一种基于格理论的盲签名方案

王希震[1] 陈辉焱[2]

[1](西安电子科技大学通信工程学院 陕西 西安 710071)

[2](北京电子科技学院 北京 100070)

摘 要 量子计算机的发展使得传统公钥加密系统不再具有足够的安全性,研究抗量子的签名方案迫在眉睫,而格基签名可以满足这一需要。数字货币系统的出现使得盲签名得到了更多的关注,主要应用于匿名认证、电子投票等。通过对 qTESLA 方案以及 RBS 方案的研究和分析,给出一个基于格的盲签名方案,安全性基于 RLWE 问题以及 RSIS 问题的困难性,并证明了方案的盲性和 one-more 不可伪造性。

关键词 格 随机预言模型 盲签名

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.04.047

A BLIND SIGNATURE SCHEME BASED ON LATTICE THEORY

Wang Xizhen[1] Chen Huiyan[2]

[1](*School of Telecommunications Engineering, Xidian University, Xi'an 710071, Shaanxi, China*)

[2](*Beijing Electronics Science and Technology Institute, Beijing 100070, China*)

Abstract The development of quantum computer makes the traditional public key encryption system no longer provide enough security. Research on quantum-resistant signature schemes is urgent, and lattice-based signature can meet this need. With the emergence of digital currency system, blind signature attracts more attention, and it is mainly used in anonymous authentication and e-voting. In this paper, through the research and analysis of the qTESLA scheme and the RBS scheme, we gave a blind signature scheme based on lattice. The security was based on the difficulty of the RLWE problem and the RSIS problem, and the blindness and one-more unforgeability of the scheme was proved.

Keywords Lattice Random oracle model Blind signature

0 引 言

盲签名由 Chaum[1] 首次提出,在基于区块链的数字货币系统出现后得到了较多的关注。盲签名中,签名者无法得到关于正在签名的消息的任何信息,满足盲性;用户无法在不与签名者交互的情况下生成任何有效签名,满足 one-more 不可伪造性。盲签名的主要应用有匿名认证,即可使用户在几乎不泄露自身信息的情况下私下获取认证凭据[2],还有电子货币交易、电子投票系统[3]等。

格上盲签名的安全性基于格上困难问题,比起传统的基于大整数分解问题、离散对数问题等密码体制,它是抗量子计算机攻击的。格问题允许最坏情况对平均情况的归约,即随机选择的某个格问题实例至少与相关格问题的最坏情况实例同样难解[4]。Gentry 等[4]于 2008 年证明基于格的签名方案是安全的,并提出了使用单向陷门函数来构造格签名方案的框架,但 Rückert[5] 于 2010 年在亚密会上指出此框架不适用于盲签名方案,并提出了盲签名方案 RBS,该方案基于 Fiat-Shamir 方法构造[6],安全性基于哈希碰撞。2012 年,Gu 等[7] 在格上构造了一个基于身份的盲签名方案,方案是随机预言模型下安全的。2017 年,Gao 等[8] 提出了新的基于身份的盲签名方案,并在标准模型下证明了其安全性。2020 年 Alkadri 等[9] 给出了 BLAZE 盲签名方案,该方案基于 2010 年的 RBS 方案,且安全性基于格上计算问题 RSIS 的困难性假设。同年,Canard 等[10] 提出了一个新的盲签名方案,该方案没有

收稿日期:2020-12-06。**王希震**,硕士生,主研领域:格基签名。**陈辉焱**,高工。

使用异常终止的概念,达到了不需要重启的目的,并给出了基于该方案的部分盲签名方案。

数字签名方案 qTESLA 是由 Alkim 等[11]设计提出,现已进入美国 NIST 后量子密码算法标准征集第二轮,该方案基于 Fiat-Shamir 方法构造,安全性基于格上困难问题 R-LWE(Ring Learn with Error)。本文通过对 qTESLA 方案以及 RBS 方案的研究和分析,给出了一个盲签名方案,其安全性基于 RLWE 问题以及 RSIS 问题的困难性,并证明了方案的盲性和 one-more 不可伪造性。

1 预备知识

1.1 相关符号

分别用 $\mathbf{N}$、$\mathbf{Z}$、$\mathbf{R}$ 表示自然数集、整数集、实数集。用粗斜体小写字母表示列向量,粗斜体大写字母表示矩阵。对正整数 q,Z_q 表示在范围 $\left[\frac{-q}{2},\frac{q}{2}\right]\cap\mathbf{Z}$ 内的整数。定义函数:

$$[\cdot]_L:\mathbf{Z}\to\mathbf{Z},c\to(c \bmod^{\pm} q)\bmod^{\pm} 2^d \tag{1}$$

$$[\cdot]_M:\mathbf{Z}\to\mathbf{Z},c\to\frac{(c \bmod^{\pm} q-[c]_L)}{2^d} \tag{2}$$

