文章编号:1671-8860(2010)05-0550-04　　文献标志码:A

基于格的盲签名方案

王凤和[1,2]　胡予濮[1]　王春晓[3]

(1　西安电子科技大学计算机网络与信息安全教育部重点实验室,西安市太白南路 2 号,710071)
(2　泰山学院数学与系统科学学院,泰安市迎宾大道中段 15 号,271021)
(3　山东建筑大学理学院,济南市凤鸣路 2 号,250101)

摘　要:利用原像抽样函数,在整数格上设计了一个 2 轮盲签名方案,实现了消息对签名者的无条件盲性,在随机预言机模型下,基于格上最小整数解(SIS)问题的困难性假设,证明盲签名方案满足 one-more 不可伪造性。与 Markus Rückert 设计的格上基于原像抽样函数的 3 轮盲签名比较,新方案签名轮数更少,签名长度更短,因此效率更高,而且新方案有效地解决了 Markus Rückert 方案中存在的签名失败问题。

关键词:盲签名;原像抽样函数;格
中图法分类号:TP309

盲签名的概念首先由 Chaum 提出[1],由于盲签名具有保护用户隐私的性质,使得盲签名在电子现金、电子选举、不经意传输等领域存在广泛的应用。自盲签名概念提出以来,许多基于数论假设(如大整数分解和离散对数问题)和身份的盲签名方案[2-4]等也被提出。然而在量子计算机得到应用的前提下,著名的两个数论假设大整数分解问题和离散对数问题都可以在多项式时间内得到解决[5],所以大量基于数论假设的盲签名方案在量子环境下将不再安全。因此,设计在后量子时代依然安全的盲签名方案成为盲签名领域急需解决的问题。近年来,格上密码系统成为了公钥领域的研究热点,并取得了一系列的研究成果[6-11],其中一个很有意义的研究领域是能否在格上设计具有特殊功能的密码系统。本文基于格上原像抽样函数[8]设计了一个 2 轮的盲签名方案。与文献[10]的 3 轮方案比较,本文的盲签名交互轮数少、签名长度短,效率更高。

1　基础知识

1.1　格

定义 1　设 $v_1,v_2,\cdots,v_n$ 是 R^n 上一组线性无关的向量,则格 $\boldsymbol{A}=\{\sum a_iv_i \mid a_i\in Z,i=1,\cdots,n\}$,向量组 $v_1,v_2,\cdots,v_n$ 构成格上的一组基。两类整数格近年来被广泛应用于密码设计中:

$$\Lambda(\boldsymbol{A})=\{\boldsymbol{y}\in Z^n \mid \boldsymbol{Ax}=\boldsymbol{y},\boldsymbol{x}\in Z^m,\boldsymbol{A}\in Z^{n\times m}\}$$

$$\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in Z^m \mid \boldsymbol{Ax}=0,\boldsymbol{A}\in Z^{n\times m}\}$$

定义 2　设 $\boldsymbol{\omega}$ 是一个向量,$\boldsymbol{\omega}$ 的 l_p-范数定义为 $\|\boldsymbol{\omega}\|_p=(\sum|\omega_i{}^p)^{1/p}$,当 $p=2$ 时,叫作欧几里德范数。

1.2　格上的几个困难问题

1) SVP 和 CVP 问题。设 $\boldsymbol{B}$ 是格的一组基,SVP 问题就是在格上寻找一个非零向量 $\boldsymbol{u}$,满足对任意格上的向量 $\boldsymbol{v}$,有 $\|\boldsymbol{u}\|\leqslant\|\boldsymbol{v}\|$ 成立。设 $\boldsymbol{\omega}$ 是任意一个向量,而 CVP 问题是要在格上寻找向量 $\boldsymbol{u}$,使任意格上的向量 $\boldsymbol{v}$ 有 $\|\boldsymbol{u}-\boldsymbol{\omega}\|\leqslant\|\boldsymbol{v}-\boldsymbol{\omega}\|$。

2) SIS 问题(小整数解问题)。设参数 $q(\cdot)$、$m(\cdot)$、$\beta(\cdot)$,给定 n 和 $\boldsymbol{A}\in Z_q^{n\times m}$,寻找一个非零向量 $\boldsymbol{e}$,$\boldsymbol{Ae}=0\bmod(q(n))$,$\|\boldsymbol{e}\|\leqslant\beta(n)$。

1.3　格上的高斯分布

近年来,离散高斯分布和光滑参数成为整数格的重要分析工具。对任意 $s>0$,定义以向量 c 为中心、参数为 s 的高斯分布:$\forall x\in R^n$,$\rho_{s,c}(x)=e^{-\pi\|x-c\|/s^2}$,格 Λ 上的高斯分布为 $\forall x\in\Lambda$,$D_{\Lambda,s,c}=\rho_{s,c}(x)/\rho_{s,c}(\Lambda)$。

