格上基于身份的单向代理重签名

江明明*① 胡予濮① 王保仓① 来齐齐① 刘振华②
①(西安电子科技大学综合业务网理论与关键技术国家重点实验室 西安 710071)
②(西安电子科技大学数学与统计学院 西安 710071)

摘 要：代理重签名是简化密钥管理的重要工具，能够提供路径证明和简化证书管理等。目前的代理重签名方案都是基于整数分解与离散对数的，其在量子环境下都不安全。针对这个问题，该文利用原像抽样技术与固定维数的格基委派技术，基于格上的小整数解问题(Small Integer Solution, SIS)的困难性，构造了格上基于身份的代理重签名方案。该方案具有单向性，多次使用性等性质。与其它具有相同性质的基于身份的代理重签名相比，该方案具有验证开销小，渐近复杂度低等优点。

关键词：代理重签名；格；高斯抽样；小整数解问题
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2014)03-0645-05
DOI: 10.3724/SP.J.1146.2013.00818

Identity-based Unidirectional Proxy Re-signature over Lattice

Jiang Ming-ming① Hu Yu-pu① Wang Bao-cang① Lai Qi-qi① Liu Zhen-hua②
①(*State Key Laboratory of Integrated Service Networks*, *Xidian University*, *Xi'an* 710071, *China*)
②(*School of Mathematics and Statistics*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Proxy re-signature is an important tool for simplifying key management, and can be used to prove a proof for a path, manage group signatures, simplify certificate management and so on. Currently, proxy re-signature schemes are based on large integer factorization and discrete logarithm which are not security in quantum setting. For this problem, the first identity-based proxy re-signature scheme over lattices is constructed in this paper, which uses preimage sampleable technology and lattice basis delegation in fixed dimension technology. Its security is based on the hardness of Small Integer Solution (SIS) problem. This scheme possesses the properties of unidirectional, multi-use and so on. Compared with the previous schemes which have the same properties, the proposed scheme has the advantage of low verification cost and low asymptotic computational complexity.

Key words: Proxy re-signature; Lattice; Gaussian sampling; Small Integer Solution (SIS) problem

1 引言

代理重签名是由Blazed等人[1]在1998年欧密会上提出的一种新的密码原型。在代理重签名中，一个半可信的代理者可以把一个消息在Alice的签名转化为Bob的签名，并且这个代理者不能得到Alice或Bob的签名密钥的任何信息。由于代理重签名相当于一个转换函数，把一个用户的签名转换成另一个用户的签名，这使其在很多方面都有重要的应用，例如简化密钥管理，提供路径证明，管理群签名，简化证书管理等。但是在以后的一段时间内，却没有新的成果出现。2005年，Ateniese等人[2]进一步研究了代理重签名并给出了形式化的安全定义和新的应用环境。他们提出了两个代理重签名方案并给出了一个公开问题，即如何构造一个多次使用的单向代理重签名方案。Libert等人[3]解决了这个公开问题，构造了一个多次使用的单向代理重签名方案。Shao等人[4]利用Schnorr签名[5]和文献[3]的代理重签名构造了第1个基于身份的多次使用的单向代理重签名方案。在文献[4]中利用文献[3]的代理重签名构造的方案，其验证开销随着重签名层数的增加呈线性增长，使得验证开销较大。然而，随着量子计算机的发展，该方案在量子环境下不再安全。因而，构造量子计算环境下的基于身份的代理重签名方案成为了一个有意义的问题。

格公钥密码作为量子环境下安全的公钥密码之一，具有良好的密码学性质。首先，格密码是一个线性密码，其大多数运算都是在小整数上进行，因此计算复杂度较低；其次，格密码上的困难问题在

2013-06-07 收到，2013-09-11 改回
国家自然科学基金(61173151, 61173152, 61100229)资助课题
*通信作者：江明明 jiangmm3806586@126.com

最差情况下与平均情况下是等价的；第三，目前不存在比传统算法更好的量子算法来解决格上的困难问题，因此密码学家认为格密码在量子环境下是安全的。因此，格密码受到了越来越多密码学家的关注。2008年，Gentry等人[6]利用高斯抽样算法构造了格上的第1个可证明安全的格签名和第1个基于身份的加密方案。在此之后，格签名、基于身份的加密以及相关的方案进入了快速发展的时期，并取得了大量的成果[7−15]。本文利用文献[6]中的原像抽样技术与文献[8]中的固定维数的格基委派技术，构造一个在量子环境下安全的，并且具有单向性，多次使用性，以及验证开销小的基于身份的代理重签名方案。

2 基础知识

2.1 格

设 $\boldsymbol{B}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m)\in\mathbb{R}^{m\times m}$ 是一个 $m\times m$ 阶矩阵，并且 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\in\mathbb{R}^m$ 是线性无关的向量。一个 m 维满秩格 Λ 定义为向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 的所有整系数线性组合所构成的集合，即

$$\Lambda=\mathcal{L}(\boldsymbol{B})=\left\{\boldsymbol{B}\boldsymbol{c}=\sum_{i=1}^{m}c_i\boldsymbol{b}_i\mid c_i\in\mathbb{Z}\right\}\tag{1}$$

这里 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 构成了格 Λ 的一组基。我们主要关注的是整数格，即格 $\Lambda\subseteq\mathbb{Z}^m$。

