doi:10.3969/j.issn.1000-436x.2014.08.026

可证安全的有效代理签名方案

曾捷[1,2]，聂伟[1,2]
(1. 深圳大学 信息工程学院，广东 深圳 518060；2. 深圳市现代通信与信息处理重点实验室，广东 深圳 518060)

摘 要：针对固定维数的格基委托算法或格上基于盆景树生成的代理签名方案中私钥和签名的长度均过大的问题，提出一种较小尺寸的代理签名方案。该方案对随机预言机进行了合并优化，并使用一个更小范数但是向量盲化的消息，从而控制代理签名私钥的维数，其安全性基于格上最短向量问题和小整数解问题的困难性,并且满足代理签名方案所有的安全性要求。与现有方案相比,该方案有效地减小了代理签名私钥和代理签名的长度，使代理私钥长度与原始签名用户私钥长度相当。

关键词：无陷门；小范数；代理签名；盆景树
中图分类号：TP 309 **文献标识码**：A **文章编号**：1000-436X(2014)08-0216-07

Provably secure and efficient proxy signature scheme

ZENG Jie[1,2], NIE Wei[1,2]
(1. College of Information Engineering, Shenzhen University, Shenzhen 518060, China;
2. Shenzhen Modern Communication and Information Processing Key Lab, Shenzhen 518060, China)

Abstract: The size of proxy signature secret key in proxy signature scheme based on lattice basis delegation in fixed dimension or bonsai tree is greater than that of original signature secret key. Aiming at the situation above, a new efficient proxy signature scheme is proposed. The random oracles are combined in the scheme and a smaller vector norm blind message is used to control the dimension of proxy signature secret key. The security of proposed scheme is based on the hardness of shortest vector problem and small integer solution problem, and the scheme satisfies the security requirements of a proxy signature scheme. Compared with other schemes over lattice, the size of proxy signature secret key and proxy signature is reduced, and the size of proxy signature secret key is equivalent to that of the original signature secret key in magnitude.

Key words: without trapdoor; small norm; proxy signature; bonsai tree

1 引言

Mambo 等在 1996 年提出代理签名[1]的概念。在该方案中，原始签名者委托代理签名者完成签名。验证者可以通过该方案鉴别该签名是代理签名者完成的还是原始签名者完成的，从而保证了代理签名者不能伪造原始签名者的签名。随着对量子计算机及量子算法的深入研究，研究者发现利用量子计算机与量子算法可在多项式时间内解决大整数分解和离散对数问题[2]。因此，研究新的可应对量子环境下攻击的代理签名方案十分必要。格密码是一种具有良好密码学性质的后量子密码，近年来受到广泛关注。首先，格密码是线性密码，运算主要为矩阵−向量的乘积运算；其次，格密码可以保证

收稿日期：2013-12-10；**修回日期**：2014-05-12
基金项目：国家自然科学基金资助项目(61103174, 61301182, 61375015)；教育部博士点基金资助项目(20134408120004)；广东省自然科学基金资助项目(S2013010012227, S2013040016857, S2013040015481)；广东省教育厅基金资助项目(2013KJCX0162, 2013LYM0077)；深圳市科技计划基础研究基金资助项目(JCYJ20130329105415965, JCYJ20120613113535357)
Foundation Items: The National Natural Science Foundation of China (61103174, 61301182, 61375015); The Ph.D Programs Foundation of Ministry of China (20134408120004); The Natural Science Foundation of Guangdong Province (S2013010012227, S2013040016857, S2013040015481); Scientific and Technological Innovation Project of Department of Education of Guangdong Province (2013KJCX0162, 2013LYM0077); Fundamental Research General Program of Shenzhen City (JCYJ20130329105415965, JCYJ20120613113535357)

最差情况与平均情况困难性等价；再次，找不到比传统算法更好的量子算法来解决格上的困难问题。因此，格公钥密码在量子环境下是安全的。近年来，格密码研究得到很大的发展[3~7]。很多学者对基于格的代理签名进行了研究，如 Jiang 等[8]利用文献[4]的盆景树原理构造了一个基于格的代理签名方案。该方案的代理签名私钥的维数是原始签名私钥维数的 2 倍，并且代理者是未受保护的，即原始签名者可以伪造代理签名者的签名。夏峰等[9]和 Wang 等[10]分别利用盆景树原理构造了基于格的代理签名方案；Kim[11]、Biswas[12]和 Swapna[13]等利用文献[6]固定维数的格基委托技术构造了一个基于身份的代理签名方案。固定维数的格基委托技术虽然没有增加代理签名私钥的维数，但是却明显增大了私钥的范数。本文利用无陷门签名技术，使用一个更小范数但是向量盲化的消息控制代理签名私钥的维数，构造了一个基于格的代理签名方案，有效减小了代理签名私钥与代理签名的长度。

2　基础知识

2.1　格

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

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

其中，$\boldsymbol{b}_1,\cdots,\boldsymbol{b}_m$ 构成了格 Λ 的一组基。本文关注的是整数格，即格 $\Lambda\subseteq \boldsymbol{Z}^m$。

定义 1　设 $\boldsymbol{\alpha}$ 是一个向量，则 $\boldsymbol{\alpha}$ 的 l_p 范数定义为 $\|\boldsymbol{\alpha}\|_p=\left(\sum \boldsymbol{\alpha}_i{}^p\right)^{1/p}$，当 $p=2$ 时，称为欧几里得范数。对于欧几里得范数，一般把 $\|\boldsymbol{\alpha}\|_2$ 中的下标省略，记为 $\|\boldsymbol{\alpha}\|$。