定义 3　(光滑参数)设任意一个 n 维格 Λ,

收稿日期:2010-03-15。
项目来源:国家自然科学基金资助项目(60673072,60803149,60970119)。

任意 $\varepsilon>0$,定义光滑参数 $\eta_\varepsilon(\Lambda)$ 为最小的正数,$s>0$,满足 $\rho_{1/s}(\Lambda\backslash\{0\})\leqslant\varepsilon$。

定理 1[11]　设一个 n 维格 Λ,任意 $c\in R^n$,$\varepsilon\in(0,1)$,$s\geqslant\eta_\varepsilon(\Lambda)$,则 $\underset{x\sim D_{\Lambda,s,c}}{Pr}[\|x-c\|>s\sqrt{n}]\leqslant\frac{1+\varepsilon}{1-\varepsilon}2^{-n}$。

定理 2[6]　存在一个概率多项式时间算法满足:给定一个 n 维格 Λ 的基 $\boldsymbol{B}$,参数 $s\geqslant\|\widetilde{\boldsymbol{B}}\|\omega(\sqrt{\lg n})$,一个中心 $c\in R^n$,输出的抽样统计接近 $D_{\Lambda,s,c}$ 分布。

定理 3[7]　设 $\boldsymbol{A}\in Z_q^{n\times m}$,令 $m\geqslant 2n$,对任意向量 $\boldsymbol{u}\in Z_q^n$,存在 $\boldsymbol{e}\in\{0,1\}^m$,有 $\boldsymbol{Ae}=\boldsymbol{u}(\mathrm{mod}\ q)$。

定理 4[6]　设矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 的行生成 Z_q^n,参数 $\varepsilon\in(0,1/2)$,$s\geqslant\eta_\varepsilon(\Lambda^\perp(\boldsymbol{A}))$,则当向量服从 $\boldsymbol{e}\sim D_{Z^m,s}$ 时,$\boldsymbol{u}=\boldsymbol{Ae}(\mathrm{mod}q)$ 以统计距离 2ε 接近 Z_q^n 上的均匀分布。

2　格基盲签名

文献[10]中合法签名范数的范围较大,同样,用户在盲化变换时所选择的向量也有较大的范数,这些直接造成了最后用户去盲后范数可能会溢出,造成签名失败。鉴于以上问题,对原像抽样函数的参数进行调整,要求签名者在一个较小参数 s' 下完成抽样,同时要求用户用一个更小范数但是满足定理 4 的向量盲化消息,而最后的签名验证则在一个较大的参数 s 下进行。采用 s 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,从而有效地避免了签名失败的发生,同时,盲签名的轮数缩小为 2 轮。

2.1　参数选择

整个方案中,n 为安全参数,其他参数都是 n 的函数。设签名者掌握一个 n 维格 Λ 的一组小范数的基(好基)$\boldsymbol{B}$,设格 Λ 的校验矩阵为 $\boldsymbol{A}\in Z_q^{n\times m}$,$\widetilde{\boldsymbol{B}}$ 为基 $\boldsymbol{B}$ 的施密特正交基。又设 $h(\cdot):\{0,1\}^*\rightarrow Z_q{}^n$ 是一个安全的防碰撞的 Hash 函数。定义格 Λ 上两个离散高斯分布的参数 $s=a\|\widetilde{\boldsymbol{B}}\|\omega(\sqrt{\lg n})$,$a\geqslant 1$,$s'=a[(\|\widetilde{\boldsymbol{B}}\|-x)/x]\omega(\sqrt{\lg n})$,$x<\|\widetilde{\boldsymbol{B}}\|/2$,$a\omega(\sqrt{\lg n})\geqslant\eta_\varepsilon(\Lambda)$ 成立,其中,函数 $\omega(\cdot)$ 的定义为:若 $g(n)=\omega(f(n))$,则 $g(n)$ 增长的速度比任何 $cf(n)(c>1)$ 都快。显然,参数 s、s' 均大于格 Λ 的光滑参数 $\eta_\varepsilon(\Lambda)$,所以以参数 s、s' 进行高斯取样时,定理 4 成立。设 L_M 为签名者所签署盲化消息的数据库,综上可知,公开 $\boldsymbol{A}$、n、m、q、s、s'、a、x,好基 $\boldsymbol{B}$ 为签名者的签名密钥。

