文章编号:1004-3918(2017)03-0369-05

基于格的分级盲签名

邓银娟

(宝鸡文理学院 数学与信息科学学院,陕西 宝鸡 721013)

摘 要:在现有的基于身份的盲签名基础上,依据格基扩展算法的特性,提出了格上基于身份的分级盲签名方案,增加了上级签名者对下级签名者权限的有效管理. 并验证了正确性、安全性和分级性,效率分析后,得出公钥、私钥和签名长度并无明显增加.

关键词:格; 盲签名; 安全性

中图分类号:TP 309.7 **文献标识码**:A

A Hierarchical Blind Signature Scheme on Lattice

DENG Yinjuan

(Mathematics and Computer Information Institute, Baoji University of Arts and Sciences, Baoji 721013, Shaanxi China)

Abstract: Based on identity-base blind signature, we propose a hierarchical blind signature through lattice expansion algorithm, which increases permissions management of the subordinate signer to superior signer, and it is the correctness, security and scalability. By efficiency analysis, the lengths of public key, private key and the signature are not significantly increased.

Key words: lattice; blind signatures; security

盲签名除了具有一般数字签名的性质外,还需具有以下特殊性:1)签名者对其所签署的文件的内容是不可见的,即签名者不知道他所签署消息的具体内容. 2)签名消息是不可追踪的,即当签名消息被公布后,签名者无法知道这是他哪次签署的. 量子计算机的出现给传统密码体制的安全性带来了威胁,基于格的密码体制作为可以抵御量子计算机攻击的候选密码体制之一受到越来越多人的关注. 2008年Markus Ruckert[1]最先提出了基于格的盲签名方案,文章中的盲签名方案所基于的困难问题是SIS(小整数解问题)[2-3],由于方案中的合法签名范数的范围比较大,同样,用户在盲化变换时所选择的向量也有较大的范数,这就导致了申请者在去盲变换后得到的范数会超出范围,而使得签名失败. 2010年王凤和[4]等人在Markus提出的基于格的盲签名的基础上,对签名过程和盲化过程中的参数适当缩小,但同样使方案保证满足SIS困难问题,最终把盲签名的交互轮数由3轮降为2轮,有效地避免了签名失败的发生. 2012年夏维[5]在王凤和等[6]提出的格上基于盆景树模型的环签名的基础上,提出了一种新型的格上基于盆景树模型的盲签名方案.

1 基础知识

1.1 格

一个 n 维格是 R^n 的一个满秩的离散子群,主要研究整数格,即那些点的坐标在 Z^n 中的格. 格的定义为 $\Lambda=\left\{\sum_{i=1}^{n}\mu_i\boldsymbol{v}_i\middle|\mu_i\in Z\right\}$,其中 $\boldsymbol{v}_1,\boldsymbol{v}_2,...,\boldsymbol{v}_n$ 是格 Λ 的一组基. 常用的还有 q 元格,定义如下:

对于任意的整数 $q\geqslant 2$,以及任意的 $\boldsymbol{A}\in Z_q^{m\times n}$,定义为

收稿日期:2016-10-06

基金项目:国家自然基金项目(61402015);宝鸡文理学院硕士科研启动项目(ZK14061)

作者简介:邓银娟(1987-),女,讲师,硕士,研究领域为密码与网络安全.

$$\Lambda_q^{\perp}(A)=\left\{e\in Z^n: A\cdot e=0 \bmod q\right\}. \tag{1}$$

$\Lambda_q^{u}(A)=\left\{e\in Z^n: A\cdot e=u \bmod q\right\}$. 格 $\Lambda_q^{u}(A)$ 是 $\Lambda_q^{\perp}(A)$ 的一个陪集，对于任意的 t 使得 $\Lambda_q^{u}(A)=\Lambda_q^{\perp}(A)+t$，或者 $A\cdot t=u \bmod q$.