2.2　格上困难问题

定义 2[14]　最短向量问题（SVP, shortest vector problem）。给定格的一组基 $\boldsymbol{B}$，找出格 $\mathcal{L}(\boldsymbol{B})$ 中的最短向量 $\boldsymbol{u}$，使对格上的任意向量 $\boldsymbol{v}$，都有 $\|\boldsymbol{u}\|\leqslant\|\boldsymbol{v}\|$。

定义 3[15]　最短独立向量问题（SIVP, shortest independent vector problem）。设 $\boldsymbol{B}$ 是格 Λ 的一组基，目标是输出 n 个线性无关的格向量的集合 $\boldsymbol{S}\subset\Lambda$，满足 $\|\boldsymbol{S}\|\leqslant\gamma(n)\lambda_n(\Lambda)$，$\lambda_n(\Lambda)$ 表示包含 n 个线性无关的格向量的球的最小半径。

定义 4[16]　小整数解问题（SIS, small integer solution problem）。给定一个随机的矩阵 $\boldsymbol{A}\in \boldsymbol{Z}_q^{n\times m}$ 和一个实数 β，找到一个非零向量 $\boldsymbol{e}$，使 $\boldsymbol{Ae}=0 \bmod q$ 且 $\|\boldsymbol{e}\|\leqslant\beta$。

引理 1[16]　对于任意多项式边界的 m，$\beta=\mathrm{poly}(n)$，那么对任意的素数 $q\geqslant\beta\omega\left(\sqrt{n\log n}\right)$，平均情况下的 $\mathrm{SIS}_{q,m,\beta}$ 问题和 $\mathrm{ISIS}_{q,m,\beta}$ 问题与最差情况下的近似 SIVP 问题的困难度是相同的，其中，近似 SIVP 问题的近似因子 $\gamma=\beta\tilde{O}\left(\sqrt{n}\right)$。

引理 2[7]　对于任意的矩阵 $\boldsymbol{A}\in \boldsymbol{Z}_q^{n\times m}$，$m>64+n\log q/\log(2d+1)$，对随机选择的 $\boldsymbol{s}\in\{-d,\cdots,0,\cdots,d\}^m$，以 $1-2^{-100}$ 的概率存在另一个 $\boldsymbol{s}'\in\{-d,\cdots,0,\cdots,d\}^m$ 使 $\boldsymbol{As}=\boldsymbol{As}'$。

2.3　离散高斯分布

对于任意的 $\sigma>0$，定义以 c 为中心，以 σ 为参数的高斯函数为

$$\rho_{\sigma,c}(x)=\exp\left(-\pi\|x-c\|^2/\sigma^2\right),\forall x\in \boldsymbol{R}^m$$

对于任意 $c>0$，实数 $\sigma>0$，一个 m 维格 Λ，定义格 Λ 上的离散高斯分布为

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

当 $c=0$ 时，简写为 $D_{\Lambda,\sigma}$。整数构成的格的高斯分布简写为 $D_{\sigma,\boldsymbol{c}}$。

引理 3[3]　设 $q\geqslant 2$，矩阵 $\boldsymbol{A}\in \boldsymbol{Z}_q^{n\times m}$，$m>n$。设 $\boldsymbol{T}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一组基，$\sigma\geqslant\|\tilde{\boldsymbol{T}}\|\omega\left(\sqrt{\log m}\right)$。那么对于 $c\in \boldsymbol{R}^m$，$\boldsymbol{u}\in \boldsymbol{Z}_q^n$，有

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

2.4　无陷门签名和小范数矩阵

David 等[17]在 2010 年把盆景树的思想引入到格中，给出了对格进行扩展和对基进行随机化操作的具体方法。在盆景树模型下以某个格作为根节点生成一个更大维数的格作为下一级的枝节点。这种由“根”到“枝”的“生长”（undirected growth）可以是无陷门的，此时“盆景师”在分级过程中没有使用陷门，因此没有任何特权。在同样的安全登记下，基于无陷门技术的代理签名私钥与代理签名的

尺寸会比使用陷门的小 2 个数量级，这很大程度是因为隐藏在陷门生成算法中的常量的缘故。而在无陷门技术下，这些常量可以改善甚至被去除[18]。

在基于格签名中，潜在的困难问题通常是小整数解问题 SIS（见定义 4）。其中，给定一个随机的矩阵，非零向量的长度非常接近于签名的长度。因此，改善基于格签名的挑战是如何降低签名方案的范数。代理签名范数的区间一般较大，而且盲化向量的范数也较大，因而，去盲后范数值可能会溢出，造成签名私钥的维数过大。鉴于以上问题，要求用户用一个更小范数但是满足向量盲化消息[19]。采用小范数矩阵传递的前提是必须保证此时格上 SIS 问题的困难性。这样，用户在进行去盲变换时，合理增加向量的范数也不会超出验证算法的要求，从而有效地使代理签名私钥的维数小于原始用户签名私钥的维数。

3 方案介绍与安全性证明

新方案的基本意图是降低代理签名私钥与代理签名的尺寸，从签名值中攻击者既不能得到单个私钥的倍式， 也不能得到多个私钥的线性组合式，而只能得到多个私钥的复杂函数。新方案利用无陷门签名技术，使用一个更小范数但是向量盲化的消息控制代理签名私钥的维数，为了保持简洁的计算和提高效率，新方案还对随机预言机进行了合并优化。

