具有消息恢复功能的无陷门格签名方案

张襄松[1] 刘振华[2,3,4]

(西安工业大学理学院 西安 710032)[1] (西安电子科技大学数学与统计学院 西安 710071)[2]

(中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)[3]

(桂林电子科技大学广西信息科学实验中心 桂林 541004)[4]

摘 要 利用Lyubashevsky拒绝抽样(无陷门)技术,提出了一个高效的具有消息恢复功能的格签名方案。新方案可以看作是具有消息恢复功能的Abe-Okamato签名的格密码版本。在随机预言机模型下,利用General Forking Lemma,证明了新方案的选择消息攻击下存在的不可伪造安全性依赖于格上小整数解困难问题假设。新方案没有使用高斯原像抽样作为签名,仅需要简单的矩阵与向量乘法运算,具有短的消息-签名总长度。

关键词 签名,格密码,消息恢复,小整数解问题,可证明安全

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.09.031

Non-trapdoors Lattice Signature Scheme with Message Recovery

ZHANG Xiang-song[1] LIU Zhen-hua[2,3,4]

(School of Science, Xi'an Technological University, Xi'an 710032, China)[1]

(School of Mathematics and Statistics, Xidian University, Xi'an 710071, China)[2]

(State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)[3]

(Guangxi Experiment Center of Information Science, Guilin University of Electronic Technology, Guilin 541004, China)[4]

Abstract Based on Lyubashevsky's rejection sampling approach (without trapdoors), a lattice-based signature scheme with message recovery was proposed. This scheme can be regarded as lattice-based cryptographic version of Abe-Okamato signature with message recovery. In the random oracle model, we proved the new scheme's existential unforgeability under chosen message attacks security relies on the Small Integer Solution hardness assumption by using the General Forking Lemma. The proposed scheme does not use Gauss pre-image sampling as a signature, requires just simple matrix-vector multiplication operations, and has short message- signature size.

Keywords Signature, Lattice-based cryptography, Message recovery, Small integer solution, Provable security

1 引言

在网络传输带宽受限的环境中,如Ad hoc网络,具有短的消息-签名对长度的签名方案非常适用。目前研究如何缩小消息及其签名总长度的方法基本上有两种:一种是设计短签名长度的方案,如在相同安全级别下BLS签名[1]的长度约为DSA签名长度的一半;另一种是压缩消息长度的签名方案,如Nyberghe等设计的具有消息恢复功能的签名方案[2]。现有的具有消息恢复功能的签名方案大多是基于传统数论困难问题构造的,如基于离散对数[2-4](ISO/IEC 9796-3方案[5]等)和基于RSA(ISO/IEC 9796-2方案[6]等)。Yang和Lin[7]将具有消息恢复功能的签名方案首次应用于多播消息的源认证,大大提高了实时应用的安全性和效率。

基于传统数论困难问题的消息恢复签名方案面临重大的安全隐患——量子算法攻击。Shor提出的在多项式时间内可以求解离散对数和大整数分解问题的量子算法,将导致传统的密码系统无法提供量子安全性。一旦实用的量子计算机诞生,当前采用的RSA密码算法、DSA算法等都将不再安全。所以研究构造量子环境下安全的密码算法——后量子密码学,成为当前密码学界研究的热点问题,其主要集中于格密码、多变量密码、基于Hash的密码和基于代数编码译码问题的密码等方面。1996年Ajtai[8]提出了第一个基于格上困难问题的公钥密码方案,使得国际密码学界对格密码的研究开始空前活跃起来。格密码拥有许多优势:运算简单,抵抗量子攻击,安全性依赖于困难问题的平均复杂度情形。这为基于格构造安全的密码方案提供了有力保证。格密码研究取得了丰富的成果,包括格签名方案[9-15],但是它们都没有涉及消息恢复功能。由于具有消息恢复功能的签名方案能够缩短消息

到稿日期:2013-11-26 返修日期:2014-01-31 本文受国家自然科学基金项目(61100229,61173151,11101321),陕西省教育厅科研计划项目(12JK0852),信息安全国家重点实验室开放基金项目(GW0704127001),广西信息科学实验中心经费,中央高校基本科研业务费项目(K5051270003)资助。

张襄松(1980-),女,博士,讲师,主要研究方向为密码学中的数学基础问题,E-mail:xs-zhang@hotmail.com;刘振华(1978-),男,博士,副教授,主要研究方向为密码学与信息安全。

及其签名的总长度，适用于资源受限的环境，本文基于 Lyubashevsky 无陷门的格签名方案[14]，构造一个具有消息恢复功能的格签名方案，并在随机模型下给出安全性证明。