2.2　消息盲化

设原始消息为 M,用户计算 $\boldsymbol{H}=h(M)$,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 $\boldsymbol{c}=(c_1,c_2,\cdots,c_m)$,则 $\|\boldsymbol{c}\|\leqslant a\omega(\sqrt{\lg n})\sqrt{m}$ 以极大概率成立(定理 1)。若不满足,只需重新抽取。且此次抽样满足定理 4,因此,$\boldsymbol{Ac}$ 近似服从均匀分布。任意选择 $t\in Z$,$1<t<x<\|\widetilde{\boldsymbol{B}}\|-1$,计算 $\boldsymbol{\mu}=(t^{-1}\boldsymbol{H}+\boldsymbol{Ac})\mathrm{mod}q$,将 μ 送给签名者。

2.3　签　名

签名者首先在自己的数据库 L_M 中寻找 $\boldsymbol{\mu}$,若找到 $\boldsymbol{\mu}$,则终止签名;若 $\boldsymbol{\mu}$ 不在 L_M 中,则签名者通过自己掌握的格 Λ 上的好基 $\boldsymbol{B}$,利用原像抽样函数产生盲化消息的签名。签名者首先任意选择向量 $\boldsymbol{t}_1\in Z_q^m$,满足 $\boldsymbol{At}_1=\boldsymbol{\mu}$(定理 3),以 $-\boldsymbol{t}_1$ 为中心,在参数 s' 下利用抽样算法抽取向量 $\boldsymbol{v}\sim D_{\Lambda,s',-t_1}$,计算 $\boldsymbol{e}'=\boldsymbol{v}+\boldsymbol{t}_1$,检查 $\|\boldsymbol{e}'\|\leqslant s'\sqrt{m}$,若不然,重新抽取向量 $\boldsymbol{v}$。事实上,由定理 1 知,$\|\boldsymbol{e}'\|\leqslant s'\sqrt{m}$ 以极大概率成立,则消息 $\boldsymbol{e}'$ 作为签名者的签名,同时签名者在 L_M 中存储 $\boldsymbol{\mu}$。

2.4　去　盲

用户得到盲化消息的签名 $\boldsymbol{e}'$ 后,进行去盲变换:计算 $\boldsymbol{e}=\boldsymbol{t}(\boldsymbol{e}'-\boldsymbol{c})$,$\boldsymbol{e}$ 作为 M 的签名。

2.5　验　证

验证者得到消息 M 的签名 $(M,\boldsymbol{e})$ 后,计算 $\boldsymbol{H}=h(M)$,如果 $\boldsymbol{Ae}=\boldsymbol{H}(\mathrm{mod}q)$,且 $\|\boldsymbol{e}\|\leqslant s\sqrt{m}$ 成立,则接受签名,否则拒绝。

3　安全性分析

3.1　盲　性

定义 4(盲性)　设 (μ_0,e_0')、(μ_1,e_1') 是签名阶段用户得到的两个盲化消息及其盲签名,给定 μ_b,e_b',$b\in(0,1)$,签名方案满足盲性,如果任意多项式时间的签名者或区分者输出一个 b',使得 $b=b'$ 发生的概率至多为 $1/2+1/n^c$,其中 n 足够大,c 为常数,即 (μ_0,e_0')、(μ_1,e_1') 对签名者和区分者不可区分。

定理 5　本文的盲签名满足盲性要求。

证明　由定理 4,签名者收到的盲化消息 $\boldsymbol{\mu}=(t^{-1}\boldsymbol{H}+\boldsymbol{Ac})\mathrm{mod}q$ 中的 $\boldsymbol{Ac}$ 服从 Z_q^n 上的均匀分布,$\boldsymbol{H}$ 作为一个安全 Hash 函数的输出也近似服从均匀分布,而 t 是随机选取的随机数。对签名者而言,消息 $\boldsymbol{\mu}$ 服从的分布与 Z_q^n 上的均匀分布是不可

区分的。设签名者希望通过随机选择 Z_q^m 上的向量和随机选择小于 x 的自然数来恢复真实消息 $\boldsymbol{H}$，证明签名者这样选择所得到的结果分布与均匀分布的统计距离为0，即

$$\Delta(t(\boldsymbol{\mu}-\boldsymbol{c}),\boldsymbol{H})=\sum_{H\in Z_q^n,\boldsymbol{c}\in Z_q^m,t\in Z,t<x}|\,p[\boldsymbol{t}_1(\boldsymbol{\mu}-\boldsymbol{c}_1)=\boldsymbol{H}(m)]-P[\boldsymbol{H}=\boldsymbol{H}(m)]\,|=\sum_{\boldsymbol{H}\in Z_q^n,\boldsymbol{c}\in Z_q^m,t\in Z,t<x}[(\frac{1}{q})^m-(\frac{1}{q})^m]=0$$