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：

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

定理 1[16] 设 $q\geq 3$ 是一个奇数且 $m=\lceil 6n\log_2 q\rceil$。那么，存在一个概率多项式时间算法 $\mathrm{TrapGen}(1^n)$，输出矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}\in\mathbb{Z}_q^{m\times m}$，其中 $\boldsymbol{A}$ 在 $\mathbb{Z}_q^{n\times m}$ 上是接近于均匀的，$\boldsymbol{T}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一组基，且除了一个不可忽略的概率外都满足

$$\left\|\widetilde{\boldsymbol{T}}\right\|\leq O\left(\sqrt{n\log_2 q}\right),\ \ \|\boldsymbol{T}\|\leq O(n\log_2 q)\tag{3}$$

定义 2 小整数解问题 $\mathrm{SIS}_{q,n,m,\beta}$ (Small Integer Solution)：给定随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和实数 β，找到非零向量 $\boldsymbol{e}$，使得 $\boldsymbol{A}\boldsymbol{e}=\boldsymbol{0}\bmod q$ 且 $\|\boldsymbol{e}\|\leq\beta$。

2.2 离散高斯

对任意的 $\boldsymbol{c}\in\mathbb{R}^m$，实数 $\sigma>0$，m 维格 Λ，定义格 Λ 上的离散高斯分布为

$$D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\sum\limits_{x\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})},\quad\forall\boldsymbol{x}\in\mathbb{R}^m\tag{4}$$

引理 1[6] 设 $q\geq 2$，矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m},m>n$。$\boldsymbol{T}_{\boldsymbol{A}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一组基，$\sigma\geq\left\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\right\|\cdot\omega\left(\sqrt{\log m}\right)$。那么，对于 $\boldsymbol{c}\in\mathbb{R}^m,\boldsymbol{u}\in\mathbb{Z}_q^n$ 有：

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

(2) 存在一个概率多项式时间算法 $\mathrm{SampleGaussian}(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\sigma,\boldsymbol{c})$，抽取一个格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 中的向量 $\boldsymbol{x}$，使得 $\boldsymbol{x}$ 的分布统计接近于 $D_{\Lambda,\sigma,\boldsymbol{c}}$；

(3) 存在一个概率多项式时间算法 $\mathrm{SamplePre}(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},\sigma)$，抽取一个 $\Lambda_q^{u}(\boldsymbol{A})$ 中的向量 $\boldsymbol{x}$，使得 $\boldsymbol{x}$ 的分布统计接近于 $D_{\Lambda_q^{u}(\boldsymbol{A}),\sigma,\boldsymbol{c}}$。

引理 2[6] 设 n 和 q 是正整数，且 q 是素数，$m\geq 2n\log_2 q$。那么对于 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\sigma\geq\omega\left(\sqrt{\log_2 m}\right)$，$\boldsymbol{e}\sim D_{\mathbb{Z}^m,\sigma}$，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。

定义 3 对于任意 n 维格 Λ 和正实数 $\varepsilon>0$，光滑参数 $\eta_{\varepsilon}(\Lambda)$ 定义为满足 $\rho_{1/s}(\Lambda^{*}\setminus\{0\})<\varepsilon$ 的最小的 s。

引理 3[10] 设 $\Lambda\subseteq\mathbb{Z}^m$ 是一个格，参数 $\sigma\in\mathbb{R}$。对于 $i=1,2,\cdots,k$，$\boldsymbol{v}_i\in\mathbb{Z}^m$。$X_i$ 是从 $D_{\Lambda+\boldsymbol{v}_i,\sigma}$ 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 $g:=\gcd(c_1,c_2,\cdots,c_k),\boldsymbol{v}:=\sum_{i=1}^{k}c_i\boldsymbol{v}_i$。假设对于可忽略的 ε，$\sigma>\|\boldsymbol{c}\|\cdot\eta_{\varepsilon}(\Lambda)$，那么 $Z=\sum_{i=1}^{k}c_iX_i$ 的分布统计接近于 $D_{g\Lambda+\boldsymbol{v},\|\boldsymbol{c}\|\sigma}$。

2.3 重要算法

定义 4 对于一个矩阵 $\boldsymbol{A}\in\mathbb{Z}^{m\times m}$，如果 $\boldsymbol{A}\bmod q$ 作为 $\mathbb{Z}_q^{m\times m}$ 中的矩阵是可逆的，则称 $\boldsymbol{A}$ 是 $\mathbb{Z}_q$ 可逆的。

定义 5 设 $\sigma_{\boldsymbol{s}}=\sqrt{n\log_2 q}\cdot\omega\left(\sqrt{\log_2 m}\right)$，令 $D_{m\times m}$ 表示 $\mathbb{Z}^{m\times m}$ 上的矩阵分布，这些矩阵是按照分布 $(D_{\mathbb{Z}^m,\sigma_{\boldsymbol{R}}})^m$ 来抽取的并且在 $\mathbb{Z}^{m\times m}$ 上 $\mathbb{Z}_q$ 可逆。

算法 1[8] $\mathrm{Sample}\boldsymbol{R}(1^m)$：该算法的输出矩阵分布统计接近于 $D_{m\times m}$。

(1) 设 $\boldsymbol{T}_0$ 格 $\mathbb{Z}^m$ 上的标准基；

(2) 对于 $i=1,2,\cdots,m$，利用高斯抽样算法随机抽取一个 $\boldsymbol{r}_i\xleftarrow{R}\mathrm{SampleGaussian}(\mathbb{Z}^m,\boldsymbol{T}_0,\sigma_{\boldsymbol{r}},\boldsymbol{0})$；