输入为 v_i 时,向量 $\boldsymbol{v}$ 的欧几里得范数(ℓ_2 范数)定义为 $\|\boldsymbol{v}\|=(\sum_i|v_i|^2)^{1/2}$,它的 ℓ_∞ 范数定义为 $\|\boldsymbol{v}\|_\infty=\max_i|v_i|$。定义环 $R=\mathbf{Z}[x]/(x^n+1)$ 及其商 $R_q=R/qR$,其中 n 为奇素数。用 $\hat{a}$ 表示环元素 $a_0+a_1x+\cdots+a_{n-2}x^{n-2}\in R_q$,其系数对应一个向量 $\boldsymbol{a}\in\mathbf{Z}_q^{n-1}$,有 $\|\hat{a}\|=\|\boldsymbol{a}\|$ 且 $\|\hat{a}\|_\infty=\|\boldsymbol{a}\|_\infty$。用 $\hat{\boldsymbol{a}}=(\hat{a}_1,\hat{a}_2\cdots,\hat{a}_k)\in R_q^k$ 表示环元素向量,它的 ℓ_2 和 ℓ_∞ 范数分别为 $\|\hat{\boldsymbol{a}}\|=(\sum_i^k\|\hat{a}_i\|^2)^{1/2}$ 和 $\|\hat{\boldsymbol{a}}\|_\infty=\max_i\|\hat{a}_i\|_\infty$。文中对数底数都为 2,安全参数定义为 $\lambda\in\mathbf{N}$。一个函数 $f:\mathbf{N}\to\mathbf{R}$ 称为可忽略的,若存在 $n_0\in\mathbf{N}$,使得对任意多项式 p,当 $n>n_0$ 时,$f(n)<\frac{1}{p(n)}$ 成立。用 $negl(\lambda)$ 表示 λ 中一个可忽略函数。当概率至少为 $1-negl(\lambda)$ 时,概率被称为压倒性的。可数定义域 D 上的两个分布 X、Y 之间的统计距离定义为:

$$\Delta(X,Y)=\frac{1}{2}\sum_n|X(n)-Y(n)| \tag{3}$$

当 $\Delta(X,Y)=negl(\lambda)$ 时,分布 X、Y 称为统计学上接近的。用 $x\leftarrow D$ 表示 x 是根据分布 D 采样的。用 $x\leftarrow_{\$}S$ 表示 x 是一个有限集合 S 中的均匀随机元素。对两个算法 A 和 B,$(x,y)\leftarrow(A(a),B(b))$ 表示算法 A 和 B 的联合执行,其中 a 和 b 分别为 A 和 B 的私密输入,x 和 y 分别为 A 和 B 的私密输出。若 A 最多可以调用 B 的 k 次方案执行,记为 $A^{(\cdot,B(b))^k}(a)$。

1.2 盲签名方案概念及其安全性定义

本盲签名方案包含三个概率多项式时间算法:KeyGen、Sign 和 Verify。

(1) KeyGen 为密钥生成算法。输入安全参数 1^λ,PKG 运行 KeyGen 算法,生成用于验证的公钥 pk 和用于签名的私钥 sk。

(2) Sign 为签名算法。签名者 S 输入私钥 sk,用户 U 输入公钥 pk 和消息 μ,其中 $\mu\in M$,M 为消息空间。S 得到输出的随机变量 V 和签名 σ,即 $(V,\sigma)\leftarrow(S(sk),U(pk,\mu))$。用 $\sigma=\perp$ 表示算法执行失败,需要重启签名方案。

(3) Verify 为验证算法。输入公钥 pk、消息 μ 及其签名 σ,若签名 σ 是有效的,算法输出 1;反之则输出 0。

盲签名方案需要具有正确性,即验证算法 Verify 总是以压倒性的概率在合法创建的密钥下验证合法签名的消息。盲签名方案的安全性由盲性和 one-more 不可伪造性构成[8],由以下用户 U 和敌手 S^* 之间的博弈 Blind 和 Forge 来定义。若用户 U 在任意执行过程中输出 $\perp$,则敌手 S^* 失败且得不到任意签名。以下博弈在敌手 S^* 恶意选择公钥 pk 的情况下也成立。

定义 1 盲性。盲性保证恶意的签名者无法知道关于所签名消息的任何信息。若对于一盲签名方案,任意敌手 S^* 运行时间至多为 t,且完成下述博弈输出 1 的概率为:

$$P_r[Blind_{S^*}(\lambda)=1]\leqslant\frac{1}{2}+\varepsilon \tag{4}$$

即 S^* 在博弈中的优势定义为:

$$\varepsilon=A_{dv_{S^*}}=\left|P_r[b^*=b]-\frac{1}{2}\right| \tag{5}$$

则此盲签名被称为具有 (t,ε)-盲性的。

Blind:

(1) 敌手签名者 S^* 运行密钥生成算法 $(pk,sk)\leftarrow Keygen(1^\lambda)$,得到 pk 和 sk。然后选择两个消息 μ_0、μ_1,与 pk 一起发给合法用户 U。U 随机选择一比特 b。

