ISSN 1673-9418 CODEN JKYTA8
Journal of Frontiers of Computer Science and Technology
1673-9418/2017/11(12)-1965-07
doi: 10.3778/j.issn.1673-9418.1611022

E-mail: fcst@vip.163.com
http://www.ceaj.org
Tel: +86-10-89056056

标准模型下格上基于身份的盲签名方案*

汤永利,周 锦,刘 琨,叶 青+,闫玺玺
河南理工大学 计算机科学与技术学院,河南 焦作 454000

Lattice-Based Identity-Based Blind Signature Scheme in Standard Model*

TANG Yongli, ZHOU Jin, LIU Kun, YE Qing+, YAN Xixi
College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan 454000, China
+ Corresponding author: E-mail: yeqing@hpu.edu.cn

TANG Yongli, ZHOU Jin, LIU Kun, et al. Lattice-based identity-based blind signature scheme in standard model. Journal of Frontiers of Computer Science and Technology, 2017, 11(12): 1965-1971.

Abstract: The blind signature scheme in the random oracle model relies on the random oracle assumption. The scheme is proven to be secure in theory, but it may not be secure in practice. This paper constructs an identity-based blind signature scheme with lattice in the standard model. A short basis delegation algorithm is introduced to generate the private key. The signature of the message is generated by the forward sampling algorithm proposed by Gentry et al. Under the standard hardness assumption of the small integer solutions problem (SIS), the new scheme is proven to be one-more unforgeable based on Juels and Pointcheval's security model in the standard model. The comparison results show that the key length and signature length are shorter, and the efficiency is higher.
Key words: lattice; identity-based; standard model; blind signature

摘 要: 随机预言模型下的盲签名方案都依赖于随机预言假设,即使方案被证明安全,在实际应用时未必安全。构造了一个标准模型下格上基于身份的盲签名方案。该方案中引入一个短格基派生算法,根据用户的身份产生对应的私钥,并利用Gentry等人提出的原像抽样陷门单向函数产生消息的签名。在标准模型下依据

* The "13th Five-Year" National Crypto Development Foundation of China under Grant No. MMJJ20170122 (国家密码管理局"十三五"国家密码发展基金); the Project of Science and Technology Department of Henan Province under Grant No. 142300410147 (河南省科技厅项目); the Project of Education Department of Henan Province under Grant Nos. 12A520021, 16A520013 (河南省教育厅项目); the Doctoral Fund of Henan Polytechnic University under Grant No. B2014-044 (河南理工大学博士基金).
Received 2016-11, Accepted 2017-03.
CNKI网络优先出版: 2017-03-22, http://kns.cnki.net/kcms/detail/11.5602.TP.20170322.1754.002.html

Juels和Pointcheval等人提出的安全模型，基于小整数解问题（small integer solutions，SIS）的困难性，证明了该方案满足one-more不可伪造性。分析表明，与同类方案相比，该方案密钥长度和签名长度有所减小，效率更高。

关键词：格；基于身份；标准模型；盲签名

文献标志码：A **中图分类号：**TP309

1 引言

盲签名的概念首先由Chaum[1]在1982年提出，消息拥有者在不公布消息真实内容的情况下，即可获得消息签名者对真实消息的合法签名。由于盲签名具有保护用户隐私的性质，在电子现金、电子选举、不经意传输等领域得到了广泛的应用。1985年Shamir[2]提出了基于身份密码学的概念，降低了密码算法的计算开销和实现成本，而且去除了PKI体制中的公钥证书管理负担。结合盲签名和基于身份密码学，Zhang和Kim在2003年利用双线性对提出了基于身份的盲签名方案[3]。目前，很多研究者仍继续对基于身份的盲签名方案进行研究，但是大多方案的安全性是基于数论难题（如大整数分解和离散对数问题）的，然而在量子计算机得到应用的前提下，基于数论假设的困难问题都可以在多项式时间内得到解决[4]。因此，设计能抵抗量子攻击的签名方案成为该领域需解决的问题。