(3) 如果 $\boldsymbol{R}$ 是 $\mathbb{Z}_q$ 可逆的，则输出 $\boldsymbol{R}$；否则重复第(2)步。

算法 2[7] 陷门基委派算法 $\mathrm{BasisDel}(\boldsymbol{A},\boldsymbol{R},\boldsymbol{T}_{\boldsymbol{A}},\sigma)$

(1) 设 $\boldsymbol{T}_{\boldsymbol{A}}=\{\boldsymbol{t}_1,\boldsymbol{t}_2,\cdots,\boldsymbol{t}_m\}\subseteq\mathbb{Z}^m$，计算 $\boldsymbol{T}_{\boldsymbol{B}}'=\{\boldsymbol{R}\boldsymbol{t}_1,\boldsymbol{R}\boldsymbol{t}_2,\cdots,\boldsymbol{R}\boldsymbol{t}_m\}\subseteq\mathbb{Z}^m$，那么 $\boldsymbol{T}_{\boldsymbol{B}}'$ 是格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的一组线性无关的集合，这里 $\boldsymbol{B}=\boldsymbol{A}\boldsymbol{R}^{-1}\bmod q$；

(2) 把 $\boldsymbol{T}_{\boldsymbol{B}}'$ 转化成格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的一个基 $\boldsymbol{T}_{\boldsymbol{B}}''$，但 $\boldsymbol{T}_{\boldsymbol{B}}''$ 不是一个随机的基；

(3) 利用随机化算法 $\mathrm{RandBasis}(\boldsymbol{T}_{\boldsymbol{B}}'',\sigma)$，输出格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的一个随机的小基 $\boldsymbol{T}_{\boldsymbol{B}}$。

算法 3[8] SampleRwithBasis($\boldsymbol{A}$)，设 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m \in \mathbb{Z}_q^n$ 是 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ 的 m 个列向量。

(1)利用概率多项式时间算法 TrapGen(1^n)产生一个随机的矩阵 $\boldsymbol{B} \in \mathbb{Z}_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的一个小基 $\boldsymbol{T}_{\boldsymbol{B}}$，且满足 $\left\|\widetilde{\boldsymbol{T}}_{\boldsymbol{B}}\right\| \le \sigma_{\boldsymbol{R}} / \omega\left(\sqrt{\log_2 m}\right)$。

(2)对于 $i = 1,2,\cdots,m$，进行如下操作：

(a)抽取一个向量 $\boldsymbol{r}_i \leftarrow \text{SamplePre}(\boldsymbol{B},\boldsymbol{T}_{\boldsymbol{B}},\sigma_{\boldsymbol{R}},\boldsymbol{a}_i)$，那么 $\boldsymbol{B}\boldsymbol{r}_i = \boldsymbol{a}_i \bmod q$；

(b)重复(a)直到 $\boldsymbol{r}_i$ 与 $\boldsymbol{r}_1,\boldsymbol{r}_2,\cdots,\boldsymbol{r}_{i-1}$ 是 $\mathbb{Z}_q$ 线性无关的。

(3)令 $\boldsymbol{R} = \{\boldsymbol{r}_1,\boldsymbol{r}_2,\cdots,\boldsymbol{r}_m\} \in \mathbb{Z}^{m\times m}$，那么 $\boldsymbol{R}$ 是 $\mathbb{Z}_q$ 上的一个秩为 m 的矩阵。输出矩阵 $\boldsymbol{R}$ 和 $\boldsymbol{T}_{\boldsymbol{B}}$。

引理 4[8] 设 $m \ge 2n\log_2 q$ 且 q 是素数。对于 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$，算法 SampleRwithBasis($\boldsymbol{A}$)输出一个矩阵 $\boldsymbol{R}$，其分布统计接近于 $D_{m\times m}$。生成的格 $\Lambda_q^{\perp}(\boldsymbol{A}\boldsymbol{R}^{-1})$ 的基 $\boldsymbol{T}_{\boldsymbol{B}}$ 满足 $\left\|\widetilde{\boldsymbol{T}}_{\boldsymbol{B}}\right\| \le \sigma_{\boldsymbol{R}} / \omega\left(\sqrt{\log_2 m}\right)$，这里 $\boldsymbol{B} = \boldsymbol{A}\boldsymbol{R}^{-1} \bmod q$。

3　基于身份的代理重签名

3.1 方案介绍

该方案中使用了两个Hash函数，$H_1 : \{0,1\}^* \to \mathbb{Z}_q^{m\times m} : id \to H(id) \sim D_{m\times m}$，$H_2 : \{0,1\}^* \to \mathbb{Z}_q^n$（$\{0,1\}^*$ 表示任意比特长的二进制）。

(1)主密钥生成：输入安全参数 1^n，运行概率多项式时间算法 TrapGen(1^n)产生一个随机的矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一个陷门基 $\boldsymbol{T} \in \mathbb{Z}^{m\times m}$，并且 $\left\|\widetilde{\boldsymbol{T}}\right\| \le O\left(\sqrt{n\log_2 q}\right)$，（$\|\bullet\|$ 表示欧几里得范数）。原像抽样函数 $f_{\boldsymbol{A}}(\boldsymbol{x}) = \boldsymbol{A}\boldsymbol{x} \bmod q$（$f : \mathbb{Z}^m \to \mathbb{Z}_q^n$）。那么主公钥为 $\boldsymbol{A}$，主私钥为 $\boldsymbol{T}$。