一个格基的Gram-Schmidt正交化模：用 S 表示向量，$S=\{s_1,s_2,\cdots,s_k\}$ 在 R^m 中的集合. 用以下的标准记号：$\|S\|$ 表示 S 中最长的向量，即 $\|S\|=\max_{1\leqslant i\leqslant k}\|s_i\|$，$\tilde{S}=\left\{\tilde{s}_1,\tilde{s}_2,\cdots,\tilde{s}_k\right\}\in R^m$，表示向量 $s_1,s_2,\cdots,s_k$ 的Gram-Schmidt正交化.

1.2 高斯分布

对任意的 $\sigma>0$，在 R^n 上以 c 为中心的具有偏差参数 σ 的高斯函数定义为：

$\forall x\in R^n, \rho_{\sigma,c}(x)=\exp(-\pi\|x-c\|^2/\sigma^2)$ 对任意的 $c\in R^n,\sigma>0$ 和 n 维格 Λ，在格 Λ 上的离散高斯分布定义为

$$\forall x\in\Lambda,\ D_{\Lambda_{\sigma,c}}(x)=\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\Lambda)}, \tag{2}$$

其中 $\rho_{\sigma,c}(\Lambda)=\sum_{x\in\Lambda}\rho_{\sigma,c}(x)$.

对一个由矩阵 $A\in Z_q^{n\times m}$ 张成的空间的确定向量 $y\in Z_q^n$，以 $\Lambda^{\perp}(A)$ 的陪集为：

$\Lambda^{\perp}(A)=\left\{e\in Z^m: Ae=y \bmod q\right\}=t+\Lambda^{\perp}(A) \bmod q$，其中 t 为等式 $At=y \bmod q$ 的一个任意解. 所以格 $\Lambda_y^{\perp}(A)$ 上的高斯分布 $D_{Z^m,\sigma}$ 关于 $At=y \bmod q$ 的条件分布，如下所示：

$$\forall x\in\Lambda,\ D_{\Lambda_{\sigma}^{\perp}(A),\sigma}(x)=\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(t+\Lambda^{\perp}(A))}. \tag{3}$$

1.3 SIS困难问题

设参数为整数 $q(\cdot)$，$m(n)$ 和 $\beta(\cdot)$，给定正整数 n 和一个矩阵 $A\in Z_{q(n)}^{m\times n}$，寻找一个非零的整数向量 $e\in Z_q^n$ 使得 $Ae=0 \bmod q$ 并且满足 $\|e\|\leqslant\beta(n)$.

Gentry 等人使用在离散高斯分布中随机选取格点的方法，证明了一般情况下在较小的模数 q 上 SIS 问题的困难性与特定因子下的近似 SIVP 和 GapSVP 问题的困难性相同[7].

1.4 格上的几个重要算法

引理1 Samplepre 概率多项式算法

存在一个概率多项式时间算法 Samplepre，给定 n 维格 Λ 一个基 T，一个参数 $\sigma\geqslant\|\tilde{T}\|\cdot\omega(\sqrt{\log n})$，以及一个向量 $t\in R^n$，则可以输出一个抽样，使得该抽样统计接近于 $D_{\Lambda+t,\sigma}$.

引理2 ExtBasis 格基扩展算法

在文献[8]中提出了一组格基扩展算法：ExtBasis，具体构造如下：

ExtBasis $(S_0, A=A_0\|A_1)$：输入 $A_0\in Z_q^{n\times m_0}$ 和任意 $A_1\in Z_q^{n\times m_1}$，$S_0\in Z^{m_0\times m_0}$ 是格 $\Lambda^{\perp}(A_0)$ 的一组基，该算法输出格 $\Lambda^{\perp}(A)$ 的一组基 $S\in Z_q^{(m_0+m_1)\times(m_0+m_1)}$，且 $\|\tilde{S}\|=\|\tilde{S}_0\|$；注意到该输出基 $S\in Z_q^{(m_0+m_1)\times(m_0+m_1)}$ 也一定是格 $\Lambda^{\perp}(A_1\|A_0)$ 的一组基，因此该算法有的时候也可以写为 ExtBasis $(S_0, A=A_1\|A_0)$.