1996年，Ajtai在STOC上发表的文献[5]中论证了基于格的公钥密码体制是量子计算机不能攻破的少数经典公钥密码体制之一。格[6]是$\mathbb{R}^m$中一类具有周期性结构离散点的集合。严格地说，格是m维欧式空间$\mathbb{R}^m$的n（$m>n$）个线性无关向量组$v_1,v_2,\cdots,v_n$的所有整系数线性组合，即$L(B)=\left\{\sum_{i=1}^{n}a_iv_i|a_i\in\mathbb{Z},i=1,2,\cdots,n\right\}$，向量组$v_1,v_2,\cdots,v_n$称为格的一组基。基于格的公钥密码体制还有其他优良特性，如平均情况与最差情况一样安全以及简单高效等，因而近几年引起了国内外密码学家的密切关注。2008年Gentry和Peikert等人[7]基于小整数解问题（small integer solutions，SIS）提出了一个带原像抽样的陷门单向函数，并指出该原像抽样陷门单向函数可用于构造基于格的签名方案和格上基于身份的加密方案。2010年Rückert在文献[8]中，利用原像抽样陷门单向函数设计了第一个基于格的盲签名方案（lattice-based blind signature scheme，LBSS）。同年Rückert在文献[9]中提出了第一个格上基于身份的签名方案（lattice-based identity-based signature scheme，LIBSS）。此后其他的LIBSS也被提出[10-11]，它们的构造大部分是基于Gentry和Peikert等人[7]提出的框架，在生成签名密钥的时候都要用到格基派生技术。基于此框架构造的基于身份的签名方案，在使用格基派生技术产生签名密钥的时候，通常情况下会导致格基的维度膨胀，进而使签名密钥和消息签名的尺寸变大，影响签名方案的效率。Gu等人[12]在2012年提出了一个在随机预言模型下格上基于身份的盲签名方案，该方案是在随机预言模型下可证明安全的，方案中假设存在一个理想的抗碰撞的哈希函数，即使方案被证明安全，在实际应用中未必安全。目前还没有一个在标准模型下可证明安全的基于身份的盲签名方案。

Agrawal和Boneh等人[13]在2010年美密会上提出了一个新的短格基派生算法，该算法并不会增加格的维度，即能使生成密钥的长度保持不变，从而提高密码方案效率。

本文将Agrawal提出的新的短格基派生算法引入基于身份的盲签名方案[12,14]中，构造了一个标准模型下格上基于身份的盲签名方案。方案中，使用新的短格基派生算法根据用户的身份信息生成用户的私钥，从而达到缩短用户私钥和签名长度的目的，并利用Gentry等人提出的原像抽样陷门单向函数产生消息的签名。根据文献[15-16]提出的盲签名的安全模型，基于格上SIS困难问题证明方案满足one-more不可伪造性，本文方案与现有其他基于格的盲签名方案[17-18]相比，生成的用户私钥和签名长度要小，效率更高。

2 预备知识

2.1 格上困难问题

定义1 对于整数 q 与矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$，定义两个整数格：

$$\Lambda(\boldsymbol{A},q)=\{y\in Z^n|y=\boldsymbol{A}x \bmod q, x\in Z^m\}$$

$$\Lambda^{\perp}(\boldsymbol{A},q)=\{x\in Z^m|\boldsymbol{A}x=0 \bmod q\}$$

定义2（小整数解问题）给定整数 q，矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$，实数 β，找到一个非零向量 $\boldsymbol{x}\in Z^m$，使得 $\boldsymbol{A}\boldsymbol{x}=0 \bmod q$，并且 $\|\boldsymbol{x}\|\leqslant\beta$。

定义3（非齐次小整数解问题）给定整数 q，矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$，实数 β，找到一个非零向量 $\boldsymbol{x}\in Z^m$，使得 $\boldsymbol{A}\boldsymbol{x}=y \bmod q$，并且 $\|\boldsymbol{x}\|\leqslant\beta$。

定义4[19]（光滑参数 smoothing parameter）设任意一个 n 维格 Λ 和一个实数 $\varepsilon>0$，光滑参数 $\eta_{\varepsilon}(\Lambda)$ 为使得 $\rho_{1/s}(\Lambda^*\backslash\{0\})\leqslant\varepsilon$ 成立的最小的 $s(s>0)$。

定理1[7] 对于任意秩为 k 的 n 维格 Λ，$c\in R^n$，正数 $\varepsilon<\exp(-4\pi)$ 和 $s\geqslant\eta_{\varepsilon}(\Lambda)$，对于每一个 $\boldsymbol{x}\in\Lambda$ 有：

$$D_{\Lambda,s,c}(\boldsymbol{x})\leqslant\frac{1+\varepsilon}{1-\varepsilon}2^{-k}$$