3.1 方案介绍

设存在以下 3 个散列函数

$$H_1:\{0,1\}^*\to D_{H_1}=\left\{\boldsymbol{c}:\boldsymbol{c}\in\{-1,0,1\}^k,\|\boldsymbol{c}\|_1\leqslant\kappa_1\right\},$$

$$H_2:\{0,1\}^*\to D_{H_2}=\left\{\boldsymbol{c}:\boldsymbol{c}\in\{-1,0,1\}^l,\|\boldsymbol{c}\|_1\leqslant\kappa_2\right\},$$

$$H_3:id\to\{-1,0,1\}^{k\times l}$$

其中，H_1,H_2 被看作为随机预言机。这里，$l<k<m$，κ_i 满足 $2^{\kappa_i}\binom{n}{\kappa_i}\geqslant 2^{100}$，$i=1,2$。

为了提高计算效率，把其中 2 个随机预言机合并为一个随机预言机，其输出长度为原来长度的和，如 $H_2:\{0,1\}^*\to\left\{\boldsymbol{c}:\boldsymbol{c}\in\{-1,0,1\}^{k+l},\|\boldsymbol{c}\|_1\leqslant\kappa\right\}$，

这里 H_2 被看作为随机预言机，另一个散列函数为 $H_1:id\to\{-1,0,1\}^{k\times l}$，这里 $l<k<m$。

密钥生成：随机选择矩阵 $\boldsymbol{A}\in\boldsymbol{Z}_q^{n\times m}$，$\boldsymbol{S}\in\{-d,\cdots,0,\cdots,d\}^{m\times k}$，$\boldsymbol{S}_1\in\{-d,\cdots,0,\cdots,d\}^{m\times k}$，计算

$$\boldsymbol{T}=\boldsymbol{A}\boldsymbol{S}\bmod q\in\boldsymbol{Z}_q^{n\times k}$$

$$\boldsymbol{T}_1=\boldsymbol{A}\boldsymbol{S}_1\bmod q\in\boldsymbol{Z}_q^{n\times k}$$

原始签名者的公、私钥对为 $(\boldsymbol{A},\boldsymbol{T},\boldsymbol{S})$，代理者自己的公、私钥对为 $(\boldsymbol{A},\boldsymbol{T}_1,\boldsymbol{S}_1)$。

代理签名密钥生成: 对于代理签名者 id，计算

$$\boldsymbol{U}_{id}=H_3(id)\in\{-1,0,1\}^{k\times l}$$

$$\boldsymbol{S}_2=\boldsymbol{S}\boldsymbol{U}_{id}\in\boldsymbol{Z}_q^{m\times l}$$

$$\boldsymbol{T}_2=\boldsymbol{T}\boldsymbol{U}_{id}\bmod q\in\boldsymbol{Z}_q^{n\times l}$$

其中，代理签名密钥为 $\boldsymbol{S}_2$，对应的公钥为 $\boldsymbol{T}_2$。原始签名者通过安全信道把代理签名密钥 $\boldsymbol{S}_2$ 发送给代理者。

代理者验证：代理者收到代理签名密钥后，检查 $\boldsymbol{A}\boldsymbol{S}_2=\boldsymbol{T}\boldsymbol{U}_{id}\bmod q$ 是否成立，若成立，则接受代理签名密钥，否则拒绝。

代理签名：输入一个消息 μ，代理者自己的私钥 $\boldsymbol{S}_1$，代理签名密钥 $\boldsymbol{S}_2$，签名如下。

1）消息盲化：输入一个消息 μ，计算 $\boldsymbol{H}=h(\mu)$，以零为中心按离散正态分布 $D_{z^m,a^\omega(\sqrt{\lg n})}$ 随机选择向量 $\boldsymbol{c}=(\boldsymbol{c}_1,\cdots,\boldsymbol{c}_m)$，满足 $\|\boldsymbol{c}\|\leqslant a^\omega\left(\sqrt{\log n}\right)\sqrt{m}$ 以极大概率成立。$\boldsymbol{A}\boldsymbol{c}$ 近似服从均匀分布。设签名者掌握一个 n 维格 Λ 的一组小范数的基 $\boldsymbol{B}$（好基），$\tilde{\boldsymbol{B}}$ 为基 $\boldsymbol{B}$ 的施密特正交基，任意选择 $t\in\boldsymbol{Z}$，$1<t<x<\left\|\tilde{\boldsymbol{B}}\right\|-1$，计算 $u=(t^{-1}\boldsymbol{H}+\boldsymbol{A}\boldsymbol{c})\bmod q$。

2）代理者自己的私钥 $\boldsymbol{S}_1$，代理签名密钥 $\boldsymbol{S}_2$，签名如下：选择 2 个向量 $\boldsymbol{y}_1,\boldsymbol{y}_2\leftarrow D_\sigma^m$；

3）计算

$$\boldsymbol{c}_1=H_1(\boldsymbol{A}\boldsymbol{y}_1,\mu)\in(-1,0,1)^k$$

$$\boldsymbol{c}_2=H_2(\boldsymbol{A}\boldsymbol{y}_2,\mu)\in\{-1,0,1\}^l$$

4）计算

$$\boldsymbol{z}_1=\boldsymbol{S}_1\boldsymbol{c}_1+\boldsymbol{y}_1\in\boldsymbol{Z}_q^m$$

$$\boldsymbol{z}_2=\boldsymbol{S}_2\boldsymbol{c}_2+\boldsymbol{y}_2\in\boldsymbol{Z}_q^m$$