从而不可区分，盲性满足。

3.2 one-more 不可伪造性

定义5(one-more 不可伪造) 如果对于任意多项式时间的伪造者 A 在掌握签名公钥条件下，与签名者经过多项式有界的一次签名交互，得到一个诚实签名者的 l 个不同消息的签名，伪造第 $l+1$ 个新消息的合法签名的概率是可以忽略的，则签名满足 one-more 不可伪造性。

文献[8]提出的基于原像抽样函数的签名方案在随机预言机模型下已经证明安全性等价于SIS问题，而本文方案的 one-more 不可伪造性是基于文献[8]签名方案的存在性不可伪造。假设盲签名存在攻击者 A 能够以不可忽略的概率伪造签名，则构造模拟者成功伪造文献[8]的签名，进而解决格上的SIS问题来实现。所以假设模拟者接入一个格上的原像抽样预言机，这一点与文献[10]第一个盲签名证明时接入一个陷门求逆预言机一致。

定理6 假设格 Λ 上参数 m、q、$2s\sqrt{m}$ 下的SIS问题是困难的，则盲签名满足 one-more 不可伪造性。

证明 假设敌手 A 掌握一个概率多项式时间算法 φ，以签名人的公钥和相应系统参数以及 l 个消息与其对应签名为输入，可以以不可忽略的概率 ε 输出第 $l+1$ 个消息的伪造签名，则可以构造算法 S 利用敌手 A 以近似概率 ε 来解签名格 Λ 上参数为 q、m、$2s\sqrt{m}$ 的SIS问题。假设算法 S 控制一个 Hash 随机预言机 H，同时接入一个格上的原像预言机，同时，算法 S 维护两张表 L_1、L_2 分别用来记录 Hash 询问和盲签名询问。设算法 S 要解决的SIS问题实例是 (q,s,m,A)，算法 S 的目的是找一个范数小于 $2s\sqrt{m}$ 的向量 $\boldsymbol{v}$，满足 $A\boldsymbol{v}=0(\mathrm{mod}\ q)$。发送 A、s、m、q 给敌手，开始游戏。

Hash 询问：收到敌手发来的第 i 个消息 M_i 后($i=1,2,\cdots,l+1$)，S 随机产生向量 $\boldsymbol{h}_i$，满足 $\|\boldsymbol{h}_i\|\leqslant s\sqrt{m}$，将 $A\boldsymbol{h}_i \mathrm{mod} q$ 发给敌手 A，同时在表格 L_1 中存储 $(M,\boldsymbol{h}_i,A\boldsymbol{h}_i)$。利用定理4，此时，$Ah_i \mathrm{mod} q$ 近似服从均匀分布，因此可以完美地模拟 Hash 函数的输出(若 M 的消息记录在表格 L_1 中，则返回 L_1 中相应的 $A\boldsymbol{h}_i$)。

签名询问：S 收到敌手的第 i 个消息 μ_i 的签名询问后，首先在表格 L_2 中寻找条目 (μ_i,e_i')，若存在，则返回 e_i' 作为签名的应答；否则，S 把 μ_i 重发给原像抽样预言机，获得消息的盲签名 e_i'，存储 (μ_i,e_i') 到表格 L_2，返回 e_i' 作为签名。敌手 A 收到签名后，可以进行去盲变换，得到真实的签名 e_i。

敌手 A 满意后，使用概率多项式时间算法 φ，以概率 ε 输出第 $l+1$ 个消息的伪造签名 $(M_{l+1},\boldsymbol{e}_{l+1})$，$S$ 作同样的输出。S 从 L_1 中获得消息 M_{l+1} 的 Hash 询问记录，得到向量 $\boldsymbol{h}_{l+1}$，检查是否有 $\boldsymbol{h}_{l+1}=\boldsymbol{e}_{l+1}$，若等式成立，则 S 终止游戏，宣布失败；若等式不成立，则 S 得到两个范数小于 $s\sqrt{m}$ 的向量，满足 $A\boldsymbol{e}_{l+1}l=A\boldsymbol{h}_{l+1}l$，所以模拟者得到 $A(\boldsymbol{h}_{l+1}-\boldsymbol{e}_{l+1})=0 \mathrm{mod} q$，而且 $\|\boldsymbol{h}_{l+1}l-\boldsymbol{e}_{l+1}l\|<\|\boldsymbol{h}_{l+1}l\|+\|\boldsymbol{e}_{l+1}l\|\leqslant 2s\sqrt{m}$，从而 S 可以解参数为 q、m、$2s\sqrt{m}$ 的SIS问题。