定理2[19] 设一个任意的秩为 k 的 n 维格 Λ，任意 $c\in R^n$，$\varepsilon\in(0,1)$，$s\geqslant\eta_{\varepsilon}(\Lambda)$，则有：

$$\Pr_{x\leftarrow D_{\Lambda,s,c}}\left[\|\boldsymbol{x}-c\|>s\sqrt{n}\right]\leqslant\frac{1+\varepsilon}{1-\varepsilon}2^{-k}$$

2.2 原像抽样算法和格基派生算法

定理3[7] 对于任意格的基 $\boldsymbol{B}\in Z^{n\times k}$，高斯参数 $s\geqslant\|\boldsymbol{B}\|\omega(\sqrt{\mathrm{lb}\,n})$ 和 $c\in R^n$，算法 $SampleD(\boldsymbol{B},s,c)$ 的输出分布与 $D_{Z^k,s,c}(\boldsymbol{x})$ 在统计上是不可区分的。

定理3中算法 $SampleD(\boldsymbol{B},s,c)$ 采样输出的向量 $\boldsymbol{e}$ 满足 $\boldsymbol{Be}$ 的分布在 Z_q^n 上是均匀的。

定理4[7] 对于矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 和 $\Lambda_q^{\perp}(A)$ 上的一个短陷门基 $T_{\boldsymbol{A}}$，向量 $\boldsymbol{y}\in Z_q^n$，高斯参数 $s\geqslant\|\tilde{T}_{\boldsymbol{A}}\|\omega(\mathrm{lb}\,m)$，算法 $SamplePre(\boldsymbol{A},T_{\boldsymbol{A}},\boldsymbol{y},s)$ 输出向量 $\boldsymbol{e}\in Z_q^m$ 与 $D_{\Lambda_q^{\perp}(\boldsymbol{A}),s}(\boldsymbol{x})$ 在统计距离上是不可区分的。

定理5[7] 给定任意素数 $q=poly(n)$ 和任意 $m\geqslant 5n\lg q$，存在一个概率多项式算法 $TrapGen(1^n)$，输入为 1^n，输出矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 和一个满秩的集合 $S\subset\Lambda^{\perp}(\boldsymbol{A},q)$，$\boldsymbol{A}$ 在 $Z_q^{n\times m}$ 上是均匀分布的，并且 $\|S\|\leqslant L=m^{1+\varepsilon}$，$\varepsilon>0$。

定理6[13] 输入一个矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 和 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一个短基 $T_{\boldsymbol{A}}$，在 $\boldsymbol{D}_{m\times m}$ 中选取的可逆矩阵 $\boldsymbol{R}\in Z^{m\times m}$，高斯参数 $s\geqslant\|\tilde{T}_{\boldsymbol{A}}\|m^d\omega(\lg^{d+1}(m))$，算法 $BasisDel(\boldsymbol{A},\boldsymbol{R},T_{\boldsymbol{A}},s)$ 随机输出格 $\Lambda^{\perp}(\boldsymbol{A}\boldsymbol{R}^{-1})$ 的一个基 $\boldsymbol{B}$，并且 $\|\tilde{\boldsymbol{B}}\|\leqslant s\sqrt{m}$。

3 标准模型下格上基于身份的盲签名方案

下面介绍本文提出的标准模型下格上基于身份的盲签名方案。方案中各个参数的取值范围和参数符号介绍如下：n 为安全参数且 n 是大于0的整数，q 为素数且 $q\geqslant 2$，$m\geqslant 5n\lg q$，本方案中用到一个哈希函数 H: $\{0,1\}^*\rightarrow Z_q^{m\times m}$ 是一个抗碰撞的哈希函数。