2 预备知识

文中安全参数是正整数 n，其他的量都与它相关。矩阵和向量(均为列向量)分别用黑体大写字母和黑体小写字母表示。$\|\boldsymbol{v}\|_p$ 表示向量 $\boldsymbol{v}$ 的 p-范数(p 为 2 时，可省)。$\omega(\sqrt{\log m})$表示渐近增长速度比 $\sqrt{\log m}$快的函数。对分布 $\mathcal{D}$，$x\leftarrow\mathcal{D}$ 表示根据 $\mathcal{D}$ 选取 x。若将向量看成串，对于串 s 和 t，$|t|$表示用二进制表示 t 时的比特长度，$s\|t$ 和 $s\oplus t$ 分别表示二进制串级联和异或运算。$[s]_{l_1}$ 表示从 s 的二进制表示的最高位往低位依次取 l_1 比特，$[s]_{l_2}$ 表示从 s 的二进制表示的最低位往高位依次取 l_2 比特。

2.1 格

定义 1 令基 $\boldsymbol{B}=[\boldsymbol{b}_1,\cdots,\boldsymbol{b}_m]\in\mathbb{R}^{m\times m}$ 包含 m 个线性无关的向量，由基 $\boldsymbol{B}$ 生成的格定义为：$\Lambda=\mathcal{L}(\boldsymbol{B})=\{\boldsymbol{y}\in\mathbb{R}^m\mid\exists\boldsymbol{x}\in\mathbb{Z}_q^m,\boldsymbol{y}=\boldsymbol{B}\boldsymbol{x}=\sum_{i=1}^{m}x_i\boldsymbol{b}_i\}$。

特别地，对正整数 q，向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$ 和矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，两个 m 维满秩整数格分别定义为：

$$\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}_q^m\mid\boldsymbol{A}\boldsymbol{e}=0\bmod q\}$$

$$\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}_q^m\mid\boldsymbol{A}\boldsymbol{e}=\boldsymbol{u}\bmod q\}$$

2.2 小整数解(Small Integer Solution,SIS)问题及其困难假设

定义 2 给定一个均匀随机的矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和参数 n，$m(n)$，$q(n)$，$\beta(n)$。小整数解 $SIS_{q,n,m,\beta}$ 问题是寻找一个非零向量 $\boldsymbol{x}\in\mathbb{Z}_q^m$，满足 $\boldsymbol{A}\boldsymbol{x}=0\bmod q$，且 $\|\boldsymbol{x}\|<\beta$。

Gentry 和 Peikert 等人[11]运用离散高斯抽样算法简单且紧致地证明对多项式界 $m(n)$，$\beta(n)$ 和素数 $q\geqslant\beta\cdot\omega(\sqrt{n\log n})$，求解小整数解 $SIS_{q,n,m,\beta}$ 问题的平均困难复杂度与近似求解最短无关向量组问题和间隙最短向量问题的最坏困难复杂度等价。因此，多项式时间敌手求解 $SIS_{q,n,m,\beta}$ 问题的概率是可忽略的。

2.3 离散正态分布

定义 3 $\mathbb{R}^m$ 上以 $\sigma>0$ 为标准偏差，以 $\boldsymbol{v}\in\mathbb{Z}^m$ 为中心的连续正态分布函数定义为 $\rho_{\boldsymbol{v},\sigma}^m(\boldsymbol{x})$；$\mathbb{Z}^m$ 上以 $\sigma>0$ 为标准偏差，$\boldsymbol{v}\in\mathbb{Z}^m$ 为中心的离散正态分布函数定义为 $D_{\boldsymbol{v},\sigma}^m(\boldsymbol{x})$，其中：

$$\rho_{\boldsymbol{v},\sigma}^m(\boldsymbol{x})=\left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^m\mathrm{e}^{\frac{-\|\boldsymbol{x}-\boldsymbol{v}\|^2}{2\sigma^2}}$$

$$D_{\boldsymbol{v},\sigma}^m(\boldsymbol{x})=\frac{\rho_{\boldsymbol{v},\sigma}^m(\boldsymbol{x})}{\sum_{\boldsymbol{z}\in\mathbb{Z}^m}\rho_{\boldsymbol{v},\sigma}^m(\boldsymbol{z})}$$

当 $\boldsymbol{v}=0$ 时，$\rho_{\boldsymbol{v},\sigma}^m$ 和 $D_{\boldsymbol{v},\sigma}^m$ 可以分别简记为 ρ_σ^m 和 D_σ^m。下面是离散正态分布的一个结论[14]：