(2)用户私钥提取：输入用户的身份 id，计算 $R_{id} = H_1(id)$，利用算法 BasisDel(A,R_{id},T_A,σ)输出用户的公钥 $A_{id} = AR_{id}^{-1} \bmod q$，私钥 $\boldsymbol{T}_{id}$。

(3)代理重签名密钥生成：输入用户 id_1 公钥 $pk_{id_1} = \boldsymbol{A}_{id_1}$，用户 id_2 的公钥 $pk_{id_2} = \boldsymbol{A}_{id_2}$ 和私钥 $sk_{id_2} = \boldsymbol{T}_{id_2}$。设 $\boldsymbol{A}_{id_1} = (\boldsymbol{a}_{11},\boldsymbol{a}_{12},\cdots,\boldsymbol{a}_{1m})^{\mathrm{T}}$，这里 $\boldsymbol{a}_{1i} \in \mathbb{Z}_q^n$。对每一个 $\boldsymbol{a}_{1i}, i = 1,2,\cdots,m$，利用原像抽样算法 SamplePre($\boldsymbol{A}_{id_2},\boldsymbol{T}_{id_2},\boldsymbol{a}_{1i},\sigma$)抽取一个向量 $\boldsymbol{s}_i$ 使得 $\boldsymbol{A}_{id_2}\boldsymbol{s}_i = \boldsymbol{a}_{1i} \bmod q$ 且 $\left\|\boldsymbol{s}_i\right\| \le \sigma\sqrt{m}$。令 $\boldsymbol{S}_{id_1\to id_2} = (\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_m) \in \mathbb{Z}^{m\times m}$，那么 $\boldsymbol{A}_{id_2}\boldsymbol{S}_{id_1\to id_2} = \boldsymbol{A}_{id_1} \bmod q$ 且 $\left\|\boldsymbol{S}_{id_1\to id_2}\right\| \le \sigma\sqrt{m}$。输出重签名密钥 $rk_{id_1\to id_2} = \boldsymbol{S}_{id_1\to id_2}$。

(4)签名：

第 1 层签名：输入私钥 $sk = \boldsymbol{T}$ 和一个消息 m，签名如下：

(a)选择一个随机的向量 $\boldsymbol{r} \in \{0,1\}^*$，计算 $\boldsymbol{u} = H_2(m\|\boldsymbol{r}) \in \mathbb{Z}_q^n$；

(b)利用原像抽样算法 SamplePre($\boldsymbol{A},\boldsymbol{T},\boldsymbol{u},\sigma$)抽取一个向量 $\boldsymbol{e}_1$ 使得 $\boldsymbol{A}\boldsymbol{e}_1 = \boldsymbol{u} \bmod q$ 且 $\left\|\boldsymbol{e}_1\right\| \le \sigma\sqrt{m}$；

(c)输出 $(\boldsymbol{e}_1, r)$ 作为消息 m 的第 1 层签名。

第 i 层签名：输入私钥 $sk = \boldsymbol{T}$ 和一个消息 m，签名如下：

(a)选择一个随机的向量 $\boldsymbol{r} \in \{0,1\}^*$，计算 $\boldsymbol{u} = H_2(m\|\boldsymbol{r}) \in \mathbb{Z}_q^n$；

(b)利用原像抽样算法 SamplePre($\boldsymbol{A},\boldsymbol{T},\boldsymbol{u},\sigma^i m^{(i-1)/2}$)抽取一个向量 $\boldsymbol{e}_i$ 使得 $\boldsymbol{A}\boldsymbol{e}_i = \boldsymbol{u} \bmod q$ 且 $\left\|\boldsymbol{e}_i\right\| \le \sigma^i m^{i/2}$；

(c)输出 $(\boldsymbol{e}_i, \boldsymbol{r})$ 作为消息 m 的第 i 层签名。

(5)重签名：输入重签名密钥 $\boldsymbol{r}k_{id_1\to id_2} = \boldsymbol{S}_{id_1\to id_2}$，用户 id_1 的公钥 $pk_{id_1} = \boldsymbol{A}_{id_1}$，一个消息 m 和它对应的第 l 签名 $(\boldsymbol{e}_{id_1,l}, \boldsymbol{r})$。首先检查 $\boldsymbol{A}_{id_1}\boldsymbol{e}_{id_1,l} = \boldsymbol{u} \bmod q$ 且 $||\boldsymbol{e}_{id_1,l}|| \le \sigma^l m^{l/2}$。如果 $\boldsymbol{e}_{id_1,l}$ 不是消息 m 的第 l 层签名，则停止；否则，计算 $\boldsymbol{e}_{id_2,l+1} = \boldsymbol{S}_{id_1\to id_2}\boldsymbol{e}_{id_1,l}$，则 $(\boldsymbol{e}_{l+1}, \boldsymbol{r})$ 为用户 $id_1 \to id_2$ 的重签名。

(6)验证：输入用户 id_2 的公钥 $pk_{id_2} = \boldsymbol{A}_{id_2}$，消息 m 和用户 $id_1 \to id_2$ 对应的重签名 $(\boldsymbol{e}_{id_2,l+1}, \boldsymbol{r})$。如果 $\boldsymbol{A}_{id_2}\boldsymbol{e}_{id_2,l+1} = \boldsymbol{u} \bmod q$ 且 $\left\|\boldsymbol{e}_{id_2,l+1}\right\| \le \sigma^{l+1} m^{(l+1)/2}$，则接受，否则拒绝。