方案具体描述如下。

$Setup(1^n)$：私有密钥生成器PKG（private key generator）以安全参数 n 为输入，运行陷门生成算法 $TrapGen(1^n)$，根据定理5可知生成矩阵 $\boldsymbol{A}_0\in Z_q^{n\times m}$ 和对应的短基 $S_0\subset\Lambda^{\perp}(\boldsymbol{A}_0,q)$，$S_0\in Z_q^{m\times m}$ 为系统主密钥，$\boldsymbol{A}_0$ 为系统公钥。假设消息 M 是由任意 d 比特长的比特串 $\{0,1\}^d$ 组成，那么随机选择 d 个不相关的向量 $\boldsymbol{C}_1,\boldsymbol{C}_2,\cdots,\boldsymbol{C}_d\in Z_q^n$。公布系统的公共参数 $PP=\langle\boldsymbol{A}_0,\boldsymbol{C}_1,\boldsymbol{C}_2,\cdots,\boldsymbol{C}_d\rangle$，主密钥 $MK=S_0$。

$Extract(PP,id,MK)$：系统根据收到的签名者的身份信息 id，通过自己的主秘密密钥 S_0 和公共参数 PP，使用定理6提出的格基派生算法 $BasisDel(\boldsymbol{A}_0,H(id),S_0,s)$ 输出签名者的私钥 S_{id}，其中 S_{id} 为格 $\Lambda^{\perp}(\boldsymbol{A}_0H(id)^{-1})$ 的一个基，s 为高斯采样参数。

$Sign(PP,SK_{id},\boldsymbol{\mu})$：假设要签名的消息为 M，则签名者 S 和消息拥有者 C 做如下操作。

（1）消息盲化：消息拥有者 C 随机均匀选取 $t\in D=\{t\in R|\|t\|\geqslant 1/s\}$，使用定理3中的算法 $SampleD(\boldsymbol{A}_0H(id)^{-1},s)$ 输出一个向量 $\boldsymbol{u}$，计算 $\mu=t\sum_{i=1}^{d}(-1)^{M[i]}C_i+\boldsymbol{A}_0H(id)^{-1}\boldsymbol{u}$，$\mu$ 为盲化后的消息，把 μ 发给签名者 S。

（2）对盲化消息签名：签名者 S 在接收到消息拥有者 C 发来的盲化消息 μ 之后，使用定理4中的原像采样陷门算法对 μ 进行签名。$SamplePre(\boldsymbol{A}_0H(id)^{-1},S_{id},\mu,s)$ 输出盲化消息的签名 $e'\in Z_q^m$，签名者 S 验证 $\|e'\|\leqslant s\sqrt{m}$ 且 $e'\neq 0$，如果不满足则重新选取，事实上

根据定理2以极大概率成立，并在本地存储 (μ,e')，然后将签名发送给消息拥有者 C。

(3)消息去盲：消息拥有者 C 收到签名之后，做去盲操作 $e=t^{-1}(e'-u)$，e 即为消息 M 的签名。

Verify(PP,id,M,e)：任意验证者都能验证 (M,e) 的正确性，通过下面的计算。

(1)验证 $e\neq 0$ 且 $\|e\|\leqslant 2s^2\sqrt{m}$，如果满足进行(2)验证，不满足则拒绝。

(2)验证 $\boldsymbol{A}_0H(id)^{-1}e=\sum_{i=1}^{d}(-1)^{M[i]}C_i$，如果满足则接受，不满足则拒绝。

4 安全性分析

本文基于Juels等人[15]和Pointcheval等人[16]提出的安全模型，证明本文方案满足正确性、盲性和one-more不可伪造性。盲性是指签名者对消息进行签名时不能获得任何有关签名消息的信息。one-more不可伪造性是指攻击者与签名者交互，获得 l 个不同消息的诚实签名，无法伪造第 $l+1$ 个新消息的签名。

4.1 正确性

定理7 本文提出的签名方案满足正确性。

证明 (1)因为消息签名 $e=t^{-1}(e'-u)$，所以 $\|e\|=\|t^{-1}(e'-u)\|$，由定理4可知 $\|e'\|\leqslant s\sqrt{m}$，由定理3可知 $\|u\|\leqslant s\sqrt{m}$，由用户盲化操作可知 $\frac{1}{\|t\|}\leqslant s$，因此 $\|e\|\leqslant\frac{1}{\|t\|}(\|e'\|+\|u\|)\leqslant 2s^2\sqrt{m}$。