1.5 盲签名简介

一个盲签名方案由三部分组成（密钥生成、签名、验证），这里的签名部分是一个签名者和用户之间的交互协议. 具体细节如下[9]：

- 密钥生成（Key Generation）：密钥生成算法 $\mathrm{Kg}(1^n)$ 输出一个私钥 sk 和一个公共验证密钥 pk.
- 签名协议（Signature Protocol）：Sign(sk,M) 由签名者和用户共同执行. 首先由用户对消息 M 的哈希进行盲化，将盲化的结果传送给签名者，签名者对其进行签名，将签名结果传给用户，用户对签名结果进行去盲变换得到消息的签名 s.
- 签名验证（Signature Verification）：用户执行验证算法 Vf(pk,s,M)，如果 s 是消息 M 的有效签名则输出 1，

否则输出0.

2 基于格的分级盲签名

对参数 L,r 做如下定义：

$L\geqslant O(n\log q)$：用户的密钥基上界；

$\tilde{L}\geqslant O\left(\sqrt{n\log q}\right)$：用户密钥基 Gram－Schmidt 正交化后基的上界；

$r\geqslant\tilde{L}\cdot\omega\left(\sqrt{\log n}\right)$：格的高斯平滑参数.

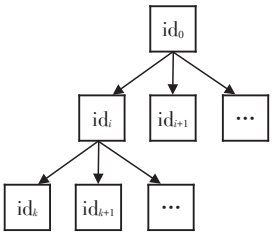

图1 身份关系图

Fig.1 Identity relationship diagram

2.1 方案构造[10-12]

设 n,m 为正整数，q 为素数，且满足 $m\geqslant 5n\log q$，

$H_1:\{0,1\}^*\rightarrow Z_q^n$ 为一个哈希函数.

$H_2:\{0,1\}^*\rightarrow Z_q^n$ 为一个哈希函数.

密钥生成 KeyGen(1^n)：输入一个安全参数 n，调用 TrapGen(q,n) 生成一个随机均匀的矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$，以及 $\boldsymbol{\Lambda}_q^{\perp}(\boldsymbol{A})$ 的一个短基 $\boldsymbol{T}_A$，公钥为 PK＝$\boldsymbol{A}$，私钥为 SK＝$\boldsymbol{T}_A$.

根节点签名者的秘钥生成，id_0 为签名者的身份标识符，计算签名者公钥 $\boldsymbol{A}_0\leftarrow\boldsymbol{A}\|H_2(\mathrm{id}_0)\in Z_q^{n\times(m+1)}$，根据格基扩展函数计算 $\boldsymbol{A}_0$ 的一组基 $\boldsymbol{T}_0=\mathrm{ExtBasis}(\boldsymbol{T},\boldsymbol{A}_0)$.

非跟节点签名者的秘钥生成，id_i 为签名者的身份标识符，其父节点的身份标识符为 id_k，计算签名者公钥 $\boldsymbol{A}_i\leftarrow\boldsymbol{A}_k\|H_2(\mathrm{id}_i)\in Z_q^{n\times(m+j)}$（$j$ 为节点的层级），根据格基扩展函数计算 $\boldsymbol{A}_i$ 的一组基 $T_i=\mathrm{ExtBasis}(T_k,\boldsymbol{A}_i)$.

盲化过程：

盲化过程由签名验证中心完成，设 H 为原始消息 M 的哈希值 $H=H_1(M)$，以零为中心，按离散正态分布 $D_{Z^{m+i},a\omega(\sqrt{\lg n})}$ 随机选择向量 $\boldsymbol{c}=(c_1,c_2,\cdots,c_{m+i})$，则 $\|\boldsymbol{c}\|\leqslant a\omega(\sqrt{\lg n})\sqrt{m+i}$（其中 $a\geqslant 1$）以极大概率成立. 若不满足，只需重新抽取，且此次抽样满足关于原像抽样的要求，$\boldsymbol{A}_i\boldsymbol{c}$ 近似服从均匀分布. 任意选择 $t\in Z$，$1<t<\boldsymbol{x}<\|\tilde{\boldsymbol{T}}\|-1$，计算 $\mu=(t^{-1}H+\boldsymbol{A}_i\boldsymbol{c})\bmod q$，将 μ 传送给签名者.