(2) 用户 U 和敌手 S^* 执行两次签名算法。由 b,U 按序输出两个签名 σ_b 和 σ_{1-b}。

(3) 敌手 S^* 得到两个签名 σ_0 和 σ_1,并猜测签名生成的顺序,输出 b^*。若猜测正确,即 $b^*=b$,则输出 1;否则输出 0。

定义 2 one-more 不可伪造性。one-more 不可伪造性确保每一次完整运行签名算法,只能生成一个

有效签名。对于某个盲签名,如果任意敌手用户 U^* 运行时间至多为 t,进行至多 q_{Sign} 次签名查询和 q_{H} 次随机预言机查询,且完成下述博弈输出 1 的概率为 $P_r[Forge_{U^*}(\lambda)=1]\leqslant\varepsilon$,则此盲签名被称为($t$,$q_{\text{Sign}}$,$q_{\text{H}}$,$\varepsilon$)-one-more 不可伪造的。若上述博弈中的条件 $\mu_i\neq\mu_j$ 变为$(\mu_i,\sigma_i)\neq(\mu_j,\sigma_j)$时,输出 1 的概率仍为 $P_r[Forge_{U^*}(\lambda)=1]\leqslant\varepsilon$,则此盲签名被称为强($t$,$q_{\text{Sign}}$,$q_{\text{H}}$,$\varepsilon$)-one-more 不可伪造的。

Forge:

(1) 执行密钥生成算法$(pk,sk)\leftarrow Keygen(1^\lambda)$,得到 pk 和 sk。

(2) 用户 U^* 和签名者 S 执行 l 次签名算法,得到 l 对(μ_i,σ_i)。

(3) 设 k 为成功调用签名算法的次数,若对于所有的$1\leqslant i<j\leqslant l$,任取 $i\in\{1,2,\cdots,l\}$,$k+1=l$,当 $\mu_i\neq\mu_j$时,$Verify(pk,\mu_i,\sigma_i)=1$,则返回 1;否则返回 0。

1.3　格

定义 3　格。设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\in\mathbf{R}^m$ 为一组线性无关的向量,则 $\boldsymbol{B}^{m\times n}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)$ 为格 L 的一组基,格 L 可由下式表示:

$$L=L(\boldsymbol{B})=\{z_1\boldsymbol{b}_1+z_2\boldsymbol{b}_2+\cdots+z_n\boldsymbol{b}_n\mid z_i\mid\in\mathbf{Z}\}\quad(6)$$

其中格 L 的维度为 m,秩为 n,且 $n\leqslant m$。当 $m=n$ 时,L 为满秩格。每个格有不止一个格基,相同格的格基可通过幺模矩阵相互转换。格的行列式用 $det(L)$ 表示,为 L 的体积,$\det(L)=\sqrt{\det(\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{B})}$。$L$ 为满秩格时,$\det(L)=|\det(\boldsymbol{B})|$。对相同的格,不同的格基仍能得到相同的行列式。

1.4　格上困难问题

定义 4　RSIS 问题。设 $n,q,k\in\mathbf{Z}^+,\beta\in\mathbf{R}^+$。给定一均匀随机选取的向量 $\hat{\boldsymbol{a}}=(\hat{a}_1,\hat{a}_2,\cdots,\hat{a}_k)\in R_q^k$,求一非零向量 $\hat{\boldsymbol{x}}=(\hat{x}_1,\hat{x}_2,\cdots,\hat{x}_{k+1})\in R^{k+1}$,使得$[\hat{\boldsymbol{a}}\ \boldsymbol{1}]\cdot\hat{x}=0(\bmod q)$,其中$\|\hat{\boldsymbol{x}}\|\leqslant\beta$。

定义 5　RLWE 问题[13]。令 $R=\mathbf{Z}[x]/\boldsymbol{\Phi}_n(x)$,$\psi$ 为 $\boldsymbol{Q}[x]/\boldsymbol{\Theta}_n(x)$ 上的一个分布。定义 $\overline{\psi}$ 为 R 上的分布,由 $\hat{e}=\lfloor\hat{e}'\bmod\boldsymbol{\Phi}_n(x)\rceil\in R$ 得到,其中,$\hat{e}'\leftarrow\psi$,$\lfloor f\rceil$表示多项式的系数舍入到最近整数后得到的多项式。令 q 为满足 $q=1(\bmod 2n)$ 的素数,$R_q=R/qR$,对 $\hat{s}\in R_q$,定义 $A_{\hat{s},\psi}$ 为 $R_q\times R_q$ 上的分布,由采样对$(\hat{a},\hat{a}\hat{s}+\hat{e})$得到,其中 $\hat{a}\leftarrow_{\$}R_q$,$\hat{e}\leftarrow\overline{\psi}$。定义 $RLWE_{q,\psi,l}$问题如下:

给定 l 对服从分布 $A_{\hat{s},\psi}$的采样$(\hat{a},\hat{a}\hat{s}+\hat{e})$,和 l 对从 $R_q\times R_q$ 上均匀随机选取的$(\hat{a},\hat{b})$,以优势 $1/poly(n)$ 进行区分。