5）以 $\min\left(\dfrac{D_\sigma^m(\boldsymbol{z}_1)}{MD_{\boldsymbol{S}_1\boldsymbol{c}_1,\sigma}^m(\boldsymbol{z}_1)},1\right)$ 的概率输出 $(\boldsymbol{z}_1,\boldsymbol{c}_1)'$ 以 $\min\left(\dfrac{D_\sigma^m(\boldsymbol{z}_2)}{MD_{\boldsymbol{S}_2\boldsymbol{c}_2,\sigma}^m(\boldsymbol{z}_2)},1\right)$ 的概率输出 $(\boldsymbol{z}_2,\boldsymbol{c}_2)'$；

6）去盲：得到签名$(\boldsymbol{z}_1,\boldsymbol{c}_1)'$，$(\boldsymbol{z}_2,\boldsymbol{c}_2)'$后计算

$$(\boldsymbol{z}_1,\boldsymbol{c}_1)=\boldsymbol{t}\left((\boldsymbol{z}_1,\boldsymbol{c}_1)'-\boldsymbol{c}\right)$$

$$(\boldsymbol{z}_2,\boldsymbol{c}_2)=\boldsymbol{t}\left((\boldsymbol{z}_2,\boldsymbol{c}_2)'-\boldsymbol{c}\right)$$

其中，$(\boldsymbol{z}_1,\boldsymbol{c}_1)$，$(\boldsymbol{z}_2,\boldsymbol{c}_2)$作为消息$\mu$的签名。

验证：输入消息μ及其对应的签名$(\boldsymbol{z},\boldsymbol{c})$，矩阵$\boldsymbol{A}$、$\boldsymbol{T}_1$、$\boldsymbol{T}_2$，验证$\|\boldsymbol{z}\|\leqslant 2\sigma\sqrt{m}$，$\boldsymbol{c}=H_2\left(\boldsymbol{Az}-(\boldsymbol{T}_1\|\boldsymbol{T}_2)\boldsymbol{c}_1,\mu\right)$是否同时成立。若成立，则接受，否则拒绝。

3.2　安全性证明

代理签名可证明安全性理论评估的指标主要包括代理签名的正确性、不可伪造性和原始签名者的安全性。以下定理 1 证明了代理签名的正确性，定理 2 和定理 3 的不可伪造性说明了任何人都不能伪造代理签名者的签名，保证了代理签名者的安全性。

定理 1　（正确性）对于消息μ及其对应的代理签名$(\boldsymbol{z}_1,\boldsymbol{c}_1)$，$(\boldsymbol{z}_2,\boldsymbol{c}_2)$，需验证$\|\boldsymbol{z}_1\|,\|\boldsymbol{z}_2\|\leqslant 2\sigma\sqrt{m}$，$\boldsymbol{c}_1=H_1\left(\boldsymbol{Az}_1-\boldsymbol{T}_1\boldsymbol{c}_1,\mu\right)$，$\boldsymbol{c}_2=H_2\left(\boldsymbol{Az}_2-\boldsymbol{T}_2\boldsymbol{c}_2,\mu\right)$同时成立。

证明　首先，$\|\boldsymbol{z}_i\|=\|\boldsymbol{S}_i\boldsymbol{c}_i+\boldsymbol{y}_i\|\leqslant\|\boldsymbol{S}_i\boldsymbol{c}_i\|+\|\boldsymbol{y}_i\|\leqslant 2\sigma\sqrt{m}$，$i=1,2$。其次，$\boldsymbol{Az}_i-\boldsymbol{T}_i\boldsymbol{c}_i=\boldsymbol{A}(\boldsymbol{S}_i\boldsymbol{c}_i+\boldsymbol{y}_i)-\boldsymbol{T}_i\boldsymbol{c}_i=\boldsymbol{AS}_i\boldsymbol{c}_i+\boldsymbol{Ay}_i-\boldsymbol{T}_i\boldsymbol{c}_i=\boldsymbol{Ay}_i$，故$\boldsymbol{c}_i=H_1(\boldsymbol{Ay}_i,\mu)=H_1(\boldsymbol{Az}_i-\boldsymbol{T}_i\boldsymbol{c}_i,\mu)$，$i=1,2$。因此，这个方案的正确性是显然的。

定理 2　（不可伪造性）假设敌手$\mathcal{A}$能够以一个较大数量级而不可忽略的概率ε在一个概率多项式时间内产生一个有效的伪造代理签名，那么就存在一个算法$\mathcal{B}$，对于一个随机矩阵$\boldsymbol{A}\in\boldsymbol{Z}_q^{n\times m}$，能够以至少

$$\left(\frac{1}{2}-2^{-100}\right)\left(\varepsilon-\frac{1}{|D_{H_2}|}\right)\left(\frac{\varepsilon-1/|D_{H_2}|}{q_s+q_{H_2}}-\frac{1}{|D_{H_2}|}\right)$$

的概率找到一个非零向量$\boldsymbol{v}$，使$\|\boldsymbol{v}\|\leqslant(4\sigma+2d\kappa_2)\sqrt{m}$，且$\boldsymbol{Av}=0$。