3.2 安全性分析

定理 2 在随机预言机模型下，该方案在小整数解问题($\text{SIS}_{q,n,m,\beta}$)的困难假设下是安全的；换句话说，如果敌手能够产生一个有效的伪造签名，则对于一个随机矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$，能找到一个向量 $\boldsymbol{v} \ne 0$，且 $\|\boldsymbol{v}\| \le 2\sigma\sqrt{m}$，使得 $\boldsymbol{A}\boldsymbol{v} = \boldsymbol{0} \bmod q$。

证明 考虑方案的外部安全与内部安全。

内部安全：由于在本方案中，第 2 层签名包含第 1 层签名，所以在内部安全中只考虑限制代理安全和和被授权人安全。

限制代理安全：假设存在一个概率多项式时间敌手 $\mathcal{A}$ 在进行了 q_H 随机预言机询问，q_s 次签名询问和 q_{rk}（$< m$）次重签名密钥询问后，可以以不可忽略的概率 ε 攻破该方案，那么构造一个算法 $\mathcal{B}$，利用敌手 $\mathcal{A}$ 的能力来解决 $\text{SIS}_{q,n,m,\beta}$ 困难问题实例。

系统参数：输入一个随机的矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$，算法 $\mathcal{B}$ 输出一个非零向量 $\boldsymbol{v}$ 使得 $\boldsymbol{A}\boldsymbol{v} = \boldsymbol{0} \bmod q$ 且 $\|\boldsymbol{v}\| \le 2\sigma\sqrt{m}$。

设置公钥：当 $\mathcal{A}$ 询问用户 id_i, $i \in \{1,2,\cdots,\kappa\}$，$\mathcal{B}$ 需要准备 κ 个公钥 $\boldsymbol{A}_{id_1},\boldsymbol{A}_{id_2},\cdots,\boldsymbol{A}_{id_\kappa}$，生成过程如下：

(1)设置 $\boldsymbol{A} = \boldsymbol{A}_{id_t} = \boldsymbol{A}_0\boldsymbol{R}_{id_t}^{-1} \bmod q$。首先 $\mathcal{B}$ 利用 Sample$\boldsymbol{R}$ 算法产生一个 $\mathbb{Z}_q$ 可逆的矩阵 $\boldsymbol{R}_{id_t}$，接着计算 $\boldsymbol{A}_0 = \boldsymbol{A}\boldsymbol{R}_{id_t} \bmod q$，$\boldsymbol{A}_0$ 为主公钥。

(2)利用 SampleRwithBasis($\boldsymbol{A}_0$)算法产生 $\kappa - 1$ 个公、私钥对 $(\boldsymbol{A}_{id_i},\boldsymbol{T}_{id_i})$ 和 $\boldsymbol{R}_{id_i}$，$i = 1,2,\cdots,t-1,t+$

$1,\cdots,\kappa$。

预言机询问：$\mathcal{B}$ 需要回答 4 个预言机询问：随机预言机 H_1，随机预言机 H_2，签名预言机 $\mathcal{O}_{\text{sign}}$ 和重签名密钥预言机 $\mathcal{O}_{\text{rekey}}$。$\mathcal{B}$ 回答预言机询问如下：

随机预言机 H_1 询问：当敌手 $\mathcal{A}$ 询问用户 id_i 时，$\mathcal{B}$ 查找并返回 $\boldsymbol{R}_{id_i}$ 给 $\mathcal{A}$。

随机预言机 H_2 询问：$\mathcal{B}$ 维持一个表 $(id_i,\boldsymbol{u}_k,\boldsymbol{e}_k,(m_k,r_k))$。当敌手询问 H_2 时，如果 (m_k,r_k) 在列表中，则 $\mathcal{B}$ 返回 $\boldsymbol{u}_k$ 给 $\mathcal{A}$。否则，$\mathcal{B}$ 抽取一个向量 $\boldsymbol{e}_k \leftarrow D_{\mathbb{Z}^m,\sigma}$ 并计算 $\boldsymbol{u}_k=\boldsymbol{A}_{id_i}\boldsymbol{e}_k \bmod q$，存储 $(id_i,\boldsymbol{u}_k,\boldsymbol{e}_k,(m_k,r_k))$ 并返回 $\boldsymbol{u}_k$ 给 $\mathcal{A}$。

签名询问：敌手 $\mathcal{A}$ 对 (id_i,m_k) 进行签名询问。假设 m_k 已经进行过随机预言机 H_2 询问，$\mathcal{B}$ 在列表中查找 $(id_i,\boldsymbol{u}_k,\boldsymbol{e}_k,(m_k,r_k))$ 并返回 $\boldsymbol{e}_k$ 给 $\mathcal{A}$。

重签名密钥询问：敌手 $\mathcal{A}$ 对 (id_i,id_j) 进行重签名密钥询问。若 $i=t$ 或 $j=t$，则停止。否则，$\mathcal{B}$ 计算重签名密钥 $rk_{id_i\to id_j}$ 如下：利用用户 id_i 的公钥 $\boldsymbol{A}_{id_i}$，用户 id_j 的公、私钥 $(\boldsymbol{A}_{id_j},\boldsymbol{T}_{id_j})$ 以及重签名密钥生成算法生成重签名密钥 $rk_{id_i\to id_j}=\boldsymbol{S}_{id_i\to id_j}$，使得 $\boldsymbol{A}_{id_j}\boldsymbol{S}_{id_i\to id_j}=\boldsymbol{A}_{id_i} \bmod q$，发送 $\boldsymbol{S}_{id_i\to id_j}$ 给 $\mathcal{A}$。