签名过程：

签名者任意选择向量 $\boldsymbol{t}_1\in Z_q^m$，满足 $\boldsymbol{A}_i\boldsymbol{t}_1=\mu$，以 $-\boldsymbol{t}_1$ 为中心，在参数 $\sigma=a\left[(\|\boldsymbol{A}_i\|-\boldsymbol{x})/\boldsymbol{x}\right]\omega\sqrt{\lg n},\boldsymbol{x}<\|\tilde{\boldsymbol{A}}\|/2$ 下抽取向量 $\boldsymbol{v}\leftarrow\mathrm{Sample\,Pr}\,\boldsymbol{e}(\boldsymbol{A}_i,r,\sigma,\mu)$ 计算 $\boldsymbol{e}'=\boldsymbol{v}+\boldsymbol{t}_1$，检查 $\|\boldsymbol{e}'\|\leqslant\sigma\sqrt{2m}$，否则，重新抽取向量 $\boldsymbol{v}$. 向量 $\boldsymbol{e}'$ 作为签名者的签名.

去盲过程：

计算 $\boldsymbol{e}=t(\boldsymbol{e}'-\boldsymbol{c})$，$\boldsymbol{e}$ 作为消息 M 的签名.

验证过程：

给定公钥 PK＝$\boldsymbol{A}_i$，签名 $\boldsymbol{e}$，如下操作：

计算 $\boldsymbol{A}_i\boldsymbol{e}=H\bmod q$ 且 $\|\boldsymbol{e}\|\leqslant r\sqrt{2m}$，如果成立，输出1，否则输出0.

2.2 效率分析[13]

由表1可以看到，与文献[4]相比，本方案在功能上增加分级管理的信息，但是签名、公钥、私钥的长度都在相同数量级.

表1 签名效率对比表

Tab.1 Efficiency comparison of the signatures

bit

效率指标	本文方案	文献[4]
公钥长度	$4*(m+j)n$	$4*mn$
密钥长度	$4*(m+j)^2$	$4*m^2$
签名长度	$4*(m+j)$	$4*m$

2.3 安全性证明

正确性：

引理3 如上方案，签名者 id_i 的签名 e' 满足验证正确性．

证明 验证中心得到签名 e' 后，对 e' 进行去盲变换：

$$e=t(e'-c)=t(v+t_1-c)=t(v+A_i^{-1}\mu-c)\ .$$

对于去盲后的消息签名 e，验证中心用公钥 A_i 来验证签名的正确性：

$$A_ie=tA_i(v+A_i^{-1}(t^{-1}H+A_ic)-c)=tA_iv+H+tA_ic-tA_ic=tA_iv+H(\mathrm{mod}\,q)=H(\mathrm{mod}\,q)\ .$$

盲性：

我们证明我们基于身份的盲签名在统计学上是盲的，也就是签名者所看到的值是独立于将要被签名的消息的．更准确地说，由两个消息所产生的签名是不可区分的．

所谓盲性是指签名者对其所签署的消息具体内容是不可见的．

定义1 盲性，设 (μ_0,e'_0)、(μ_1,e'_1) 是申请者对消息进行盲化得到的盲化消息和签名者对盲化消息进行签名得到的盲签名．给定 $\mu_b,e'_b,b\in(0,1)$，使得签名方案满足盲性，若签名者或挑战者在任意多项式时间内输出一个 b'，而 $b'=b$ 发生的概率至多为 $\frac{1}{2}+\frac{1}{n^c}$（其中 n 充分大，c 为一个常数），即 (μ_0,e'_0)、(μ_1,e'_1) 对于签名者或挑战者是不可区分的[14]．

引理4 本文给出的基于身份的盲签名满足盲签名对于盲性的要求．

证明 从方案中消息盲化的过程中我们知道，消息通过 $\mu=(t^{-1}H+A_ic)\mathrm{mod}\,q$ 被盲化，由抽样的过程我们知道，A_ic 近似服从均匀分布，H 作为原始消息 M 的哈希值也近似服从均匀分布，t 是任意选取的整数．所以对于签名者和挑战者来说，盲化消息 μ 在 Z_q^n 上是均匀分布的不可区分的．