引理 1 对任意 $\sigma>0$ 和正整数 m，有

(i)$\Pr[\boldsymbol{x}\leftarrow D_\sigma^1:|x|>12\sigma]<2^{-100}$；

(ii)$\Pr[\boldsymbol{x}\leftarrow D_\sigma^m:\|\boldsymbol{x}\|>2\sigma\sqrt{m}]<2^{-m}$。

2.4 拒绝抽样技术

Lyubashevsky 利用拒绝抽样技术构造了高效的格签名方案[14]：签名私钥是 $\boldsymbol{S}\in\mathbb{Z}_q^{m\times k}$，公钥是 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}=\boldsymbol{A}\boldsymbol{S}\bmod q$，哈希函数 H 输出 $\mathbb{Z}^n$ 中小范数元素，对消息 μ，签名算法首先从离散高斯分布 D_σ^m 中抽取向量 $\boldsymbol{y}$，然后计算 $\boldsymbol{c}=H(\boldsymbol{A}\boldsymbol{y}\bmod q,\mu)$，最后输出签名 $(\boldsymbol{z}=\boldsymbol{S}\boldsymbol{c}+\boldsymbol{y},\boldsymbol{c})$。由于 $\boldsymbol{z}$ 的分布依赖于 $\boldsymbol{S}\boldsymbol{c}$ 的分布，因此依赖于 $\boldsymbol{S}$ 的分布。为消除签名对 $\boldsymbol{S}$ 的依赖，可以使用拒绝抽样技术。需要的签名分布是 D_σ^m，而从分布 $D_{\boldsymbol{S}\boldsymbol{c},\sigma}^m$ 中得到抽样。为使用拒绝抽样，需要找到一个正实数 M，对所有根据 D_σ^m 抽样的 $\boldsymbol{x}$ 满足 $D_\sigma^m(\boldsymbol{x})\leqslant M\cdot D_{\boldsymbol{S}\boldsymbol{c},\sigma}^m(\boldsymbol{x})$。下面的定理[14]证实了 M 的存在性。

定理 1 令 $\mathbf{V}$ 是 $\mathbb{Z}^m$ 的子集，且其元素的范数不超过 T，$\sigma\in\mathbb{R}$ 满足 $\sigma=\omega(T\sqrt{\log m})$，$h:\mathbf{V}\to\mathbb{R}$ 是一个概率分布。则存在一个常数 $M=O(1)$，使得下面两个算法输出的概率分布是一致的：(i)$\boldsymbol{c}\leftarrow h,\boldsymbol{z}\leftarrow D_{\boldsymbol{v},\sigma}^m$，以概率 $\min(D_\sigma^m(\boldsymbol{z})/(M\cdot D_{\boldsymbol{v},\sigma}^m(\boldsymbol{z})),1)$ 输出 $(\boldsymbol{z},\boldsymbol{c})$；(ii)$\boldsymbol{c}\leftarrow h,\boldsymbol{z}\leftarrow D_\sigma^m$，以概率 $1/M$ 输出 $(\boldsymbol{z},\boldsymbol{c})$。

3 形式化定义和安全模型

3.1 形式化定义

一个具有消息恢复功能的签名方案(Signature scheme with Message Recovery，SMR)由以下 3 个多项式时间内的算法构成：密钥生成(Key Generation)、签名(Sign)、验证(Verify)算法。

密钥生成：输入安全参数 n，输出用户的公、私钥对 (pk,sk)。

签名：输入私钥 sk 和签名消息 $\mu=\mu_1\|\mu_2\in\{0,1\}^*$，输出签名 θ 和部分消息 μ_2。如果待消息 μ 的长度比能签消息的长度短，则部分消息 $\mu_2=\perp$。

验证：输入签名 θ 和部分消息 μ_2，若签名有效，则输出 1 且恢复出完整消息 $\mu\in\{0,1\}^*$；否则输出 0。

一致性要求：sk 对消息 $\mu\in\{0,1\}^*$ 的有效签名 θ 和部分消息 μ_2，一定有：

$$Verify(Sign(sk,\mu),\mu_2,pk)=1$$

3.2 安全模型

定义 4(不可伪造性) 称一个具有消息恢复功能的签名方案在自适应性选择消息密文攻击存在不可伪造性(EUF-SMR-CMA)，若没有概率多项式时间内的敌手 $\mathcal{A}$ 在下面的 EUF-SMR-CMA 游戏中以不可忽略的优势取胜。这个 EUF-SMR-CMA 游戏是挑战者 $\mathcal{B}$ 和敌手 $\mathcal{A}$ 之间的游戏。