(2)因为 $\boldsymbol{A}_0H(id)^{-1}(t^{-1}(e'-u))=t^{-1}(\boldsymbol{A}_0H(id)^{-1}e'-\boldsymbol{A}_0H(id)^{-1}u)$，在签名算法中 $e'\leftarrow SamplePre(\boldsymbol{A}_0H(id)^{-1},S_{id},\boldsymbol{\mu},s)$，所以 $\boldsymbol{A}_0H(id)^{-1}e'=\boldsymbol{\mu}$，$\boldsymbol{\mu}$ 为盲化的消息，从而 $\boldsymbol{A}_0H(id)^{-1}e=t^{-1}(\boldsymbol{\mu}-\boldsymbol{A}_0H(id)^{-1}u)$。又因为 $\boldsymbol{\mu}=t\sum_{i=1}^{d}(-1)^{M[i]}C_i+\boldsymbol{A}_0H(id)^{-1}u$，所以 $\boldsymbol{A}_0H(id)^{-1}e=\sum_{i=1}^{d}(-1)^{M[i]}C_i$。故所提出的签名方案是正确的。 □

4.2 盲性

定理8 本文提出的签名方案满足消息的盲性。

证明 签名者 S 不能从盲化后的消息 μ 中得到有关消息 M 的任何信息，也就是要证明消息 M 的概率分布和盲化消息 μ 的概率分布的统计距离为0，即：

$$\Delta\left(\sum_{i=1}^{d}(-1)^{M[i]}\boldsymbol{C}_i,\boldsymbol{\mu}\right)=\frac{1}{2}\sum_{c\in Z_q^n}\left|pro\left(\sum_{i=1}^{d}(-1)^{M[i]}C_i=c\right)-pro(\mu=c)\right|=0$$

因为 $\boldsymbol{C}_1,\boldsymbol{C}_2,\cdots,\boldsymbol{C}_d\in Z_q^n$ 是在 Z_q^n 中均匀选取的，所以 $pro\left(\sum_{i=1}^{d}(-1)^{M[i]}\boldsymbol{C}_i=c\right)$ 是 $(1/2)^n$。因为 $\boldsymbol{\mu}=t\sum_{i=1}^{d}(-1)^{M[i]}\boldsymbol{C}_i+\boldsymbol{A}_0H(id)^{-1}u$ 并且 $u\sim D_{Z^m,s}$，所以 $pro(\mu=c)$ 也近似等于 $(1/2)^n$，$\Delta\left(\sum_{i=1}^{d}(-1)^{M[i]}\boldsymbol{C}_i,\boldsymbol{\mu}\right)$ 近似接近于0。从而不可区分，故盲性满足。 □

4.3 不可伪造性

Juels和Pointcheval等人在文献[15]和文献[16]中定义了盲签名的安全模型，其中要求盲签名满足one-more不可伪造性，即如果对于任意伪造者 A 在掌握签名公钥条件下，与诚实签名者进行 l 次签名交互，得到 l 个不同消息的签名，伪造第 $l+1$ 个新消息的签名的概率是可以忽略的，则签名方案满足one-more不可伪造性。

定理9 如果平均情况下的 $SIS_{q,m,s}$ 是困难的，则本文提出的签名方案在选择消息攻击下满足one-more不可伪造性。

证明 如果敌手 F 能够攻破本文方案，即成功伪造出合法签名，且其优势(攻击成功的概率)为 ε，则可构造多项式时间算法 T 求解SIS问题。其中敌手在攻击时至少要进行 $q_\varepsilon(q_\varepsilon>1)$ 次私钥询问，q_s 次签名询问。

构造算法 T 模拟 F 的攻击环境并利用 F 的伪造签名求解SIS问题的一个实例。

Setup：算法 T 随机产生一个矩阵 $\boldsymbol{B}\in Z_q^{n\times m}$ 和对应的陷门 $T_0\subset\Lambda^{\perp}(\boldsymbol{B})$，选择 $\boldsymbol{R}_1\sim\boldsymbol{D}_{m\times m}$，然后运行 *BasisDel* $(\boldsymbol{B},\boldsymbol{R}_1,T_0,s)$ 输出 S_0，其中 S_0 是 $\Lambda^{\perp}(\boldsymbol{B}\boldsymbol{R}_1^{-1})$ 的基，设 $\boldsymbol{A}_0=\boldsymbol{B}\boldsymbol{R}_1^{-1}$ 为主公钥，S_0 为主秘密密钥。使用算法 *SampleD* $(\boldsymbol{B},s)$ 随机选取 d 个非零向量 $\boldsymbol{E}_1,\boldsymbol{E}_2,\cdots,\boldsymbol{E}_d\in Z_q^m$，并且使得 $\boldsymbol{B}\boldsymbol{E}_i$ 在 Z_q^n 上是均匀分布的。选择 $q_\varepsilon-1$ 个不相关的非奇异矩阵 $\boldsymbol{R}_2,\boldsymbol{R}_3,\cdots,\boldsymbol{R}_{q_\varepsilon}\sim\boldsymbol{D}_{m\times m}$。令 $C_i=\boldsymbol{B}\boldsymbol{E}_i$，公