分级性：

引理5 本方案中，父节点的签名者 id_k 对子节点的签名者 id_i 具有签名权[15]．

证明 父节点的签名者 id_k 的公钥为 A_k，私钥为 T_k，子节点的签名者 id_i 的公钥为 $A_i\leftarrow A_k\|H_2(\mathrm{id}_i)\in Z_q^{n\times(m+j)}$，私钥为 $T_i=\mathrm{ExtBasis}(T_k,A_i)$，并且 $\|\tilde{T}_k\|=\|\tilde{T}_i\|$ ．

利用 id_k 的公钥为 T_k 构造 A_i 的一组短基 $\begin{bmatrix}T_k & I_{m+j-1}\\ I_{m+j-1} & 0\end{bmatrix}$，

$$A_i\begin{bmatrix}T_k & I_{m+j-1}\\ I_{m+j-1} & 0\end{bmatrix}=A_k\|H_2(\mathrm{id}_i)\begin{bmatrix}T_k & I_{m+j-1}\\ I_{m+j-1} & 0\end{bmatrix}=A_kT_k+H_2(\mathrm{id}_i)*0=A_kT_k=0\ ,$$

并且满足 $\|\tilde{T}_k\|=\|\tilde{T}_i\|$，因此 $\begin{bmatrix}T_k & I_{m+j-1}\\ I_{m+j-1} & 0\end{bmatrix}$ 为 A_i 正交好基．

综上所述，父节点签名者 id_k 能利用自己的公钥和私钥构造出子节点的签名者 id_i 的一组好基，父节点对自己的节点具有签名权．

3 总结

本文在基于身份的盲签名基础上，运用格基扩展算法构造了盲签名的分级性，实现了上级签名者对下级签名者权限的有效管理，并且验证了正确性、安全性和分级性，通过对比分析，得出签名的效率相较于之前的签名方案没有增加．

参考文献：

[1] RÜCKERT M. Lattice-based blind Signatures[J]. Lecture Notes in Computer Science，2010，6477：413-430.

[2] CASH D，HFHEINZ D，KILTZ E. Bonsai trees，or how to delegate a lattice basis[C]//Proceeding of International Conference on

Theory & Applications of Cryptographic Techniques. Berlin：Springer，2010.
[3] PEIKERT C. Bonsai trees：arboriculture in lattice-based cryptography[J]. Manuscript，2009，2009(2)：147-191.
[4] 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)，2010，5(35)：550-553.
[5] 夏维. 格上基于盆景树模型的盲签名研究与设计[D]. 西安：西安电子科技大学，2012.
[6] 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.
[7] GENTRY C，PEIKERT C，VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]// Prodeeding of the 29th Annual ACM Symposium on Theory of Computing. New York：ACM，2008.
[8] ALWEN J，PEIKERT C. Generating shorter bases for hard random lattice[C]//Proceeding of 26th International Symposium on Theoretical Aspects of Computer Science. Freiburg，Germany：Springer，2009.
[9] WEN Xiaojun，CHEN Yongzhi，FANG Junbin. An interbank E-payment protocol based on quantum proxy blind signature[J]. Quantum Information Processing，2013，12(1)：549-558.
[10] VERMA G K. A proxy blind signature scheme over braid group[J]. I J Network Security，2009，1(3)：214-217.
[11] BELLARE M，NAMPREPRE C，NEVEN G. Security proofs for identity-based identification and signature schemes[J]. Journal of Cryptology，2009，22(1)：1-61.
[12] BELLARE M，KILTZ E，PEIKERT C. Identity-based trapdoor functions and applications[C]//Advences in Cryptology Eurocrypt'12. Berlin：Springer-Verlag，2012.
[13] 郑东，李祥学，黄征. 密码算法与协议[M]. 北京：电子工业出版社，2009.
[14] HOWGRAVE-GRAHAM N A，SMART N P. Lattice attacks on digital signature schemes[J]. Designs，Codes and Cryptography，2001，23(3)：283-290.
[15] SCHNORR C P. A hierarchy of polynomial time lattice basis reduction algorithms[J]. Theoretical Computer Science，1987，53(2)：201-224.

（编辑 张继学）