建立：挑战者 $\mathcal{B}$ 运行具有消息恢复功能的签名方案中的密钥生成算法产生一对公、私钥 (pk,sk)，然后 $\mathcal{B}$ 将 pk 发送给 $\mathcal{A}$，而自己保存 sk。

询问：敌手 $\mathcal{A}$ 以自适应性的方式选择消息 $(\mu_1),\cdots,(\mu_{q_s})\in\{0,1\}^*$ 向 $\mathcal{B}$ 关于 pk 进行至多 q_s 次签名询问，$\mathcal{B}$ 响应签名询问，并返回签名值 $\theta_i=Sign(sk,(\mu_i))$ 和部分消息 $(\mu_i)_2$。

伪造：$\mathcal{A}$ 输出一个签名 θ^* 和部分消息 $(\mu^*)_2$。若消息 μ^* 没有在签名询问阶段询问过，且 $Verify(Sign(sk,\mu^*),(\mu^*)_2,pk)=1$，则称 $\mathcal{A}$ 赢得游戏。$\mathcal{A}$ 的优势是其赢得上述游戏的概率。

4 具有消息恢复功能的格签名方案

首先定义参数[3,14]如下：素数 $q=poly(n)$，$m>64+n\log q/\log 3$，k，l_1，l_2，λ 都是正整数，常数 $M=O(1)$，任意 $\boldsymbol{v}\in\mathbb{Z}^m$，标准偏差 $\sigma=\omega(\|\boldsymbol{v}\|\sqrt{\log m})$；4 个哈希函数：$F_1:\{0,1\}^{l_2}\to\{0,1\}^{l_1}$，$F_2:\{0,1\}^{l_1}\to\{0,1\}^{l_2}$，$H_1:\mathbb{Z}_q^n\to\{0,1\}^{l_1+l_2}$，$H_2:\{0,1\}^*\to\{v:v\in\{-1,0,1\}^k,\|v\|_1\leqslant\lambda\}$。下面描述具有消息恢复功能的格签名方案。

· 密钥生成(Key generation):选取随机矩阵 $\boldsymbol{S} \xleftarrow{\$} \{-1,0,1\}^{m\times k}$ 和随机矩阵 $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$,计算 $\boldsymbol{T}=\boldsymbol{A}\cdot\boldsymbol{S} \bmod q$。私钥为 $\boldsymbol{S}$,公钥为 $(\boldsymbol{A},\boldsymbol{T})$。

· 签名(Sign):输入签名消息 $\mu\in\{0,1\}^*$ 和签名私钥 $\boldsymbol{S}$,签名算法执行如下:

1. 选取随机向量 $\boldsymbol{y} \xleftarrow{\$} D_\sigma^m$,并计算 $\alpha=H_1(\boldsymbol{A}\boldsymbol{y} \bmod q)$;

2. 划分消息 $\mu=\mu_1 \| \mu_2$,其中 $|\mu_1|=l_2$。如果 $|\mu|\leqslant l_2$,那么 $\mu_2=\perp$;

3. 置 $\mu'=F_1(\mu_1)\|(F_2(F_1(\mu_1))\oplus\mu_1)$ 和 $r=\alpha\oplus\mu'$;

4. 计算 $\boldsymbol{c}=H_2(r,\mu_2)$ 和 $\boldsymbol{z}=\boldsymbol{S}\cdot\boldsymbol{c}+\boldsymbol{y}$;

5. 以概率 $\min\{1,\frac{D_\sigma^m(\boldsymbol{z})}{M\cdot D_{\boldsymbol{S}\cdot\boldsymbol{c},\sigma}^m(\boldsymbol{z})}\}$ 输出签名值 $(r,\boldsymbol{z})$ 和部分消息 μ_2。

· 验证(Verify):给定部分消息 μ_2 和签名值 $(r,\boldsymbol{z})$,验证和恢复消息如下:

1. 计算 $\alpha=H_1(\boldsymbol{A}\cdot\boldsymbol{z}-\boldsymbol{T}\cdot H_2(r,\mu_2) \bmod q)$,置 $\mu_1'=\alpha\oplus r$;

2. 恢复部分消息 $\mu_1=\lfloor\mu'\rfloor_{l_2}\oplus F_2(\lfloor\mu'\rfloor_{l_1})$;

3. 如果 $F_1(\mu_1)=\lfloor\mu'\rfloor_{l_1}$ 和 $\|\boldsymbol{z}\|\leqslant 2\sigma\sqrt{m}$ 成立,则接受恢复完整消息 $\mu=\mu_1\|\mu_2$;否则拒绝。