证明　分 2 种情况讨论代理签名的不可伪造性。其一，恶意的原始签名者（拥有代理签名密钥，但没有代理签名者的密钥）不能伪造代理签名；其二，恶意的第三方（没有代理签名密钥，也没有代理签名者的密钥）不能够伪造代理签名。由于恶意的第三方的攻击能力弱于恶意的原始签名者，所以只需要讨论恶意的原始签名者的攻击即可，即要证明任何人在知道代理签名密钥的情况下，不能伪造代理签名。不妨设存在一个概率多项式时间敌手$\mathcal{A}$（恶意的原始签名者），在进行了q_{H_2}次随机预言机H_2询问和q_S次签名询问之后，可以利用较大数量级以不可忽略的概率ε伪造一个有效的代理签名。敌手$\mathcal{A}$已经知道了代理签名密钥，那么它需要产生一个代理签名者本身签名的伪造，即产生一个伪造签名$(\mu,\boldsymbol{z},\boldsymbol{c})$，使$\boldsymbol{c}=H_2\left(\boldsymbol{Az}-\boldsymbol{Tc},\mu\right)$，且$\|\boldsymbol{z}\|\leqslant 2\sigma\sqrt{m}$。要构造一个多项式时间算法$\mathcal{B}$，利用$\mathcal{A}$的优势来破解小整数解问题$\mathrm{SIS}_{q,m,\beta}$。$\mathcal{B}$需要模拟随机预言机$H_2$和签名预言机$O_S$，模拟如下。

1）随机预言机H_2询问：$\mathcal{B}$维护一个列表$(\mu_j,\boldsymbol{z}_j,\boldsymbol{c}_j)$，当敌手$\mathcal{A}$询问消息$\mu_j$的随机预言机$H_2$值时，$\mathcal{B}$首先检查列表中是否存在$\mu_j$，如果存在，则输出$\boldsymbol{c}_j$。如果不存在，从$D_{H_2}$中随机选择一个$\boldsymbol{c}_j$，并选择一个$\boldsymbol{z}_j\leftarrow D_\sigma^m$，令$\boldsymbol{c}_j=H_2\left(\boldsymbol{Az}_j-\boldsymbol{Tc}_j,\mu_j\right)$。$\mathcal{B}$存储$(\mu_j,\boldsymbol{z}_j,\boldsymbol{c}_j)$，并返回$\boldsymbol{c}_j$给$\mathcal{A}$作为对$\mu_j$的随机预言机$H_2$询问。

2）签名询问：在敌手$\mathcal{A}$询问消息μ_j的签名的时候，如果对所有要进行签名询问的消息已经进行过随机预言机H_2询问，则$\mathcal{B}$从列表中取回$(\mu_j,\boldsymbol{z}_j,\boldsymbol{c}_j)$，返回$(\boldsymbol{z}_j,\boldsymbol{c}_j)$给$\mathcal{A}$。

3）伪造：当敌手$\mathcal{A}$决定结束这些询问之后，$\mathcal{A}$输出一个伪造$(\mu,\boldsymbol{z},\boldsymbol{c})$。$\mathcal{B}$要利用这个伪造签名$(\mu,\boldsymbol{z},\boldsymbol{c})$来解决小整数解问题。由于已经在签名询问中询问过签名询问的消息了，那么敌手$\mathcal{A}$最多进行$t=q_s+q_{H_2}$次随机预言机H_2询问，$\mathcal{B}$随机选择$\boldsymbol{c}_1,\cdots,\boldsymbol{c}_t\leftarrow D_{H_2}$。这个伪造的签名满足$\|\boldsymbol{z}\|\leqslant 2\sigma\sqrt{m}$，且$\boldsymbol{c}=H_2\left(\boldsymbol{Az}-\boldsymbol{Tc},\mu\right)$。对于给定$\boldsymbol{u}=\boldsymbol{Az}-\boldsymbol{Tc}$，敌手$\mathcal{A}$生成一个$\boldsymbol{c}$使$\boldsymbol{c}=H_2\left(\boldsymbol{u},\mu\right)$的概率为$1/|D_{H_2}|$，因此$\boldsymbol{c}$以$1-1/|D_{H_2}|$概率是消息$\mu$在随机预言机$H_2$询问时得到的，即$\boldsymbol{c}\in\{\boldsymbol{c}_1,\cdots,\boldsymbol{c}_t\}$，那么敌手$\mathcal{A}$产生一个有效的伪造，并且$\boldsymbol{c}\in\{\boldsymbol{c}_1,\cdots,\boldsymbol{c}_t\}$的概率为$\varepsilon-1/|D_{H_2}|$。可以设定$\boldsymbol{c}=\boldsymbol{c}_j$。这里$\boldsymbol{c}_j$有 2 种来源，一种产生于签名询问过程中，另一种产生于随机预言机H_2询问过程中。

当$\boldsymbol{c}_j$在签名询问中产生。由于$\boldsymbol{c}=\boldsymbol{c}_j$，则$H_2\left(\boldsymbol{Az}-\boldsymbol{Tc},\mu\right)=H_2\left(\boldsymbol{Az}_j-\boldsymbol{Tc},\mu_j\right)$。如果$\mu\neq\mu_j$或$\boldsymbol{Az}-\boldsymbol{Tc}\neq\boldsymbol{Az}_j-\boldsymbol{Tc}$，则意味着敌手$\mathcal{A}$找到了$\boldsymbol{c}_j$的