伪造：不失一般性，假设 $\mathcal{A}$ 选择 $\boldsymbol{A}_{id_t}$ 作为挑战公钥(概率为 $1/\kappa$)，并且在输出一个伪造之前 $\mathcal{A}$ 已经对挑战消息 m^* 进行过随机预言机 H_2 询问，那么 $\mathcal{A}$ 输出一个伪造 $(id_t,(m^*,r^*),e^*)$。

下文对该归约进行分析。首先，对于随机预言机 H_1 的询问，$\mathcal{B}$ 对于身份 id_i 的询问回答为 $\boldsymbol{R}_{id_i}$，由算法 1 可知 $\boldsymbol{R}_{id_i}$ 服从 $D_{m\times m}$ 分布，与随机预言机 H_2 的分布是不可区分的。其次，对于随机预言机 H_2 的询问，$\mathcal{B}$ 对消息 m_k 的询问 H_2 的回答 $\boldsymbol{u}_k=\boldsymbol{A}_{id_i}\boldsymbol{e}_k \bmod q$，由引理 2 可知，$\boldsymbol{u}_k$ 的分布与 $\mathbb{Z}_q^n$ 上的均匀分布是不可区分的，即与 H_2 的输出分布是不可区分的。再次，对于签名询问，由引理 1 可知，$\mathcal{B}$ 的回答 $\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,\sigma}$ 的分布与原像抽样的分布是不可区分的。最后，由引理 3 可知，重签名密钥的询问回答也是合理的。

当敌手 $\mathcal{A}$ 输出伪造 $(id_t,(m^*,r^*),e^*)$，$\mathcal{B}$ 在列表中查找 $(id_t,(m^*,r^*),\boldsymbol{e}_{m^*})$ 并且输出 $\boldsymbol{v}=\boldsymbol{e}_{m^*}-\boldsymbol{e}^*$ 作为 $\text{SIS}_{q,n,m,\beta}$ 问题 $\boldsymbol{A}\boldsymbol{x}=\boldsymbol{0} \bmod q$ 的解。由于 $(id_t,(m^*,r^*),e^*)$ 和 $(id_t,(m^*,r^*),e^*)$ 是同一个消息 m^* 的签名。那么

$$\boldsymbol{A}_{id_t}\boldsymbol{e}^* \bmod q = H\left(m^*\left\|r^*\right.\right) \bmod q = \boldsymbol{A}_{id_t}\boldsymbol{e}_{m^*} \bmod q \quad (5)$$

从而得到 $\boldsymbol{A}(\boldsymbol{e}^*-\boldsymbol{e}_{m^*})=\boldsymbol{A}_{id_t}(\boldsymbol{e}^*-\boldsymbol{e}_{m^*})=\boldsymbol{0} \bmod q$。由于 $\left\|\boldsymbol{e}^*\right\|$，$\left\|\boldsymbol{e}_{m^*}\right\|\le\sigma\sqrt{m}$ 且 $\boldsymbol{e}^*\ne\boldsymbol{e}_{m^*}$，所以有 $\left\|\boldsymbol{e}^*-\boldsymbol{e}_{m^*}\right\|\le 2\sigma\sqrt{m}$ 且 $\boldsymbol{e}^*-\boldsymbol{e}_{m^*}\ne\boldsymbol{0}$。

被授权人安全：假设存在一个概率多项式时间敌手 $\mathcal{A}$ 在进行了 q_H 随机预言机询问，q_s 次签名询问和 q_{rk} 次重签名密钥询问后，可以以不可忽略的概率 ε 攻破该方案，那么构造一个算法 $\mathcal{B}$，利用敌手 $\mathcal{A}$ 的能力来解决 $\text{SIS}_{q,n,m,\beta}$ 困难问题实例。

系统参数：输入一个随机的矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，算法 $\mathcal{B}$ 输出一个非零向量 $\boldsymbol{v}$ 使得 $\boldsymbol{A}\boldsymbol{v}=\boldsymbol{0} \bmod q$ 且 $\|\boldsymbol{v}\|\le 2\sigma\sqrt{m}$。

设置公钥：当 $\mathcal{A}$ 询问用户 id_i，$i\in\{1,2,\cdots,\kappa\}$，$\mathcal{B}$ 需要准备 κ 个公钥 $\boldsymbol{A}_{id_1},\boldsymbol{A}_{id_2},\cdots,\boldsymbol{A}_{id_\kappa}$，生成过程如下：

(1)设置 $\boldsymbol{A}=\boldsymbol{A}_{id_1}=\boldsymbol{A}_0\boldsymbol{R}_{id_1}^{-1} \bmod q$。首先 $\mathcal{B}$ 利用 $\text{Sample}\boldsymbol{R}$ 算法产生一个 $\mathbb{Z}_q$ 可逆的矩阵 $\boldsymbol{R}_{id_1}$，接着计算 $\boldsymbol{A}_0=\boldsymbol{A}\boldsymbol{R}_{id_1} \bmod q$，$\boldsymbol{A}_0$ 为主公钥。

(2)利用 $\text{SampleRwithBasis}(\boldsymbol{A}_0)$ 算法产生 $\kappa-1$ 个公、私钥对 $(\boldsymbol{A}_{id_i},\boldsymbol{T}_{id_i})$ 和 $\boldsymbol{R}_{id_i}$，$i=2,3,\cdots,\kappa$。