5 方案分析

定理 2 新方案中签名算法输出的合法有效签名能通过验证,并能恢复完整消息。

证明:给定部分消息 μ_2,签名值 $(r,\boldsymbol{z})$ 和公钥 $(\boldsymbol{A},\boldsymbol{T})$。由于

$$\begin{aligned}&\boldsymbol{A}\cdot\boldsymbol{z}-\boldsymbol{T}\cdot H_2(r,\mu_2)\\&=\boldsymbol{A}\cdot(\boldsymbol{S}\cdot\boldsymbol{c}+\boldsymbol{y})-\boldsymbol{T}\cdot\boldsymbol{c}\\&=(\boldsymbol{A}\cdot\boldsymbol{S})\cdot\boldsymbol{c}+\boldsymbol{A}\cdot\boldsymbol{y}-\boldsymbol{T}\cdot\boldsymbol{c}=\boldsymbol{A}\cdot\boldsymbol{y} \bmod q\end{aligned}$$

则有 $\mu'=H_1(\boldsymbol{A}\cdot\boldsymbol{y} \bmod q)\oplus r=H_1(\boldsymbol{A}\cdot\boldsymbol{z}-\boldsymbol{T}\cdot H_2(r,\mu_2) \bmod q)\oplus r$。

又由于 $\mu'=F_1(\mu_1)\|(F_2(F_1(\mu_1))\oplus\mu_1)$,能从中恢复出部分消息 $\mu_1=\lfloor\mu'\rfloor_{l_2}\oplus F_2(\lfloor\mu'\rfloor_{l_1})$,且这部分消息 μ_1 满足 $F_1(\mu_1)=\lfloor\mu'\rfloor_{l_1}$。另一方面,由定理 1,签名 $\boldsymbol{z}$ 的分布近似服从 D_σ^m。再由引理 1,得 $\|\boldsymbol{z}\|\leqslant 2\sigma\sqrt{m}$ 以至少 $1-2^{-m}$ 的概率成立。因此,合法签名通过验证,且能够以概率恢复出完整消息 $\mu=\mu_1\|\mu_2$。

定理 3 若存在敌手 $\mathcal{A}$ 以 $(t,q_{H_1},q_{H_2},q_{F_1},q_{F_2},q_s,\varepsilon)$ 攻破具有消息恢复功能的格签名方案,即 $\mathcal{A}$ 在时间 t 内经过 q_{H_1} 次 H_1 询问,q_{H_2} 次 H_2 询问,q_{F_1} 次 F_1 询问,q_{F_2} 次 F_2 询问,q_s 次签名询问后,以不可忽略的优势 ε 赢得游戏,则存在一个挑战者 $\mathcal{C}$ 能在时间 $t'<t+(q_{H_1}+q_s)t_1+(q_{H_2}+q_s)t_2+(q_{F_1}+q_s)t_3+(q_{F_2}+q_s)t_4$ 内,以概率 $\varepsilon'\approx\varepsilon^2/2(q_{H_1}+q_{H_2}+q_{F_1}+q_{F_2}+q_s)$ 解决 SIS 问题,其中 t_1,t_2,t_3,t_4 分别表示进行一次 H_1 询问,H_2 询问,F_1 询问,F_2 询问所需要的应答时间。

证明:假定挑战者 $\mathcal{C}$ 收到一个 SIS 问题实例 $SIS_{(q,n,m,\beta)}=(\boldsymbol{A}\in\mathbb{Z}_q^{n\times m},q,n,m,\beta)$,其中 $\beta=(4\sigma+2\lambda)\sqrt{m}$,它希望输出一个小的向量 $\boldsymbol{x}\in\mathbb{Z}_q^m$ 满足 $\boldsymbol{A}\cdot\boldsymbol{x}=0 \bmod q$,$\|\boldsymbol{x}\|\leqslant\beta$。挑战者 $\mathcal{C}$ 将公开参数 $\boldsymbol{A}$,系统参数 (n,m,q,s) 和 4 个哈希函数 $F_1:\{0,1\}^{l_2}\to\{0,1\}^{l_1}$,$F_2:\{0,1\}^{l_1}\to\{0,1\}^{l_2}$,$H_1:\mathbb{Z}_q^n\to\{0,1\}^{l_1+l_2}$,$H_2:\{0,1\}^*\to\{v:v\in\{-1,0,1\}^k,\|v\|_1\leqslant\lambda\}$ 发送给 $\mathcal{A}$,其中哈希函数可作为随机预言机询问。不失一般性,假设所有的哈希函数值都由挑战者生成。