一个原像。所以，有 $\mu=\mu_j$， $\boldsymbol{Az}-\boldsymbol{Tc}=\boldsymbol{Az}_j-\boldsymbol{Tc}$，所以 $\boldsymbol{A}\left(\boldsymbol{z}-\boldsymbol{z}_j\right)=0$。$\boldsymbol{z}-\boldsymbol{z}_j\neq 0$，又由于 $\|\boldsymbol{z}\|\leqslant 2\sigma\sqrt{m}$，$\|\boldsymbol{z}_j\|\leqslant 2\sigma\sqrt{m}$，那么有 $\|\boldsymbol{z}-\boldsymbol{z}_j\|\leqslant 4\sigma\sqrt{m}$。

当 $\boldsymbol{c}_j$ 是在随机预言机 H_2 询问过程中产生的。如果在这种假设条件下，$\mathcal{B}$ 记录敌手 $\mathcal{A}$ 对消息 μ 的伪造签名 $\left(\boldsymbol{z},\boldsymbol{c}_j\right)$，并产生新的随机的 $\boldsymbol{c}_1',\cdots,\boldsymbol{c}_t'\leftarrow D_{H_2}$。则依据文献[20]中一般的分支引理可以得到，敌手 $\mathcal{A}$ 产生一个新的有关消息 μ 的伪造签名 $\left(\boldsymbol{z}',\boldsymbol{c}_j'\right)$（$\boldsymbol{c}_j\neq\boldsymbol{c}_j'$）的概率为

$$\left(\varepsilon-\frac{1}{|D_{H_2}|}\right)\left(\frac{\varepsilon-1/|D_{H_2}|}{q_s+q_{H_2}}-\frac{1}{|D_{H_2}|}\right)$$

即敌手 $\mathcal{A}$ 产生消息 μ 的伪造签名 $\left(\boldsymbol{z},\boldsymbol{c}_j\right)$ 和 $\left(\boldsymbol{z}',\boldsymbol{c}_j'\right)$ 的概率。由于 $\boldsymbol{Az}-\boldsymbol{Tc}_j=\boldsymbol{Az}'-\boldsymbol{Tc}_j'$，把 $\boldsymbol{T}=\boldsymbol{AS}$ 代入，得到 $\boldsymbol{A}\left(\boldsymbol{z}-\boldsymbol{z}'+\boldsymbol{Sc}_j'-\boldsymbol{Sc}_j\right)=0$，由于 $\|\boldsymbol{z}\|\leqslant 2\sigma\sqrt{m}$，$\|\boldsymbol{z}'\|\leqslant 2\sigma\sqrt{m}$，$\|\boldsymbol{Sc}_j\|\leqslant d\kappa_2\sqrt{m}$，$\|\boldsymbol{Sc}_j'\|\leqslant d\kappa_2\sqrt{m}$，所以 $\|\boldsymbol{z}-\boldsymbol{z}'+\boldsymbol{Sc}_j'-\boldsymbol{Sc}_j\|\leqslant\left(4\sigma+2d\kappa_2\right)\sqrt{m}$。

现在说明 $\boldsymbol{z}-\boldsymbol{z}'+\boldsymbol{Sc}_j'-\boldsymbol{Sc}_j\neq 0$。由引理 2 可知，以至少 $1-2^{-100}$ 的概率存在另一个私钥 $\boldsymbol{S}'$（至少有一列与 $\boldsymbol{S}$ 不同）使 $\boldsymbol{AS}=\boldsymbol{AS}'$，所以如果 $\boldsymbol{z}-\boldsymbol{z}_j'+\boldsymbol{S}\left(\boldsymbol{c}_j'-\boldsymbol{c}_j\right)=0$，则 $\boldsymbol{z}-\boldsymbol{z}_j'+\boldsymbol{S}'\left(\boldsymbol{c}_j'-\boldsymbol{c}_j\right)\neq 0$。因为 $\boldsymbol{S}$ 在 $\mathcal{B}$ 的整个模拟过程中并没有出现，所以敌手 $\mathcal{A}$ 无法确切得知 $\mathcal{B}$ 使用的究竟是哪一个，也就是说 $\mathcal{B}$ 得到非零向量的最小概率为 1/2。

定理 3（合并随机预言机后的不可伪造性）在随机预言机模型下，该方案在小整数解问题（$\mathrm{SIS}_{q,n,m,\beta}$）的困难假设下是安全的；也就是说，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 $\boldsymbol{A}\in\boldsymbol{Z}_q^{n\times m}$，能找到一个向量 $\boldsymbol{v}\neq 0$，且 $\boldsymbol{v}\leqslant 2\sigma m$，使 $\boldsymbol{Av}=0\bmod q$。

证明 假设敌手 $\mathcal{A}$ 在一个概率多项式时间内进行了 q_H 随机预言机询问，q_S 次签名询问和 q_{rk}（$q_{rk}<m$）次签名密钥询问后，有较大数量级的概率 ε 破解该方案，则系统可构造一个算法 $\mathcal{B}$，利用敌手 $\mathcal{A}$ 的能力来解决 $\mathrm{SIS}_{q,n,m,\beta}$ 困难问题实例。

1) 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 R_{id_i} 给 $\mathcal{A}$。R_{id_i} 为一个 $\boldsymbol{Z}_q$ 可逆的矩阵。