开公共参数 $PP=\langle \boldsymbol{A}_0,\boldsymbol{C}_1,\boldsymbol{C}_2,\cdots,\boldsymbol{C}_d\rangle$，系统主秘密密钥 $MK=S_0$。

私钥询问：当身份 ID_i 被询问时产生相对应的私钥，其中 $i=1,2,\cdots,q_\varepsilon$。算法 T 收到 ID_i 计算 $H(ID_i)=\boldsymbol{R}_i^{-1}$，使用 $BasisDel(\boldsymbol{A}_0,H(ID_i),S_0,s)$ 算法生成对应的私钥 S_i，并在本地存储 (ID_i,S_i)，然后把 S_i 发送给敌手 F，假设敌手询问的 ID_i 是以前询问过的，那么算法 T 首先会在本地查找 (ID_i,S_i)，并把对应的 S_i 发送给敌手。

签名询问：当算法 T 收到 (ID_i,μ_M)，其中 ID_i 为签名者的身份信息，μ_M 为盲化后的消息，使用原像陷门采样函数对盲化消息 μ_M 签名，$e_M'\leftarrow SamplePre(\boldsymbol{A}_0H(id)^{-1},S_i,\mu_M,s)$，$e_M'$ 即为消息 μ_M 的签名。之后算法 T 检查 $\|e_M'\|\leqslant s\sqrt{m}$，如果不满足则重新签名，把 (ID_i,μ_M,e_M') 存储在本地，并且把 e_M' 发送给敌手 F。如果接收到的消息是以前询问过的，那么算法 T 首先在本地的数据库查找 (ID_i,μ_M,e_M')。如果找到，则直接把对应的 e_M' 返回给敌手 F。敌手 F 在收到签名后进行去盲操作，最后得到消息的签名 (ID_i,M,e_M)。

伪造：最终经过有限次的私钥提取询问和签名询问，敌手 F 伪造了可用签名 (ID_i,M,e_M)，伪造成功的概率为 ε。

可以知道：(1) $e_M\neq 0$ 并且 $\|e_M\|\leqslant 2s^2\sqrt{m}$；(2) $\boldsymbol{A}_0H(ID_i)^{-1}e_M=\sum_{i=1}^{d}(-1)^{M[i]}C_i$。如果 $i\neq 1$，则签名验证失败。当 $i=1$ 时，有 $\boldsymbol{A}_0H(ID_1)^{-1}=\boldsymbol{B}\boldsymbol{R}_1^{-1}\boldsymbol{R}_1=\boldsymbol{B}$，因为 $\boldsymbol{A}_0H(ID_i)^{-1}e_M=\sum_{i=1}^{d}(-1)^{M[i]}\boldsymbol{C}_i$ 并且 $\boldsymbol{C}_i=\boldsymbol{B}E_i$，所以 $\boldsymbol{B}e_M=\boldsymbol{B}\sum_{i=1}^{d}(-1)^{M[i]}E_i$。令 $E_M=\sum_{i=1}^{d}(-1)^{M[i]}E_i$ 并且 $\|E_M\|\leqslant s^2\sqrt{m}$，则上式等于 $\boldsymbol{B}e_M=\boldsymbol{B}E_M$，因此 $\boldsymbol{B}(e_M-E_M)=0 \bmod q$，$\|e_M-E_M\|\leqslant e_M\|+\|E_M\|\leqslant 2s^2\sqrt{m}+\|s^2\sqrt{m}=3s^2\sqrt{m}$。这样知道 e_M-E_M 为 SIS 问题实例的一个解，SIS 问题的参数为 $(q,m,3s^2\sqrt{m},\boldsymbol{B})$，因为这个解不能是0解，所以 $e_M\neq E_M$。那么 $e_M=E_M$ 的概率大约为 $2^{-\omega(\lg m)}$，敌手 F 成功伪造签名的概率为 ε，$pro(i=1)=1/q_\varepsilon$。因此 e_M-E_M 为 $SIS_{q,m,3s^2\sqrt{m},\boldsymbol{B}}$ 问题的解的概率近似接近于 $\left(1-2^{-\omega(\lg m)}\right)\frac{1}{q_\varepsilon}\varepsilon$。 □