预言机询问：$\mathcal{B}$ 需要回答 4 个预言机询问：随机预言机 H_1，随机预言机 H_2，签名预言机 $\mathcal{O}_{\text{sign}}$ 和重签名密钥预言机 $\mathcal{O}_{\text{rekey}}$。$\mathcal{B}$ 回答预言机询问如下：

随机预言机 H_1 询问：当敌手 $\mathcal{A}$ 询问用户 id_i 时，$\mathcal{B}$ 查找并返回 $\boldsymbol{R}_{id_i}$ 给 $\mathcal{A}$；

随机预言机 H_2 询问：$\mathcal{B}$ 维持一个表 $(id_i,\boldsymbol{u}_k,\boldsymbol{e}_k,(m_k,r_k))$。当敌手询问 H_2 时，如果 (m_k,r_k) 在列表中，则 $\mathcal{B}$ 返回 $\boldsymbol{u}_k$ 给 $\mathcal{A}$。否则，$\mathcal{B}$ 抽取一个向量 $\boldsymbol{e}_k\leftarrow D_{\mathbb{Z}^m,\sigma}$ 并计算 $\boldsymbol{u}_k=\boldsymbol{A}_{id_i}\boldsymbol{e}_k \bmod q$，存储 $(id_i,\boldsymbol{u}_k,\boldsymbol{e}_k,(m_k,r_k))$ 并返回 $\boldsymbol{u}_k$ 给 $\mathcal{A}$。

签名询问：敌手 $\mathcal{A}$ 对 (id_i,m_k) 进行签名询问。假设 m_k 已经进行过随机预言机 H_2 询问。$\mathcal{B}$ 在列表中查找 $(id_i,\boldsymbol{u}_k,\boldsymbol{e}_k,(m_k,r_k))$ 并返回 $\boldsymbol{e}_k$ 给 $\mathcal{A}$。

重签名密钥询问：敌手 $\mathcal{A}$ 对 (id_i,id_j) 进行重签名密钥询问。若 $i=1$ 则停止。否则，$\mathcal{B}$ 计算重签名密钥 $rk_{id_i\to id_j}$ 如下：利用用户 id_i 的公钥 $\boldsymbol{A}_{id_i}$，用户 id_j 的公、私钥 $(\boldsymbol{A}_{id_j},\boldsymbol{T}_{id_j})$ 以及重签名密钥生成算法生成重签名密钥 $rk_{id_i\to id_j}=\boldsymbol{S}_{id_i\to id_j}$，使得 $\boldsymbol{A}_{id_j}\boldsymbol{S}_{id_i\to id_j}=\boldsymbol{A}_{id_i} \bmod q$，发送 $\boldsymbol{S}_{id_i\to id_j}$ 给 $\mathcal{A}$。

伪造：不失一般性，假设 $\mathcal{A}$ 选择 $\boldsymbol{A}_{id_t}$ 作为挑战公钥(概率为 $1/\kappa$)，并且在输出一个伪造之前 $\mathcal{A}$ 已经对 m^* 进行过随机预言机 H_2 询问，那么 $\mathcal{A}$ 输出一个伪造 $(id_t,(m^*,r^*),e^*)$。

下文对该归约进行分析。首先，对于随机预言机 H_1 的询问，$\mathcal{B}$ 对于身份 id_i 的询问回答为 $\boldsymbol{R}_{id_i}$，由算法 1 和算法 3 可知 $\boldsymbol{R}_{id_i}$ 服从 $D_{m\times m}$ 分布，与随机预言机 H_2 的分布是不可区分的。其次，对于随机预言机 H_2 的询问，$\mathcal{B}$ 对消息 m_k 的询问 H_2 的回答 $\boldsymbol{u}_k=\boldsymbol{A}_{id_i}\boldsymbol{e}_k \bmod q$，由引理 2 可知，$\boldsymbol{u}_k$ 的分布与 $\mathbb{Z}_q^n$ 上的均匀分布是不可区分的，即与 H_2 的输出分布是不可区分的。再次，对于签名询问，$\mathcal{B}$ 的回答 $\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,\sigma}$ 的分布与原像抽样的分布是不可区分的。最后，由引理 3 可知，重签名密钥的询问回答也是

合理的。

当敌手 $\mathcal{A}$ 输出伪造 $(id_t,(m^*,r^*),e^*)$，$\mathcal{B}$ 在列表中查找 $(id_t,(m^*,r^*),e^*)$ 并且输出 $\boldsymbol{v}=\boldsymbol{e}_{m^*}-\boldsymbol{e}^*$ 作为 $\mathrm{SIS}_{q,n,m,\beta}$ 问题 $\boldsymbol{A}\boldsymbol{x}=\boldsymbol{0}\bmod q$ 的解。由于 $(id_t,(m^*,r^*),e^*)$ 和 $(id_t,(m^*,r^*),e^*)$ 是同一个消息 m^* 的签名。那么

$$\boldsymbol{A}_{id_t}\boldsymbol{e}^* \bmod q = H\left(m^*\left\|r^*\right.\right)\bmod q = \boldsymbol{A}_{id_t}\boldsymbol{e}_{m^*} \bmod q \quad (6)$$