H_1 询问:挑战者 $\mathcal{C}$ 维护一个 H_1 询问列表 $L_1=\{(\boldsymbol{A}\boldsymbol{y}_i,\alpha_i)\}$,初始值为空。对 $\boldsymbol{A}\boldsymbol{y} \bmod q$ 的询问,$\mathcal{C}$ 首先查找列表 L_1,若在列表中存在匹配对 $(\boldsymbol{A}\boldsymbol{y} \bmod q,\alpha)$,则返回相应的哈希值 α;否则,选择随机串 $\alpha\in\{0,1\}^{l_1+l_2}$,将 $(\boldsymbol{A}\boldsymbol{y} \bmod q,\alpha)$ 存储在列表 L_1 中,并返回相应的哈希值 α。

F_1 和 F_2 询问:类似上述 H_1 询问过程,挑战者 $\mathcal{C}$ 分别维护一个 F_1 询问列表 L_2 和一个 F_2 询问列表 L_3,初始值均为空。当敌手询问 F_1 和 F_2 时,$\mathcal{C}$ 类似于上述 H_1 询问-应答过程返回结果。

H_2 询问:挑战者 $\mathcal{C}$ 维护一个 H_2 询问列表 $L_4=\{(r_i,(\mu)_i,c_i,z_i)\}$,初始值为空。对于询问 $(r,\mu=\mu_1\|\mu_2)$,$\mathcal{C}$ 首先查找列表 L_4,若存在匹配对 (r,μ,c,z),则返回相应的哈希值 c;否则,选择随机向量 $z\xleftarrow{\$}D_\sigma^m$ 和 $c\xleftarrow{\$}\{v:v\in\{-1,0,1\}^k,\|v\|_1\leqslant\lambda\}$,对 $(\boldsymbol{A}\cdot z-\boldsymbol{T}\cdot c) \bmod q$ 进行 H_1 询问得到 α,置 $\mu'=\alpha\oplus r$,根据 $\mu'=F_1(\mu_1)\|(F_2(F_1(\mu_1))\oplus\mu_1)$ 将 $(\mu_1,F_1(\mu_1))$ 和 $(F_1(\mu_1),F_2(F_1(\mu_1)))$ 分别添加进列表 L_2 和 L_3 里,然后操纵随机预言机 H_2 输出哈希值 $H_2(r,\mu_2)=c$,将 (r,μ,c,z) 存储在列表 L_4 中,最后返回相应的哈希值 c。

签名询问:敌手 $\mathcal{A}$ 询问对消息 $\mu\in\{0,1\}^*$ 的签名。$\mathcal{C}$ 虽然不知道签名私钥,但是能模拟出有效签名。首先 $\mathcal{C}$ 按消息 μ 索引查找列表 L_4。若在列表中存在匹配对 (r,μ,c,z),则返回相应的签名值 (r,z);否则,选择随机向量 $c\xleftarrow{\$}\{v:v\in\{-1,0,1\}^k,\|v\|_1\leqslant\lambda\}$ 和 $z\xleftarrow{\$}D_\sigma^m$,对 $(\boldsymbol{A}\cdot z-\boldsymbol{T}\cdot c) \bmod q$ 进行 H_1 询问得到 α,对 $\mu_1(\mu=\mu_1\|\mu_2)$ 依次进行 F_1 和 F_2 询问,得到 $(\mu_1,F_1(\mu_1))$ 和 $(F_1(\mu_1),F_2(F_1(\mu_1)))$,计算得到 $\mu'=F_1(\mu_1)\|(F_2(F_1(\mu_1))\oplus\mu_1)$,置 $r=\alpha\oplus\mu'$,然后操纵随机预言机 H_2 输出哈希函数值 $H_2(r,\mu_2)=c$,将 (r,μ,c,z) 存储在列表 L_4 中,最后返回相应的签名值 (r,z) 和部分消息 μ_2。