模拟者只有当 $\boldsymbol{h}_{l+1}\neq\boldsymbol{e}_{l+1}$ 时才能得到SIS问题的解，而消息可能的签名个数有 $\omega(\lg n)$，所以模拟者成功的概率为 $\varepsilon(1-1/2^{\omega(\lg n)})$，从而模拟者解SIS问题的优势近似为 ε。

3.3 效率分析

盲签名方案仅仅利用到了小整数模加、模乘运算和文献[8]的高效抽样方法，所以盲签名实现了较高的计算效率。将本文方案的效率与文献[10]中的第一个方案进行比较，结果见表1。

表1 盲签名效率比较

Tab.1 Comparison of Efficiency of Blind Signature

	文献[10]方案一	本文方案
交互轮数	3	2
签名长度	$(n+m)\lg q$	$m\lg q$
公钥长度	$nm\lg q$	$nm\lg q$
密钥长度	$nm\lg q$	$nm\lg q$
签名失败	有	无

表1说明本文方案在交互的轮数、签名长度上要优于文献[10]。此外，文献[10]采用承诺方案来保证签名失败发生时消息对签名者的盲性，而本文方案可以有效防止签名失败，从而允许用一个安全的 Hash 函数来代替承诺方案，进一步精简了用户的操作。

参 考 文 献

[1] Chaum D. Blind Signatures for Untraceable Pay-

ments[C]. Crypto 1982, California,1983

[2] Camenisch J,Koprowski M, Warinschi B. Effcient Blind Signatures Without Random Oracles[C]. Security in Communication Networks, Amalfi, Italy, 2004

[3] Okamoto T. Efficient Blind and Partially Blind Signatures Without Random Oracles[C]. Theory of Cryptography Conference (TCC) 2006, LNCS 3876, New York,2006

[4] Bresson E, Monnerat J, Vergnaud D. Separation Results on the One-More Computational Problems [C]. RSA Conference (CT-RSA) 2008, San Francisco, CA,2008

[5] Shor P W. Polynomial-time Algorithm for Prime Factorizeation and Discrete Logarithm on a Quantum Computer[J]. SIAM Journal on Computing, 1997, 26(5):1 484-1 509

[6] Lyubashevsky V, Micciancio D. Asymptotically Efficient Lattice-Based Digital Signature [C]. TCC2008, LNCS 4948, New York,2008

[7] Regev O. On Lattice, Learning with Errors, Random Linear Codes, and Cryptography [C]. STOC'05, Baltimore,2005

[8] Gentry C, Peikert C, Vaikuntanathan V . Trapdoors for Hard Lattices and New Cryptographic Constructions[C]. STOC2008, Victoria, British Columbia,2008

[9] Alwen J, Peikert C. Generating Shorter Bases for Hard Random Lattices [C]. STACS, Freiburg, 2009

[10] Rückert M. Lattice-based Blind Signatures[OL]. http://eprint.iacr.org.2008/322,2008

[11] Micciancio D,Regev O. Worst-case to Average-case Reductions Based on Gaussian Measures[J]. SIAM J Comput, 2007 37(1): 267-302

第一作者简介:王凤和,博士生,主要研究方向为格公钥、数字签名。

E-mail:fenghe2166@163.com

Lattice-based Blind Signature Schemes

WANG Fenghe[1,2]　*HU Yupu*[1]　*WANG Chunxiao*[3]

(1 Key Laboratory of Computer Networks & Information Security, Ministry of Education, Xidian University, 2 South Taibai Road, Xi'an 710071,China)

(2 Department of Mathematics, Taishan Collage, 15 Middle Yingbin Road, Taian 271021, China)

(3 School of Mathematic and Phys, Shandong Jianzhu University, 2 Fengming Road, Jinan 250101, China)

Abstract: Using preimage sampleable functions, we propose a new lattice-based two moves blind signature scheme. The proposed scheme is not only unconditionally blind but also one-more unforgeable due to the hardness of the shortest integral solution on lattice, which is proved in the random oracle model. Compared with a well known lattice-based three moves blind signature scheme introduced by Markus Rückert, it shows that the proposed scheme can avoid the failure to sign, Moreover, the proposed scheme has less moves(two moves) and shorter length of signature. Hence it can be concluded that the proposed scheme is more efficient than the known lattice-based blind signature scheme.

Key words: blind signature ; preimage samplable functions;lattice

About the first author: WANG Fenghe, Ph.D candidate,majors in lattice public key cryptography.

E-mail: fenghe2166@163.com