从而得到 $\boldsymbol{A}(\boldsymbol{e}^*-\boldsymbol{e}_{m^*})=\boldsymbol{A}_{id_t}(\boldsymbol{e}^*-\boldsymbol{e}_{m^*})=\boldsymbol{0}\bmod q$。由于 $\left\|\boldsymbol{e}^*\right\|$，$\left\|\boldsymbol{e}_{m^*}\right\|\le\sigma\sqrt{m}$ 且 $\boldsymbol{e}^*\ne\boldsymbol{e}_{m^*}$，所以有 $\left\|\boldsymbol{e}^*-\boldsymbol{e}_{m^*}\right\|\le 2\sigma\sqrt{m}$ 且 $\boldsymbol{e}^*-\boldsymbol{e}_{m^*}\ne\boldsymbol{0}$。

对于外部安全，除了重签名询问外，其过程与内部安全的限制代理安全相似。而重签名过程可以利用重签名密钥来模拟，在此不作描述。　　证毕

4　效率分析

该重签名方案除了使用一个杂凑函数的运算外，仅仅使用了小整数上的矩阵-向量的模乘运算以及高效抽样算法，其计算复杂度分别为 $O(n^2)$，$\tilde{O}(n^2)$，所以计算复杂度较低。将本文方案与具有相同性质的文献[4]的方案 2 进行比较，结果如表 1 所示。

表 1　方案的效率对比

	文献[4]的方案 2	本文方案
验证开销增长速度	$O(n)$	$O(1)$
签名长度增长速度	$O(n)$	$O(n)$
签名的计算复杂度	$O(ln^3)$	$\tilde{O}(n^2)$
重签名的计算复杂度	$O(n^3)$	$O(n^2)$

在文献[4]的方案 2 中，第 1 层重签名的验证开销需要 6 个配对运算，而第 l 层重签名的验证则需要 $4l+2$ 个配对运算，其验证开销的增长速度是线性的。而本文方案中的验证开销为一个矩阵与向量的模乘运算，不随重签名次数的增加而改变。而对于签名长度，文献[4]的方案 2 与本文方案都是线性增长的。

5　结论

本文利用原像抽样技术与固定维数的格基委派技术，构造了格上基于身份的多次使用的单向代理重签名方案。该方案基于格上的小整数解问题(Small Integer Solution, SIS)，保证了其在量子环境下的安全性。

参 考 文 献

[1] Blaze M, Bleumer G, and Strauss M. Divertible protocols and atomic proxy cryptography[J]. *Lecture Notes in Computer Science* (*LNCS*), 1998, 1403: 127–144.

[2] Ateniese G and Hohenberger S. Proxy re-signatures: new definitions, algorithms, and applications[C]. ACM Conference on Computer and Communications Security 2005, Alexandria, VA, USA, 2005: 310–319.

[3] Libert B and Vergnaud D. Multi-use unidirectional proxy re-signatures[C]. ACM Conference on Computer and Communications Security 2008, Alexandria, Virginia, USA, 2008: 511–520.

[4] Shao Jun, Feng Min, Zhu Bin, *et al*.. The security model of unidirectional proxy re-signature with private re-signature key[J]. *Lecture Notes in Computer Science* (*LNCS*), 2010, 6168: 216–232.

[5] Schnorr C P. Efficient identification and signatures for smart cards[J]. *Lecture Notes in Computer Science* (*LNCS*), 1990, 435: 688–689.

[6] Gentry C, Peikert C, and Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]. Symposium on Theory of Computing 2008, Victoria, British Columbia, Canada, 2008: 197–206.

[7] Cash D, Hofheinz D, Kiltz E, *et al*.. Bonsai trees, or how to delegate a lattice basis[J]. *Lecture Notes in Computer Science* (*LNCS*), 2010, 6110: 523–552.

[8] Agrawal S, Boneh D, and Boyen X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE[J]. *Lecture Notes in Computer Science* (*LNCS*), 2010, 6223: 98–115.

[9] 王凤和, 胡予濮, 王春晓. 格上基于盆景树模型的环签名[J]. 电子与信息学报, 2010, 32(10): 2400–2403.

[10] Boneh D and Freeman D. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures[J]. *Lecture Notes in Computer Science* (*LNCS*), 2011, 6571: 1–16.

[11] Lyubashevsky V. Lattice signatures without trapdoors[J]. *Lecture Notes in Computer Science* (*LNCS*), 2012, 7237: 738–755.

[12] Micciancio D and Peikert C. Trapdoors for lattices: simpler, tighter, faster, smaller[J]. *Lecture Notes in Computer Science* (*LNCS*), 2012, 7237: 700–718.

[13] Agrawal S, Boyen X, Vaikuntanathan V, *et al*.. Functional encryption for threshold functions (or fuzzy IBE) from lattices[J]. *Lecture Notes in Computer Science* (*LNCS*), 2012, 7293: 280–297.

[14] Ducas L and Nguyen P Q. Faster Gaussian lattice sampling using lazy floating-point[J]. *Lecture Notes in Computer Science* (*LNCS*), 2012, 7658: 25–42.

[15] Boyen X. Attribute-based functional encryption on lattices[J]. *Lecture Notes in Computer Science* (*LNCS*), 2013, 7785: 122–142.

[16] 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.

江明明：男，1984 年生，博士生，研究方向为格公钥密码、数字签名.

胡予濮：男，1955 年生，博士生导师，教授，研究方向为格公钥密码、流密码等.

王保仓：男，1979 年生，硕士生导师，副教授，研究方向为格公钥密码、多变量密码等.