal{A}$的各种询问。首先挑战者模拟真实的方案如下：

初始阶段：挑战者$\mathcal{C}$随机选择一个随机矩阵$\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$，计算$l$+1个$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l\in\mathbb{Z}_q^n$。计算步骤为：

(1)挑战者首先按照高斯分布$D_{\sigma/(l+1),0}$随机选择$l+1$个矩阵$\boldsymbol{e}_0,\boldsymbol{e}_1,\cdots,\boldsymbol{e}_l$；

(2)挑战者计算$\boldsymbol{A}\boldsymbol{e}_i(\bmod q)=\boldsymbol{u}_i$, i=0, 1, $\cdots$, l;

(3)检查$\boldsymbol{u}_i$是否是线性无关的，如果不是，则重复步骤(1)。

挑战者$\mathcal{C}$将初始阶段产生的公开参数$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l\in\mathbb{Z}^m$发送给攻击者$\mathcal{A}$。

阶段1：敌手$\mathcal{A}$在得到公开参数后，可以进行密钥提取询问、重加密密钥询问(敌手询问到重加密密钥后可自行进行重加密，因此不需要进行重加密询问)，挑战者$\mathcal{C}$回答敌手$\mathcal{A}$的询问如下：

(1)密钥提取询问：敌手$\mathcal{A}$发送身份$\mathbf{id}_i$给挑战者，挑战者计算$\boldsymbol{e}_{\mathrm{id}_i}=\boldsymbol{e}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{e}_i$, $\boldsymbol{e}_i\leftarrow D_{\sigma/(l+1),0}$，由引理4可知，$\boldsymbol{e}_{\mathrm{id}_i}\leftarrow D_{\sigma\cdot\sum_{i=0}^{l}\mathrm{id}_i/(l+1),0}$。由于$\boldsymbol{A}\boldsymbol{e}_i(\bmod q)=\boldsymbol{u}_i$，因此$\boldsymbol{A}\boldsymbol{e}_{\mathbf{id}_i}(\bmod q)=\boldsymbol{u}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{u}_i$。挑战者发送$\boldsymbol{e}_{\mathbf{id}_i}=\boldsymbol{e}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{e}_i$给敌手$\mathcal{A}$作为用户身份$\mathbf{id}_i$的私钥。

(2)重加密密钥询问：敌手$\mathcal{A}$发送$(\mathbf{id}_i,\mathbf{id}_j)$给挑战者，则挑战者利用上述方法计算$\boldsymbol{e}_{\mathbf{id}_i}$和$\boldsymbol{e}_{\mathbf{id}_j}$，并计算$\mathrm{rk}_{\mathbf{id}_i\leftrightarrow\mathbf{id}_j}=\boldsymbol{e}_{\mathbf{id}_i}-\boldsymbol{e}_{\mathbf{id}_j}$给敌手$\mathcal{A}$。

阶段2(挑战阶段)：当挑战者收到$(\mathbf{id}^*,\mu_0,\mu_1)$，挑战者选择一个随机的$b\in\{0,1\}$，计算$\boldsymbol{y}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}$，$c^*=\boldsymbol{u}_{\mathbf{id}^*}^{\mathrm{T}}\boldsymbol{s}+x+\mu_b\lfloor q/2\rfloor$，并发送$\boldsymbol{c}^*=(\boldsymbol{y},c^*)$给敌手$\mathcal{A}$。最后$\mathcal{A}$给出猜测$b'$，若$b'=b$，则挑战者输出1，否则输出0。

游戏3 在这个游戏中，与游戏2的区别是挑战密文的生成。在游戏2中，挑战密文$\boldsymbol{c}^*=(\boldsymbol{y},c^*)$是使用加密算法产生的，即$\boldsymbol{y}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}$，$c^*=\boldsymbol{u}_{\mathbf{id}^*}^{\mathrm{T}}\boldsymbol{s}+x+\mu_b\lfloor q/2\rfloor$。在游戏3中，挑战密文$\boldsymbol{c}^*$是从$\mathbb{Z}_q^n\times\mathbb{Z}_q$中随机选取的。