伪造:敌手结束上述询问,以不可忽略的概率 ε 输出消息 $\mu^*=\mu_1^*\|\mu_2^*$ 的有效消息-签名对 (μ_2^*,r^*,z^*)。

解决 SIS 问题实例:为求解 $\boldsymbol{A}\cdot\boldsymbol{x}=0 \bmod q$(注意敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 都不知道格 $\Lambda_q^\perp(\boldsymbol{A})$ 的短基),$\mathcal{A}$ 再次重复上述伪造过程中相同随机输入询问 H_1,$\mathcal{C}$ 返回新鲜的输出结果。根据 General Forking Lemma[16],敌手 $\mathcal{A}$ 以不可忽略的概率 ε 输出对相同消息 $\mu^*=\mu_1^*\|\mu_2^*$ 的一个新的有效消息-签名对 $(\mu_2^*,\tilde{r},\tilde{z})$,且满足 $H_2(\tilde{r},\mu_2^*)\neq H_2(r^*,\mu_2^*)$ 和 $\boldsymbol{A}\cdot\tilde{z}-\boldsymbol{T}\cdot H_2(\tilde{r},\mu_2^*)=\boldsymbol{A}\cdot z^*-\boldsymbol{T}\cdot H_2(r^*,\mu_2^*) \bmod q$。令 $\tilde{c}=H_2(\tilde{r},\mu_2^*)$ 和 $c^*=H_2(r^*,\mu_2^*)$,又 $\boldsymbol{T}=\boldsymbol{A}\cdot\boldsymbol{S}$,则有 $\boldsymbol{A}\cdot\tilde{z}-\boldsymbol{T}\cdot\tilde{c}-\boldsymbol{A}\cdot z^*+\boldsymbol{T}\cdot c^*=\boldsymbol{A}\cdot(\tilde{z}-z^*-\boldsymbol{S}\cdot\tilde{c}+\boldsymbol{S}\cdot c^*)=0 \bmod q$。由于 $\|z^*\|$,$\|\tilde{z}\|\leqslant 2\sigma\sqrt{m}$ 和 $\|\boldsymbol{S}\cdot c^*\|$,$\|\boldsymbol{S}\cdot\tilde{c}\|\leqslant\lambda\sqrt{m}$,则有 $\|\tilde{z}-z^*-\boldsymbol{S}\cdot\tilde{c}+\boldsymbol{S}\cdot c^*\|\leqslant(4\sigma+2\lambda)\sqrt{m}$。

由文献[14]定理 4.1 及引理 4.4 的结论,向量 $\tilde{z}-z^*-\boldsymbol{S}\cdot\tilde{c}+\boldsymbol{S}\cdot c^*\neq 0$ 的概率至少为 1/2,从而 $\mathcal{C}$ 成功解决 SIS 问题实例 $\boldsymbol{A}\cdot\boldsymbol{x}=0 \bmod q$(满足条件 $\|\boldsymbol{x}\|\leqslant(4\sigma+2\lambda)\sqrt{m}$)的概率为 $\varepsilon'\approx\varepsilon^2/2(q_{H_1}+q_{H_2}+q_{F_1}+q_{F_2}+q_s)$,同时运行时间 t' 不超过敌手伪造签名时间 t 与各次询问-应答的时间之和。

6 性能分析

现有格签名方案都没有消息恢复功能,所以在方案性能

比较分析(见表1)时，主要考虑以下指标：公钥长度、私钥长度、签名时是否需要高斯抽样运算、消息与签名的总长度、安全证明是否使用随机预言机模型。表1中长度单位均为比特，正整数 n 为安全参数，$m=O(n\log n)$，$q=O(n^2)$，$k=O(\log n)$，消息记为 μ，$|\mu|$ 表示消息的比特长。为方便比较，尽可能统一参数，以格中短基为私钥的格是满秩的，文献[14]格签名方案中 $d=1$。

从表1可以看出，文献[9-13]中格签名方案消息和签名总长度较长，且需要用到昂贵的高斯原像抽样运算，效率较低，其中仅文献[9,12,13]中方案在标准模型下可证明安全。由于新方案与文献[14,15]格签名方案中 $\mathbf{z}$ 的每个分量都不超过 12σ，所以其长度可以表示为 $m\log(12\sigma)$，同时它们都在随机预言机模型下可证明安全。进一步地，与文献[14,15]中的方案相比，我们的新方案缩短了消息和签名的总长度，具有优势。

表1 性能比较

方案	公钥长度	私钥长度	消息-签名总长度	是否抽样	预言机模型
文献[9]	$(\|\mu\|+1)nm\log q$	$m^2\log q$	$\|\mu\|+m(\|\mu\|/2+1)\log q$	是	标准模型
文献[10]	$nm\log q$	$m^2\log q$	$\|\mu\|+2m\log q$	是	随机预言机模型
文献[11]	$nm\log q$	$m^2\log q$	$\|\mu\|+n+m\log q$	是	随机预言机模型
文献[12]	$(2\|\mu\|+1)nm\log q$	$m^2\log q$	$\|\mu\|+m(\|\mu\|+1)\log q$	是	标准模型
文献[13]	$(nm+(\|\mu\|+2)n^2k+n)\log q$	$mnk\log q$	$\|\mu\|+(m+2nk)\log q$	是	标准模型
文献[14]	$2nm\log q$	$m^2\log 3$	$\|\mu\|+m\log 3+m\log(12\sigma)$	否	随机预言机模型
文献[15]	$nm\log(2q)$	$nm\log(2q)$	$\|\mu\|+n\log 2+m\log(12\sigma)$	否	随机预言机模型
新方案	$2nm\log q$	$m^2\log 3$	$\|\mu_2\|+\|\mu\|+m\log(12\sigma)$	否	随机预言机模型