1.5　高斯分布

用 $D_{L,\sigma,\boldsymbol{c}}$表示格 L 上的离散高斯分布,其中标准差 $\sigma>0$,中心 $\boldsymbol{c}\in\mathbf{R}^n$。定义如下:向量 $\boldsymbol{x}$ 在格上的概率如式(7)所示。

$$D_{L,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})/\rho_{\sigma,\boldsymbol{c}}(L)\quad(7)$$

其中:

$$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{2\sigma^2}\right)\quad(8)$$

$$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{L})=\sum_{\boldsymbol{x}\in L}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})\quad(9)$$

$\boldsymbol{c}=0$ 时此下标可忽略不写。

用 ψ_σ 表示 $\boldsymbol{Q}$ 上中心为 0,标准差为 σ 的高斯分布。ψ_σ^n 表示向量$(v_1,v_2,\cdots,v_n)$在 $\boldsymbol{Q}^n$ 上的球形高斯分布,其中每个 v_i 都从分布 ψ_σ 中独立选取。

2　盲签名方案

以下给出方案的详细描述。其中 n 为奇素数,q 为素数且满足 $q=1(\bmod n)$。为了满足 RLWE 问题的困难性归约,取 $a\in(0,1)$ 且 $aq>\omega(\sqrt{\log n})$。定义:

伪随机函数 $PRF:\{0,1\}^\kappa\rightarrow\{0,1\}^{\kappa,k+2}$,输入一个长度为 k 比特的预随机种子(pre-sedd),将其映射到 $k+2$ 个长度为 κ 比特的随机种子(seed)。

多项式 $a_1,a_2,\cdots,a_k$ 的生成函数 $Gen(x):\{0,1\}^\kappa\rightarrow(R_q^\times)^k$,输入长度为 κ 比特的随机比特串 $seed$,将其映射到 k 个多项式 $a_i\in R_q^\times$。

Com 为一统计上隐藏的绑定承诺函数,$Com:\{0,1\}^*\times\{0,1\}^\kappa\rightarrow\{0,1\}^\kappa$,其不透露关于绑定消息的信息,且要求不存在 PPT 算法能找到$\mu'\neq\mu$,使得 $Com(\mu;\boldsymbol{r})=Com(\mu';\boldsymbol{r}')$。

公共哈希函数 $\mathrm{H}:R_q^k\times\{0,1\}^\lambda\times\{0,1\}^\lambda\rightarrow\{0,1\}^\kappa$,输入 k 个多项式 $\boldsymbol{v}_i\in R_q$,$Com(\mu;\boldsymbol{r})$,输出长度为 κ 的比特串。

$RejSamp(x)$表示对输入 x 进行拒绝采样,接受则输出 1,拒绝则输出 0。

2.1　方案描述

KeyGen:给定 1^κ,生成算法选择一均匀预随机种子 $pre\text{-}seed\in\{0,1\}^\kappa$,使用 $PRF(pre\text{-}seed)$ 选择随机$\{seed_s,seed_{e_1},\cdots,seed_{e_k},seed_a\}$,使用 $Gen(seed_a)$将其扩展为一多项式 $\hat{a}\in R_q$。$\hat{s}\leftarrow D_{Z,\sigma}^n(seed_a)$,当$\frac{\kappa(\kappa+1)}{2}\cdot||\hat{s}||_\infty>L_S$时,重新取样;$\hat{e}\leftarrow D_{Z,\sigma}^n(seed_{ei})$,当$\frac{\kappa(\kappa+1)}{2}\cdot||\hat{e}||_\infty>L_E$,重新取样。

$$\hat{t}=\hat{a}\hat{s}+\hat{e}(\bmod q)\quad(10)$$

私钥 sk 为二元组$(\hat{s},\hat{e})$,公钥 pk 为二元组$(seed_a,\hat{t})$。

Sign:

step1 给出 $seed_a$,sk 和消息 μ。令 $i\in\{1,2,\cdots,k\}$,使用 $Gen(seed_a)$ 生成多项式 $\hat{a}\in R_q$,签名者 S 从分布 $D^n_{Z,s'}$ 中采样两个掩蔽项 $y^*_{i,1}$,$y^*_{i,2}$,并将:

$$y_i=a_iy^*_{i,1}+y^*_{i,2}(\bmod q) \tag{11}$$

发送给用户 U。

step2 用户 U 对要签名的消息进行盲化。得到 $\hat{a}$ 和 $\hat{y}$ 后,随机取 $\boldsymbol{r}\leftarrow_{\$}\{0,1\}^{\kappa}$,取 $\alpha,\beta\leftarrow D^n_{Z,s}$。计算承诺 $\tau=Com(\mu;\boldsymbol{r})$。$U$ 生成:

$$c^*=H(\hat{a}\hat{y}+\hat{a}\alpha+\hat{t}\beta(\bmod q),\tau) \tag{12}$$

计算 $c=c^*+\beta$ 来隐藏 c^*,采用拒绝采样 RejSamp 算法,如果输出 0,重新进行此步骤,输出 1 则将结果发送给签名者 S。

step3 S 对盲化消息进行签名。为满足最终签名的正确性,签名者 S 首先判断是否 $\|[\hat{a}\hat{y}-\hat{e}c]_L\|_\infty<2^{d-1}-L_E$ 且 $\|\hat{a}\hat{y}-\hat{e}c\|_\infty<\left\lfloor\frac{q}{2}\right\rfloor-L_E$。如果不满足,则返回签名算法 step2。对于 $i\in\{1,2,\cdots,k\}$,S 计算:

$$z^*_i=y_i+s_ic \tag{13}$$

然后 S 使用拒绝采样 RejSamp 来保证 z^* 不会泄露关于私钥 sk 的任何信息,若 $z^*_i\notin D^n_{s'}$,RejSamp 输出 0,则 S 重启签名算法,否则将 $\hat{z}^*$ 发给用户 U。

step4 U 计算 $\hat{z}=\hat{z}^*+\alpha$。使用拒绝采样,如果 $\hat{z}\notin D^n_s$,则 $RejSamp(\hat{z})=1$,给 S 发送 ok,并返回签名$(\mu,(\boldsymbol{r},\hat{z},c^*))$。若 $RejSamp(\hat{z};\rho')=0$,则发送(τ,α,β,c^*)给 S 进行验证。

S 的验证分为 3 步:

$$c^*=c-\beta=H(\hat{a}\hat{y}+\hat{a}\alpha+\hat{t}\beta(\bmod q),\tau) \tag{14}$$

$$c^*=H(\hat{a}\hat{z}^*+\hat{a}\alpha-\hat{t}c^*(\bmod q),\tau) \tag{15}$$

$$RejSamp(\hat{z})=0 \tag{16}$$

若三步检测都通过,即 S 验证 U 未得到有效签名后,重启整个签名方案。

step5 返回签名$(\mu,(\boldsymbol{r},\hat{z},c^*))$。

Verify:验证算法的输入为$(seed_a,\hat{t},\mu,(\boldsymbol{r},\hat{z},c^*))$。当且仅当 $\hat{z}\in D^n_s$,且当式(17)成立时,验证通过。

$$c^*=H(\hat{a}\hat{z}^*+\hat{a}\alpha-\hat{t}c^*(\bmod q),\tau) \tag{17}$$

3 方案分析

3.1 安全性分析

以下证明方案的正确性、盲性和 one-more 不可伪造性。

引理 1[14] 对任意 $t,\eta>0$,有:

$$P_{r_x\leftarrow D_{\mathbf{Z},\sigma}}[|x|>t\sigma]\leqslant 2e^{-\frac{t^2}{2}} \tag{18}$$

$$P_{r_x\leftarrow D_{\mathbf{Z}^m,\sigma}}[\|x\|>\eta\sigma\sqrt{m}]\leqslant\eta^m e^{\frac{m}{2}(1-\eta^2)} \tag{19}$$

引理 2[14] 设 $V\subseteq\mathbf{Z}^m$,V 中元素的范数被 T 绑定,$\sigma=\omega(T\sqrt{\log m})$,且 $h:V\to\mathbf{R}$ 为一概率分布,则存在一常数 $M=O(1)$ 使得,任取 $v\in V$,有:

$$P_{r_z\leftarrow D_{\mathbf{Z}^m,\sigma}}[D_{\mathbf{Z}^m,\sigma}(\boldsymbol{z})\leqslant M\cdot D_{\mathbf{Z}^m,\sigma,\boldsymbol{v}}(\boldsymbol{z})]\geqslant 1-\varepsilon \tag{20}$$

其中 $\varepsilon=2^{-\omega(\log m))}$。取 $\boldsymbol{v}\leftarrow h$,以下两点在统计距离为时 $\delta=\frac{\varepsilon}{M}$适用:

(1) $\boldsymbol{z}\leftarrow D_{\mathbf{Z}^m,\sigma,\boldsymbol{v}}$,以$\frac{D_{\mathbf{Z}^m,\sigma}(\boldsymbol{z})}{M\cdot D_{\mathbf{Z}^m,\sigma,\boldsymbol{v}}(\boldsymbol{z})}$的概率输出$(\boldsymbol{z},\boldsymbol{v})$,其中任意输出的概率为$(1-\varepsilon)/M$;

(2) $\boldsymbol{z}\leftarrow D_{\mathbf{Z}^m,\sigma}$,以 $1/M$ 的概率输出$(\boldsymbol{z},\boldsymbol{v})$。

若 $\sigma=\alpha T$,α 为正数,则 $M=\mathrm{e}^{\frac{12}{\alpha}+\frac{1}{2\alpha^2}}$,$\varepsilon=2^{-100}$。