2) 随机预言机 H_2 询问：$\mathcal{B}$ 维持一个表 $\left(id_i,\mu_k,\boldsymbol{e}_k,\left(m_k,r_k\right)\right)$。当敌手询问 H_2 时，如果 $\left(m_k,r_k\right)$ 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 $\boldsymbol{e}_k\leftarrow D_{Z^m,\sigma}$ 并计算 $\mu_k=\boldsymbol{A}_{id_i}\boldsymbol{e}_k\bmod q$，存储 $\left(id_i,\mu_k,\boldsymbol{e}_k,\left(m_k,r_k\right)\right)$ 并返回 μ_k 给 $\mathcal{A}$。

3) 签名询问：敌手 $\mathcal{A}$ 对 $\left(id_i,m_k\right)$ 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 $\left(id_i,\mu_k,\boldsymbol{e}_k,\left(m_k,r_k\right)\right)$ 并返回 $\boldsymbol{e}_k$ 给 $\mathcal{A}$。

4) 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 μ^* 进行过随机预言机 H_2 询问，那么 $\mathcal{A}$ 输出一个伪造 $\left(id_t,\left(u^*,r^*\right),\boldsymbol{e}^*\right)$。

对该归约进行分析。首先，对于随机预言机 H_2 的询问，$\mathcal{B}$ 对于身份 id_i 的询问回答为 R_{id_i}，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 μ_k 的询问 H_2 的回答 $\mu_k=\boldsymbol{A}_{id_i}\boldsymbol{e}_k\bmod q$，由引理 2 可知，$\mu_k$ 的分布与 $\boldsymbol{Z}_q^n$ 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 $\boldsymbol{e}\leftarrow D_{Z^m,\sigma}$ 的分布与 H_2 的输出是不可区分的。最后，由引理 3 可知，签名密钥的询问回答也是合理的。

当敌手 $\mathcal{A}$ 输出伪造 $\left(id_t,\left(m^*,r^*\right),\boldsymbol{e}^*\right)$，$\mathcal{B}$ 在列表中查找 $\left(id_t,\left(m^*,r^*\right),\boldsymbol{e}_{m^*}\right)$ 并且输出 $\boldsymbol{e}_{m^*}-\boldsymbol{e}$ 作为 $\mathrm{SIS}_{q,n,m,\beta}$ 问题 $\boldsymbol{Ax}=0\bmod q$ 的解。由于 $\left(id_t,\left(m^*,r^*\right),\boldsymbol{e}^*\right)$ 和 $\left(id_t,\left(m^*,r^*\right),\boldsymbol{e}^*\right)$ 是同一个消息 m^* 的签名。那么 $\boldsymbol{A}_{id_t}\boldsymbol{e}^*\bmod q=H\left(m^*\|r^*\right)\bmod q=\boldsymbol{A}_{id_t}\boldsymbol{e}_{m^*}\bmod q$，从而得到 $\boldsymbol{A}\left(\boldsymbol{e}^*-\boldsymbol{e}_{m^*}\right)=\boldsymbol{A}_{id_t}\left(\boldsymbol{e}^*-\boldsymbol{e}_{m^*}\right)=0\bmod q$。由于 $\|\boldsymbol{e}^*\|,\|\boldsymbol{e}_{m^*}\|\leqslant\sigma\sqrt{m}$ $\boldsymbol{e}^*$，且 $\boldsymbol{e}^*\neq\boldsymbol{e}_{m^*}$，所以有 $\|\boldsymbol{e}^*-\boldsymbol{e}_{m^*}\|\leqslant 2\sigma\sqrt{m}$ 且 $\boldsymbol{e}^*-\boldsymbol{e}_{m^*}\neq 0$。

证毕。

3.3 方案对比

将优化方案与具有相同性质的相关文献的代理私钥（不包括代理者自己的私钥以及所产生的签名）、代理签名以及原始签名用户私钥的长度进行比较，结果如表 1 所示。

表 1　　相关方案的效率比较

方案	代理私钥长度/bit	代理签名长度/bit	原始签名用户私钥长度/bit	签名长度增长速度
文献[8]	$4m^2\log(LM\sqrt{2m})$	$2m\log(LM2m^2)$	$(n+m)\log(q)$	$o(n^2)$
文献[11]	$m^2\log(LM^4m^{3/2})$	$m\log(LM^5m^2)$	$(n+m)\log(q)$	$o(n^2)$
文献[12]	$4m^2\log(LM\sqrt{2m})$	$2m\log(LM2m^2)$	$(n+m)\log(q)$	$o(n^2)$
文献[13]	$m^2\log(LM^4m^{3/2})$	$m\log(LM^5m^2)$	$(n+m)\log(q)$	$o(n^2)$
优化方案	$m\log(2md+1)$	$m\log(12\sigma)$	$m\log(q)$	$o(n)$

其中，$L=O(\sqrt{n\log q})$，$M=\omega(\sqrt{\log m})$。对于参数d、σ，取$d=1$，$\sigma=12\kappa_2\sqrt{m}$。对于上述的尺寸结果，是通过范数来估计的。通过表 1 可以看出，优化方案的代理私钥和代理签名的长度要小于现有文献方案代理私钥和代理签名的长度。同时，优化方案的代理私钥长度与原始签名用户私钥长度数量级相当，而其他方案的代理私钥长度比原始签名用户私钥长度要大，说明优化方案在控制代理私钥和代理签名的尺寸和控制签名长度的增长上要优于其他同类方案。