若游戏2与游戏1不可区分，且游戏3与游戏2也是不可区分的，则该代理重加密方案在标准模型下是IND-aID-CPA安全的。 证毕

下面将通过两个引理来说明游戏2与游戏1是不可区分的，游戏3与游戏2是不可区分的。

引理 5 游戏2与游戏1是不可区分的，并且对于敌手的询问回答与真实的方案也是不可区分的。

(1)在游戏1中，矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$是利用陷门生成算法$\mathrm{TrapGen}(1^n)$生成的，并且是随机的。在游戏2中，$\boldsymbol{A}$是从$\mathbb{Z}_q^{n\times m}$中随机选取的。因此公开参数$\boldsymbol{A}$对于敌手看来是不可区分的。

(2)在游戏1中，公开参数$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l\leftarrow\mathbb{Z}_q^n$是随机选择的；在游戏2中，$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l$的生成是由算法$\boldsymbol{A}\boldsymbol{e}_i(\bmod q)=\boldsymbol{u}_i$产生的，由引理3可知，$\boldsymbol{A}\boldsymbol{e}_i(\bmod q)=\boldsymbol{u}_i$的分布统计接近于$\mathbb{Z}_q^n$上的均匀分布。因此公开参数$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l$对于敌手看来也是不可区分的。

(3)对于密钥提取询问，在游戏1中，用户密钥$\boldsymbol{e}_{\mathbf{id}}$是利用陷门使用原像抽样算法产生的，满足$A\boldsymbol{e}_{\mathrm{id}}=\boldsymbol{u}=\boldsymbol{u}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{u}_i$且$\|\boldsymbol{e}_{\mathbf{id}}\|\le\sigma\left(\left(1+\sum_{i=1}^{l}\mathrm{id}_i\right)\Big/(l+1)\right)\sqrt{m}$。在游戏2中，用户密钥$\boldsymbol{e}_0,\boldsymbol{e}_1,\cdots,\boldsymbol{e}_l$是挑战者按照高斯分布$D_{\sigma/(l+1),0}$抽取出来的，因此对于模拟的用户密钥$\boldsymbol{e}_{\mathrm{id}}$满足$\|\boldsymbol{e}_{id}\|\le\sigma\left(\left(1+\sum_{i=1}^{l}\mathrm{id}_i\right)\Big/(l+1)\right)\sqrt{m}$，且根据$\boldsymbol{u}_0,\boldsymbol{u}_1,\cdots,\boldsymbol{u}_l$的生成，满足$\boldsymbol{A}\boldsymbol{e}_i(\bmod q)=\boldsymbol{u}_i$，$i=0,1,\cdots,l$。因此挑战者对于用户提取询问的回答对于敌手看来与游戏1中是不可区分的。

(4)对于重加密密钥询问，在游戏1中，代理重加密密钥的计算$\mathrm{rk}_{\mathbf{id}_i\leftrightarrow\mathbf{id}_j}=\boldsymbol{e}_{\mathbf{id}_i}-\boldsymbol{e}_{\mathbf{id}_j}$。而在游戏1中也是以同样的方法计算的，因此挑战者对于重加密密钥的回答对于敌手看来与游戏1中是不可区分的。

因此，游戏1与游戏2对于攻击者是不可区分的。

引理 6 游戏3与游戏2是不可区分的。

用反证法来证明游戏3与游戏2是不可区分的。假设敌手$\mathcal{A}$具有不可忽略的优势ε来区分游戏3与游戏2，则可以构造一个算法$\mathcal{B}$来解决LWE判定问题。

$\mathcal{B}$收到m个随机实例$(\boldsymbol{a}_i,y_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$，令$\boldsymbol{A}=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots\boldsymbol{a}_m)$，$\boldsymbol{y}=(y_1,y_2,\cdots y_m)$。计算$c^*=\left(\boldsymbol{e}_0+\sum_{i=1}^{l}\mathrm{id}_i\boldsymbol{e}_i\right)^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{y}+x+\mu_b\lfloor q/2\rfloor$，令$\boldsymbol{c}^*=(\boldsymbol{y},c^*)$。如果敌手$\mathcal{A}$猜测了正确的$b$，则挑战者输出1，否则输出0。