定理 3 在运行本签名算法至多 M 次之后,可以生成一个有效签名,使得验证算法输出 1。令 δ',δ,$\eta>0$,$s=\eta\delta\sqrt{kn}s'$,$s'=\delta'\sqrt{k}\|\hat{s}\|$,$B=\eta s\sqrt{n}$。那么运行算法至多 $M=M_1M_2$ 次后,本方案生成有效签名的概率至少为 $1-2^{\lambda}$。其中:

$$M_1=\exp\left(\frac{12}{\delta'}+\frac{1}{2\delta'^2}\right) \tag{21}$$

$$M_2=\exp\left(\frac{12}{\delta}+\frac{1}{2\delta^2}\right) \tag{22}$$

式中:M_1、M_2 分别为用户和签名者的重复次数。

证明:在不考虑重启时,在模 q 的意义下,我们有:

$$\begin{aligned}\hat{a}\hat{z}-\hat{t}c^*&=\hat{a}(\hat{z}^*+\alpha)-\hat{t}(c-\beta)=\\&\hat{a}(\hat{y}+\hat{s}c)+\hat{a}\alpha-\hat{t}c+\hat{t}\beta=\\&a\hat{y}-\hat{e}c+\hat{a}\alpha+\hat{t}\beta=\\&(\hat{a}\hat{y}-\hat{e}c-[\hat{a}\hat{y}-\hat{e}c]_L)/2^d+\hat{a}\alpha+\hat{t}\beta\end{aligned} \tag{23}$$

由于 $\|[\hat{a}\hat{y}-\hat{e}c]_L\|_\infty<2^{d-1}-L_E$,与 $\|\hat{a}\hat{y}-\hat{e}c\|_\infty<\left\lfloor\frac{q}{2}\right\rfloor-L_E$,且我们有:

$$L_E\geqslant\frac{\kappa(\kappa+1)}{2}\cdot||\hat{e}||_\infty\geqslant||\hat{e}||_\infty\geqslant||\hat{e}c||_\infty \tag{24}$$

因此可以得出:

$$\begin{aligned}&(\hat{a}\hat{y}-\hat{e}c-[\hat{a}\hat{y}-\hat{e}c]_L)/2^d+\hat{a}\alpha+\hat{t}\beta=\\&\quad(\hat{a}\hat{y}+[-\hat{e}c-\hat{a}\hat{y}+\hat{e}c]_L)/2^d+\hat{a}\alpha+\hat{t}\beta=\\&\quad\hat{a}\hat{y}+\hat{a}\alpha+\hat{t}\beta\end{aligned} \tag{25}$$

现在考虑重启的情况,在签名算法 step2 输出时,用户能局部处理所发生的异常终止,并不会影响方案的正确性,只需要考虑 step3 和 step4 中关于签名输出的异常终止便可。现考虑签名算法 step3 中签名者 S 采用拒绝抽样。由引理 2,拒绝抽样算法输出 1 的概率为:

$$(D^{kn}_{Z,s'}(\hat{z}^*)/(M_1 D^{kn}_{Z,s',\hat{s}c}(\hat{z}^*)) \tag{26}$$

当 $s'=\delta'\sqrt{k}\|\hat{s}\|=\delta'\|\hat{s}c\|$,重复次数为:

$$M_1=\exp\left(\frac{12}{\delta'}+\frac{1}{2\delta'^2}\right) \tag{27}$$

签名算法 step4 中用户 U 采用拒绝采样,输出 1 的概率为:

$$(D^{n}_{Z,s}(\hat{z})/(M_2 D^{n}_{Z,s,\hat{z}^*}(\hat{z})) \tag{28}$$

因为 $s=\eta\delta\sqrt{kn}s'$,而 $\hat{z}^*$ 服从分布 $D^n_{\sqrt{k}s'}$,由引理 1 有,$\|\hat{z}^*\|\leqslant\eta\sqrt{kn}s'$,故 $s=\delta\|\hat{z}^*\|$,因此重复次数为:

$$M_2=\exp\left(\frac{12}{\delta}+\frac{1}{2\delta^2}\right) \tag{29}$$

总重复次数为 $M=M_1M_2$[15],定理得证。

定理 4　在本方案中,签名者无法得到所签消息的任何信息,方案具有盲性。

证明　在定义 1 的博弈 Blind 中,敌手签名者 S^* 选择两个消息 μ_0、μ_1,并与用户 U 进行两次交互,U 随机选择一比特 b,并按序输出两个签名 σ_b 和 σ_{1-b}。以下证明,每次交互 U 都不泄露关于当前签名消息的任何信息,即协议执行过程中交换的信息与用户的输出相互独立。

签名算法最后返回签名$(\mu,(\boldsymbol{r},\hat{z},c^*))$,因 $\boldsymbol{r}$ 为均匀随机的,又 c^* 为公共哈希函数 H 的输出结果,为一长度为 κ 的比特串,因此现在只需要分析 c 和 $\hat{z}$ 与对应的消息独立即可。

现分析 c,设 c_b 和 c_{1-b}分别是用户根据消息 μ_b、μ_{1-b}生成的比特串,因为 $c=c^*+\beta$,且以 $D^{kn}_{Z,s'}(\hat{z}^*)/(M_1D^{kn}_{Z,s',\hat{s}c}(\hat{z}^*))$的概率输出,由引理 2,$c_b$ 和 c_{1-b}都服从高斯分布 $D^n_{Z,s}$,即它们的统计距离为 0,因此 c 和 μ 是独立无关的。