比较相关文献的方案的性能，结果如表 2 所示。由表 2 可以看出优化方案与现有文献方案相比性能相当。

表 2　　相关方案的性能比较

方案	签名速度/步	验证速度/步
文献[8]	$o(n)$	$o(n^2)$
文献[11]	$o(n)$	$o(n^2)$
文献[12]	$o(n)$	$o(n^2)$
文献[13]	$o(n)$	$o(n^2)$
优化方案	$o(n)$	$o(n^2)$

表 3 是优化方案与相关文献安全性的对比。优化方案基于 Full-ID 模型, 该模型比 Selective-ID 和 Generalized Selective-ID 模型安全。

因此,本文的优化方案在综合以上私钥和签名长度、安全性和计算量等各方面具有明显的优势。

表 3　　相关方案的安全性比较

方案	基于格上困难问题	安全模型
文献[8]	大数分解困难性	Selective-ID
文献[11]	离散对数困难性	Full-ID
文献[12]	SIVP	Generalized Selective-ID
文献[13]	SVP	Selective-ID
优化方案	SVP/SIVP	Full-ID

4　结束语

现有格上的代理签名方案中代理签名私钥的尺寸与原始签名者的私钥尺寸相比过大，是目前格密码发展的瓶颈。针对这个问题，本文提出了一个基于格的代理签名方案。该方案将随机预言机合并优化，可提高近一倍的计算效率，通过控制代理签名私钥的维数来降低代理签名私钥的尺寸，使代理私钥尺寸接近原始签名用户私钥尺寸。本文证明了该方案在格上最短向量和小整数解困难问题下是安全的。

参考文献：

[1] MAMBO M, USUDA K, OKAMOTO K. Proxy signatures: delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals, 1996, 79(9):1338-1353.

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

[3] YAO, YAN Q, LI Z J, GUO H. A novel nonlinear network coding signature scheme determined by the SIS problem[J].International Journal of Security and its Applications, 2012, 6(2):403-408.

[4] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai trees, or how to delegate a lattice basis[J]. Journal of Cryptology, 2012, 25(4):601-639.

[5] AGRAWAL S, BONEH D, BOYEN X. Efficient lattice (H)IBE in the standard model[A]. EUROCRYPT 2010, LNCS[C]. Riviera, France, 2010. 553-572.

[6] AGRAWAL S, BONEH D, BOYEN X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE[A]. CRYPTO 2010, LNCS[C]. CA, USA, 2010.98-115.

[7] LYUBASHEVSKY V. Lattice signatures without trapdoors[A]. Eurocrypt 2012, LNCS[C]. Cambridge, UK, 2012. 738-755.

[8] JIANG Y L, KONG F Y, JU X L. Lattice-based Proxy signature[A]. CIS 2010[C]. Nanning, China, 2010. 382-385.

[9] 夏峰，杨波，马莎等. 基于格的代理签名方案[J]. 湖南大学学报（自然科学版），2011，38（6）：84-88.
XIA F, YANG B, MA S, *et al*. Lattice-based proxy signature scheme [J]. Journal of Hunan University(Natural Sciences)，2011, 38(6):84-88.

[10] WANG C X, QI M N. Lattice-based proxy signature scheme[J]. Journal of Information and Computational Science, 2011, 12(8):

2451-2458.

[11] KIM K S, HONG D, JEONG I R. Identity-based proxy signature from lattices[J]. Journal of Communications and Networks, 2013, 15(1): 1-7.

[12] BISWAS S, MISC J, MISC V. An identity-based authentication scheme for safety messages in wave-enabled vanets[J]. International Journal of Parallel, Emergent and Distributed Systems, 2012, 27(6): 541-546.

[13] SWAPNA G, REDDY P V, GOWRI T. Efficient identity-based multi-proxy multi-signcryption scheme using bilinear pairings over elliptic curves[A]. ICACCI 2013[C]. Mysore, India, 2013. 418-423.

[14] MICHAEL S L, TERRENCE J S. Learning over complete representations[J]. Neural Computation, 2000, 12(2): 337-365.

[15] MICCIANCIO D, SHA GOLDWASSER. Complexity of Lattice Problems: a Cryptographic Perspective[M]. Boston: Kluwer Academic Publishers, 2002:1-220.

[16] MICCIANCIO D, REGEV O. Worst-case to average-case reductions based on Gaussian measures[A]. Proceedings of 45th Annual IEEE Symposium on Foundations of Computer Science[C]. Rome, Italy, 2004. 372-381.

[17] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai trees, or how to delegate a lattice basis[A]. Advances in Cryptology- EUROCRYPT 2010[C]. Riviera, France, 2010.523-552.

[18] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[A]. EUROCRYPT 2012[C]. Cambridge, UK, 2012. 700-718.

[19] RÜCKERT M. Lattice-based blind signatures[EB/OL]. http://eprint.iacr.org/2008/322, 2010.

[20] BELLARE M, NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma[A]. Proceedings of ACM CCS 2006[C]. Alexandria, 2006.390-399.

作者简介：

曾捷（1975-），男，广东广州人，硕士，深圳大学实验师，主要研究方向为智能信息处理、信息安全等。

聂伟（1973-），男，河南三门峡人，博士，深圳大学讲师，主要研究方向为网络信息安全、网络性能分析与优化、网络资源分配和调度等。