如果随机实例$(\boldsymbol{a}_i,y_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$是均匀随机生

成的，则挑战密文$\boldsymbol{c}^*$也是均匀随机的，因此$\mathcal{B}$输出1的概率至多为1/2。

如果随机实例$(\boldsymbol{a}_i, y_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$是LWE实例，即$\boldsymbol{y} = (y_1, y_2, \cdots y_m) = (\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} + \boldsymbol{x}) \bmod q$，则挑战密文$\boldsymbol{c}^*$也是均匀随机的。这和采用加密算法得到的密文分布是相同的。在这种情况下，敌手$\mathcal{A}$猜测正确的b的概率为$(1+\varepsilon)/2$，其中，ε是一个不可忽略的量。即$\mathcal{B}$输出1的概率也是$(1+\varepsilon)/2$。

综上可知，$\mathcal{B}$至少以$\varepsilon' = (1+\varepsilon)/2 - 1/2 = \varepsilon/2$的概率求解LWE判定问题。

由于LWE判定问题是一个困难问题，因此游戏3与游戏2是不可区分的。

因此，由引理5和引理6可知，该方案在标准模型下是IND-aID-CPA安全的。

4　安全与效率分析

该方案将用户的身份直接映射到一个向量，使得方案的主公钥、用户私钥与密文尺寸较短，存储空间较小。下面将该方案与格上其他相关方案的安全性、运行效率和存储空间进行比较，表1为存储空间与安全模型的比较结果，表2为计算效率的比较结果。

表 1　存储空间及安全模型比较

	主公钥尺寸	用户私钥尺寸	密文尺寸	安全模型
本文方案	$O((m+1)n\log_2 q)$	$O(m\log_2 q)$	$O(m\log_2 q)$	标准模型
文献[9]	$O(nm\log_2 q)$	$O(m\log_2 q)$	$O(m\log_2 q)$	随机预言机模型
文献[10]	$O(nm\log_2 q)$	$O(nm\log_2 q)$	$O(m\log_2 q)$	随机预言机模型

表 2　计算效率比较

	私钥生成	加密	重加密	解密
本文方案	$O(n^2)$	$O(n^2)$	$O(n)$	$O(n)$
文献[9]	$O(n^2)$	$O(n^2)$	$O(n)$	$O(n)$
文献[10]	$O(n^2)$	$O(n^2)$	$O(n^2)$	$O(n^3)$

通过表1与表2的比较可以发现，本方案在标准模型下的主公钥、用户私钥与密文尺寸和随机预言机模型下的主公钥、用户私钥、密文尺寸相当，而在计算效率上却没有降低。

5　结束语

本文采用原像抽样技术提出了一个标准模型下高效的格上基于身份的代理重加密方案。在方案中，用户的身份被编码为一个向量，与传统的格上基于身份的方案中用户私钥的提取技术相比，效率较高。该方案具有双向性，多次使用性等性质。最后证明了在LWE困难假设下是适应性选择身份的选择明文安全的。

参 考 文 献

[1] 蒋建春, 文伟平. “云”计算环境的信息安全问题[J]. 信息网络安全, 2010, 10(2): 61–63. doi: 10.3969/j.issn.1671-1122.2010.02.026.
JIANG Jianchun and WEN Weiping. The information security problems of cloud computing environment[J]. *Netinfo Security*, 2010, 10(2): 61–63. doi: 10.3969/j.issn.1671-1122.2010.02.026.

[2] BLAZE M, BLEUMER G, and STRAUSS M. Divertible protocols and atomic proxy cryptography[C]. EUROCRYPT, Espoo, Finland, 1998: 127–144. doi: 10.1007/BFb0054122.