5 效率对比

签名方案的效率主要取决于签名私钥的长度、公钥的长度和签名的长度。本文中，n 为安全参数，m 是格的维度，d 为被签名消息的比特长度，q 为素数且 $q\geqslant 2$。

本文方案主要使用了简单的线性运算(模乘、模加)，与所有数论上的基于身份的盲签名方案相比，计算效率显然更高。从表1中可知，文献[17]是格上的代理盲签名方案，其生成私钥的算法增加了格的维度，所有私钥和签名都变长了。本文使用新的派生算法，保证维度不变，因此效率有所提升。文献[18]是格上基于身份的代理盲签名，该方案为了满足强不可伪造性，使用代理密钥和用户私钥分别对消息进行处理和签名，其中用代理密钥签名生成的消息签名变大。而本文方案只进行一次签名和一次验证，故生成的签名长度不变，计算效率也有所提高。文献[12]是在随机预言模型下证明安全的基于身份的盲签名方案，随机预言模型下可证明安全并不代表真实世界的安全，因为它依赖于现实世界无法实现的随机预言假设。从表1中可以看出，本文方案在公钥和私钥长度上比文献[17]要短，签名长度比文献[17]和文献[18]都短，签名效率更高，和文献[12]相比，虽然公钥长度长，但是在标准模型下证明安全。

Table 1 Efficiency comparison

表1 效率对比

方案	公钥长度	私钥长度	签名长度	安全模型
文献[17]	$3nm\,\mathrm{lb}\,q$	$2m(m-n)\mathrm{lb}\,q$	$3m\,\mathrm{lb}\,q$	随机预言模型
文献[18]	$(mn+dm)\mathrm{lb}\,q$	$mm\,\mathrm{lb}\,q$	$2m\,\mathrm{lb}\,q$	标准模型
文献[12]	$nm\,\mathrm{lb}\,q$	$mm\,\mathrm{lb}\,q$	$m\,\mathrm{lb}\,q$	随机预言模型
本文方案	$(mn+dm)\mathrm{lb}\,q$	$mm\,\mathrm{lb}\,q$	$m\,\mathrm{lb}\,q$	标准模型

6 结论

本文提出了一个标准模型下格上基于身份的盲签名方案，并且分析了方案的安全性和效率，利用Agrawal等人[13]提出的新的短格基派生算法在不增加格的维度的情况下生成用户的私钥，从而达到缩短用户私钥和签名长度的目的，使用原像抽样陷门单向函数对消息进行签名，故方案密钥长度和签名长

度更短,计算效率更高。本文方案的安全性主要基于格上的困难问题,因此能抵抗量子攻击。

References:

[1] Chaum D. Blind signatures for untraceable payments[M]// Advances in Cryptology. Boston: Springer US, 1983: 199-203.

[2] Shamir A. Identity-based cryptosystems and signature schemes [C]//LNCS 196: Proceedings of CRYPTO 1984, Santa Barbara, USA, Aug 19-22, 1984. Berlin, Heidelberg: Springer, 1985: 47-53.

[3] Zhang Fangguo, Kim K. Efficient ID-based blind bignature and proxy signature from bilinear pairings[C]//LNCS 2727: Proceedings of the 8th Australasian Conference on Information Security and Privacy, Wollongong, Australia, Jul 9-11, 2003. Berlin, Heidelberg: Springer, 2003: 312-323.

[4] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[5] Ajtai M. Generating hard instances of lattice problems[C]// Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadelphia, USA, May 22-24, 1996. New York: ACM, 1996: 99-108.

[6] Wang Xiaoyun, Liu Mingjie. Survey of lattice-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 13-27.

[7] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for lattices and new cryptographic constructions[C]//Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, Canada, May 17-20, 2008. New York: ACM, 2008: 197-206.