结束语 本文在Lyubashevsky的无陷门签名方案的基础上，提出了一个高效的具有消息恢复功能的格签名方案，同时新方案可以看作是具有消息恢复功能Abe、Okamato的签名的格密码版本，能够抵抗未来量子计算机攻击。在随机预言机模型下，基于格上小整数解困难问题假设证明新方案是不可伪造的。新方案仅需要简单的矩阵与向量乘法运算，没有使用高斯原像抽样作为签名，提高了签名效率，同时缩短了传输消息-签名的总长度。另外，如何在标准模型下构造具有消息恢复功能的高效格签名方案是下一步值得研究的工作。

参考文献

[1] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing [J]. Journal of Cryptology, 2004, 17(4): 297-319

[2] Nyberg K, Rueppel R A. A new signature scheme based on the DSA giving message recovery [C] // CCS 1993. ACM, New York, 1993: 58-61

[3] Abe M, Okamoto T. A signature scheme with message recovery as secure as discrete logarithm [C] // ASIACRYPT 1999. LNCS 1716, Springer, Berlin, 1999: 378-389

[4] 陈辉焱，吕述望. 基于身份的具有部分消息恢复功能的签名方案[J]. 计算机学报，2006，29(9)：1622-1627

[5] ISO/IEC 9796-3: Information technology-Security techniques-Digital signature schemes giving message recovery-Part 3: Discrete logarithm based mechanisms(2nd Edition)[S]. JTC 1/SC 27. 2006

[6] ISO/IEC 9796-2: Information technology-Security techniques-Digital signature schemes giving message recovery-Part 2: Integer factorization based mechanisms(3nd Edition)[S]. JTC 1/SC 27. 2010

[7] Yang J H, Lin I C. A source authentication scheme based on message recovery digital signature for multicast[J]. International Journal of Communication Systems, 2013

[8] Ajtai M. Generating hard instances of lattice problems [C] // STOC 1996. ACM, New York, 1996: 99-108

[9] 王凤和，胡予濮，贾艳艳. 标准模型下的格基数字签名方案[J]. 西安电子科技大学学报，2012，39(4)：57-61

[10] 谢璇，喻建平，王廷，等. 基于格的变色龙签名方案[J]. 计算机科学，2013，40(2)：117-119

[11] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C] // STOC 2008. ACM, New York, 2008: 197-206

[12] Cash D, Hofheinz D, et al. Bonsai trees, or how to delegate a lattice basis[C] // EUEOCRYPT 2010. LNCS 6110, Springer, Berlin, 2010: 523-552

[13] Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller[C] // EUROCRYPT 2012. LNCS 7237, Springer, Berlin, 2012: 700-718

[14] Lyubashevsky V. Lattice signatures without trapdoors [C] // EUROCRYPT 2012. LNCS 7237, Springer, Berlin, 2012: 738-755

[15] Ducas L, Durmus A, Lepoint T, et al. Lattice signatures and bimodal Gaussians [C] // Crypto 2013. LNCS 8042, Springer, Berlin, 2013: 40-56

[16] Bellare M, Neven G. Multi-signatures in the plain public-key model and a general forking lemma[C] // CCS 2006. ACM, New York, 2006: 390-399

(上接第157页)

[12] Rafaeli S, Hutchison D. A survey of key management for secure group communication[J]. ACM Computing Surveys (CSUR), 2003, 35(3): 309-329

[13] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers[M] // Advances in Cryptology-CRYPTO 2001. Springer Berlin Heidelberg, 2001: 41-62

[14] Beimel A. Secure Schemes for Secret Sharing and Key Distribution[D]. Israel Institute of Technology, Technion, Haifa, Israel, 1996

[15] Goldreich O, Goldwasser S, Micali S. How to Construct Random Functions[J]. JACM, 1986, 33(4): 792-807

[16] Yang Kan, Jia Xiao-hua, Kui Ren. Attributed-based fine-grained access control with efficient revocation in cloud storage systems [C] // Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. ACM, New York, NY, USA, 2013: 523-528