[3] GREEN M and ATENIESE G. Identity-based proxy re-encryption[C]. International Conference on Applied Cryptography and Network Security, Berlin, Germany, 2007: 288–306. doi: 10.1007/978-3-540-72738-5_19.

[4] SHAO Jun and CAO Zhenfu. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption[J]. *Information Sciences*, 2012, 206(16): 83–95. doi: 10.1016/j.ins.2012.04.013.

[5] ZHANG Jindan, WANG Xu'an, and YANG Xiaoyuan. Identity based proxy re-encryption based on BB2 and SK IBE with the help of PKG[J]. *Journal of Computers*, 2013, 8(5): 1230–1239. doi: 10.4304/jcp.8.5.1230-1239.

[6] XAGAWA K. Cryptography with Lattices[D]. [Ph.D. dissertation], Tokyo Institute of Technology, 2010.

[7] KIRSHANOVA E. Proxy re-encryption from Lattices[C]. The IACR International Conference on Practice and Theory of Public-Key Cryptography, Berlin, Germany, 2014: 77–94. doi: 10.1007/978-3-642-54631-0_5.

[8] SINGH K, RANGAN C P, and BANERJEE A K. Lattice based identity based unidirectional proxy re-encryption scheme[C]. International Conference on Security, Privacy, and Applied Cryptography Engineering, Pune, India, 2014: 76–91. doi: 10.1007/978-3-319-12060-7_6.

[9] JIANG Mingming, HU Yupu, WANG Baocang, *et al*. Lattice-based unidirectional proxy re-encryption[J]. *Security and Commutation Networks*, 2016, 18(8): 3796–3803. doi: 10.1002/sec.1300.

[10] NUNEZ D, AGUDO I, and LOPEZ J. NTRU ReEncrypt: An efficient proxy re-encryption scheme based on NTRU[C]. Proceedings of ASIACCS, 2015: 14–17. doi: 10.1145/2714576.2714585.

[11] 江明明, 赵利军, 王艳, 等. 面向云数据共享的量子安全的无证书双向代理重加密[J]. 信息网络安全, 2018, 18(8): 17–24. doi: 10.3969/j.issn.1671-1122.2018.08.003.
JIANG Mingming, ZHAO Lijun, WANG Yan, *et al*. Quantum-security certificateless bidirectional proxy re-encryption for cloud data sharing[J]. *Netinfo Security*, 2018, 18(8): 17–24. doi: 10.3969/j.issn.1671-1122.2018.08.003.

[12] WANG Xuyang, HU Aiqun, and FANG Hao. Feasibility analysis of lattice-based proxy re-encryption[C]. Proceedings of the 2017 International Conference on Cryptography, Security and Privacy, Wuhan, China, 2017: 12–16. doi: 10.1145/3058060.3058080.

[13] ALWEN J and PEIKER C. Generating shorter bases for hard random lattices[C]. The 26th International Symposium on Theoretical Aspects of Computer Science, Freiburg, Germany, 2009: 535–553. doi: 10.1007/s00224-010-9278-3.

[14] GENTRY C, PEIKERT C, and VAIKUNTANATHAN V. How to use a short basis: Trapdoors for hard lattices and new cryptographic constructions[C]. The 40th ACM Symposium on Theory of Computing, Victoria, Canada, 2008: 197–206.

[15] BONEH D and FREENMAN D M. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures[C]. The IACR International Conference on Practice and Theory of Public-Key Cryptography, Taormina, Italy, 2011: 1–16. doi: 10.1007/978-3-642-19379-8_1.

江明明：男，1984年生，博士，讲师，研究方向为格公钥密码、数字签名.

郭宇燕：女，1984年生，博士，讲师，研究方向为抗泄露密码、信息安全.

余 磊：男，1978年生，硕士，副教授，研究方向为信息安全、安全协议.

宋万干：男，1963年生，硕士，教授，研究方向为信息安全、数据挖掘.

魏仕民：男，1962年生，博士，教授，研究方向为序列密码、信息安全.