[8] Rückert M. Lattice-based blind signatures[C]//LNCS 6477: Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, Dec 5-9, 2010. Berlin, Heidelberg: Springer, 2010: 413-430.

[9] Rückert M. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles [C]//LNCS 6061: Proceedings of the 3rd International Conference on Post-Quantum Cryptography, Darmstadt, Germany, May 25-28, 2010. Berlin, Heidelberg: Springer, 2010: 182-200.

[10] Tian Miaomiao, Huang Liusheng. Identity-based signatures from lattices: simpler, faster, shorter[J]. Fundamental Information, 2014, 145(2): 171-187.

[11] Liu Zhenhua, Zhang Xiangsong, Hu Yupu. Revocable and strongly unforgeable identity-based signature scheme in the standard model[J]. Security and Communication Networks, 2016, 9(14): 2422-2433.

[12] Gu Chunxiang, Chen Li, Zheng Yonghui. ID-based signatures from lattices in the random oracle model[C]//LNCS 7529: Proceedings of the 2012 International Conference on Web Information Systems and Mining, Chengdu, China, Oct 26-28, 2012. Berlin, Heidelberg: Springer, 2012: 222-230.

[13] Agrawal S, Boneh D, Boyen X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE[C]// LNCS 6223: Proceedings of the 30th Annual Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, Aug 15-19, 2010. Berlin, Heidelberg: Springer, 2010: 98-115.

[14] Wang Fenghe, Hu Yupu, Wang Chunxiao. Lattice-based blind signature schemes[J]. Geomatices and Information Science of Wuhan University, 2010, 35(5): 550-553.

[15] Juels A, Luby M, Ostrovsky R. Security of blind digital signatures (extended abstract)[C]//LNCS 1294: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, Aug 17-21, 1997. Berlin, Heidelberg: Springer, 1997: 150-164.

[16] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[17] Zhang Lili, Song Yongxuan. Proxy blind signature scheme from lattice basis delegation[J]. International Journal of Advancements in Computing Technology, 2012, 4(21): 99-104.

[18] Zhang Lili, Ma Yanqin. A lattice-based identity-based proxy blind signature scheme in the standard model[J]. Mathematical Problems in Engineering, 2014: 307637.

[19] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures[J]. SIAM Journal on Computing, 2007, 37(1): 267-302.

附中文参考文献:

[6] 王小云, 刘明洁. 格密码学研究[J]. 密码学报, 2014, 1(1): 13-27.

[14] 王凤和, 胡予濮, 王春晓. 基于格的盲签名方案[J]. 武汉大学学报: 信息科学版, 2010, 35(5): 550-553.

TANG Yongli was born in 1972. He received the Ph.D. degree in cryptology from Beijing University of Posts and Telecommunications in 2008. Now he is a professor at Henan Polytechnic University. His research interests include information security and cryptology, etc.

汤永利(1972—),男,河南孟州人,2008年于北京邮电大学获得博士学位,现为河南理工大学教授,主要研究领域为信息安全,密码学等。

ZHOU Jin was born in 1991. He is an M.S. candidate at Henan Polytechnic University. His research interest is cryptology.

周锦(1991—),男,河南郑州人,河南理工大学硕士研究生,主要研究领域为密码学。

LIU Kun was born in 1978. She is an associate professor and M.S. supervisor at Henan Polytechnic University. Her research interests include information security and cryptology, etc.

刘琨(1978—),女,河南焦作人,硕士,河南理工大学副教授、硕士生导师,主要研究领域为信息安全,密码学等。

YE Qing was born in 1981. She received the Ph.D. degree in cryptology from Beijing University of Posts and Telecommunications in 2014. Now she is a lecturer at Henan Polytechnic University. Her research interest is cryptology.

叶青(1981—),女,辽宁营口人,2014年于北京邮电大学获得博士学位,现为河南理工大学讲师,主要研究领域为密码学。

YAN Xixi was born in 1985. She received the Ph.D. degree in cryptology from Beijing University of Posts and Telecommunications in 2012. Now she is a lecturer at Henan Polytechnic University. Her research interest is cryptology.

闫玺玺(1985—),女,河南灵宝人,2012年于北京邮电大学获得博士学位,现为河南理工大学讲师,主要研究领域为密码学。