令 z_b 和z_{1-b}分别为用户根据消息μ_b 和μ_{b-1}输出的签名部分。由于 $\hat{z}=\hat{z}^*+\alpha$,且以 $D^n_{Z,s}(\hat{z})/(M_2D^n_{Z,s,\hat{z}^*}(\hat{z}))$的概率输出,由引理 2,$z_b$ 和 z_{1-b}都服从高斯分布 $D^n_{Z,s}$,同理,$\hat{z}$ 和消息 μ 也是独立无关的。

而若需要重启协议,则 $\boldsymbol{r}$、α、β 都需要重新选择,两次协议的执行之间是相互独立的,故签名者不会得到关于需要签名的消息的任何信息。

由本方案的参数设置,恢复私钥的难度相当于解 RLWE。接下来我们给出强 one-more 不可伪造性的证明。我们定义公钥 pk 是从 $R_q\times R_q$ 上随机均匀选取得到的$(\hat{a},\hat{t})$。

定理 5　在本签名方案中,如果格上计算问题 RSIS 是$(t_{\mathrm{R}},\varepsilon_{\mathrm{R}})$-困难的,则本方案为强$(t_{\mathrm{F}},q_{\mathrm{Sign}},q_{\mathrm{H}},\varepsilon_{\mathrm{F}})$-one-more 不可伪造的。

其中:

$$t_{\mathrm{R}}\leqslant t_{\mathrm{F}}\leqslant q_{\mathrm{H}}^{q_{\mathrm{Sign}}}(q_{\mathrm{Sign}}+q_{\mathrm{H}}) \tag{30}$$

$$\varepsilon_{\mathrm{R}}\geqslant\min\{\varepsilon_f/2(l+1),\varepsilon_a\} \tag{31}$$

概率 ε_a、ε_f 将在证明中给出。用 l 表示成功的签名查询,$l\leqslant q_{\mathrm{Sign}}$。用 M 表示签名算法的平均重复次数,签名算法成功生成一个签名的概率约为 $1/M$。

证明　假设存在伪造算法 F,能以 ε_{F} 的概率赢得定义 2 的博弈 Forge。以下构造归约算法 R,能以 ε_{R} 的概率攻破 RSIS 问题。

设置:R 的输入为一随机对$(\hat{a},\hat{t})\in R_q\times R_q$,$R$ 随机选取随机预言机查询的结果$\{\hat{c}_1,\hat{c}_2,\cdots,\hat{c}_{q_{\mathrm{H}}}\}$。$R$ 用$(\hat{a},\hat{t})$作为输入运行 F。

随机预言机查询:R 初始化一列表 L,表中存有随机预言查询的输入和 B^n_k 中对应的结果。若本次查询的输入曾经被查询过,则 R 直接从中读取结果并返回;否则,返回一个新的 $c\in B^n_k$,并更新列表 L。

盲签名查询:从 F 处得到签名查询后,R 作为签名者与作为用户的 F 依签名算法进行交互。不用计算,R 直接从 $D_{\mathbf{Z},s'}$中均匀随机选取 $\hat{z}_1^*,\hat{z}_2^*,\cdots,\hat{z}_k^*$。由引理 2,R 以概率 $1/M_1$ 将 $\hat{z}_1^*,\hat{z}_2^*,\cdots,\hat{z}_k^*$ 发回给 F;同理,F 以概率 2 将 $\hat{z}$ 发给 R。成功生成签名的概率为 $1/(M_1\cdot M_2)=1/M$。

输出:在 $l\leqslant q_{\mathrm{Sign}}$次成功执行签名算法后,若 F 能输出 $l+1$ 对有效的消息-签名对(μ_i,σ_i),则以下两种情况之一必成立:

(1) 其中两个不同消息 μ_1、μ_2 在执行签名算法时使用了相同的 c^*,则验证算法产生:

$$H(\hat{a}\hat{z}_1-\hat{t}c^*(\mathrm{mod}\ q),\tau)=H(\hat{a}\hat{z}_2-\hat{t}c^*(\mathrm{mod}\ q),\varrho) \tag{32}$$

很大概率上,这代表 $\mu_1=\mu_2$ 及 $\hat{a}\hat{z}_1-\hat{t}c^*=\hat{a}\hat{z}_2-\hat{t}c^*(\mathrm{mod}\ q)$。否则,F 能找到 c^* 的另一个原象,或 Com 的绑定性质不成立。若 $\mu_1=\mu_2$,则 $\hat{z}_1\neq\hat{z}_2$,故:

$$\hat{a}(\hat{z}_1-\hat{z}_2)\neq 0(\mathrm{mod}\ q) \tag{33}$$

有 $\|\hat{z}_1\|,\|\hat{z}_2\|\leqslant B$,有:

$$\|\hat{z}_1-\hat{z}_2\|\leqslant 2B \tag{34}$$

(2) 若 F 输出的所有签名都有不同的随机预言查询结果,则 R 取一个下标 $i\in\{1,2,\cdots,l+1\}$,使得当 $j\in\{1,2,\cdots,q_{\mathrm{H}}\}$时 $c_i^*=c_j^*$,记录$(\mu_i,(\boldsymbol{r},\hat{z},c_i^*))$。用同样的随机数和随机预言查询$\{c_1,\cdots,c_{i-1},c'_1,\cdots,c'_{q_{\mathrm{H}}-i}\}$,其中$\{\hat{c}'_1,\hat{c}'_2,\cdots,\hat{c}'_{q_{\mathrm{H}}-i}\}$为新的随机元素,再次调用 F。假设 F 的输出为$(\mu'_i,(\tau^*,\boldsymbol{r}^*,\hat{z}^*,c'^*_i))$。由分叉引理[16],令 $c_i^*\neq c'^*_i$ 的概率为 ε_f。则有很大的概率有

$$\hat{a}\hat{z}-\hat{t}c_i^*=\hat{a}\hat{z}^*-\hat{t}c'^*_i(\mathrm{mod}\ q) \tag{35}$$

得 $\hat{a}(\hat{z}-\hat{z}^*)=\hat{t}(c_i^*-c'^*_i)(\mathrm{mod}\ q)$。此处相当于解

RSIS 问题。因两对签名都是有效的,故有 $\|\hat{z}\| \leqslant B$ 和 $\|\hat{z}^*\| \leqslant B$,得到 $\|\hat{z}-\hat{z}^*\| \leqslant 2B$,且 $\|c_i^* - c_i'^*\|_\infty \leqslant 2$。

分析:算法 R 最多使用不同的随机数执行 q_H^{l+1} 次随机预言机查询。在没有私钥的情况下,比起调用完整的签名算法,用算法 R 得到的 $(\hat{z}_1^*, \hat{z}_2^*, \cdots, \hat{z}_k^*)$ 在统计上为不可区分的。

若 F 能输出 $l+1$ 对有效的消息-签名对,则其中一对有效消息-签名对不是由签名算法得到的。R 取一下标 i,使得当 $j \in \{1,2,\cdots,q_H\}$ 时,$c_i^* = c_j^*$ 的概率为 $1/(l+1)$。又 c_i^* 为 F 一随机预言查询的概率为 $1-1/|B_k^n|$,$|B_k^n| = 2^k(n)$。故 $c_i^* = c_j^*$ 的概率为 $\varepsilon_F - 1/|B_k^n|$,F 的 q_H^{l+1} 次运行中的某一次有 $c_i^* = c_j^*$ 的概率为 $\frac{1}{2}$。由分叉引理,F 在伪造签名的过程中使用了 c'^*_i 且 $c_i^* \neq c'^*_i$ 的概率至少为:

$$\varepsilon_f \geqslant (\varepsilon_F - 1/|B_k^n|)\left(\left(\varepsilon_F - \frac{1}{|B_k^n|}\right)/(q_{Sign}+q_H) - 1/|B_k^n|\right) \tag{36}$$

故 R 成功执行的概率为:

$$\varepsilon_R \geqslant \varepsilon_f/(2(l+1)) \tag{37}$$

即当 ε_f 足够大时 ε_R 也足够大。又 $c_i^* \neq c'^*_i$ 的概率不可忽略,故 R 成功执行的概率不可忽略。

若用户能在签名算法 step4 异常终止后产生一个有效签名,即签名算法的 step4 中 U 会发送 (τ,α,β,c^*) 给 S,S 对其进行三次检测。假设 U 产生的有效签名为 $(\boldsymbol{r},\hat{z}',c'^*)$。

若 $c'^* = c^*$,则第二步检测得到 $\hat{a}(\hat{z}-\hat{z}') = 0 \pmod q$。若 $\hat{z}-\hat{z}' = 0$,与第三步检测矛盾。$\|\hat{z}\| \leqslant B + \eta\sqrt{kn}s' = B + s/\alpha$,有:

$$\|\hat{z}-\hat{z}'\| \leqslant 2B + s/\alpha \tag{38}$$

若 $c'^* \neq c^*$,则 U 可能用 $c'^* = c^* + \beta$ 来隐藏 c^*,则 $\beta \neq \beta'$,故 U 为了计算 β 必须知道 H 的输出,成功概率为:

$$\varepsilon_a \geqslant \varepsilon_F(1 - 1/|\mathbf{P}_k^{n-1}|) \tag{39}$$

算法 R 总的成功概率为:

$$\min\{\varepsilon_f/2(l+1), \varepsilon_a\} \tag{40}$$

这与 RSIS 问题是格上困难问题的安全性假设相矛盾,定理得证。

3.2 效率分析

我们对方案的效率和安全性进行了分析,现给出其与文中提及的两个方案的对比分析。相较于盲签名 RBS 方案,本方案的安全性基于格上 RLWE 问题及 RSIS 问题的困难性假设,而非碰撞问题;相较于常规签名 qTESLA 方案,本方案添加了消息的盲化过程,确保消息不被签名者知道。表 1 是具体的分析。

表 1 具体分析

方法	私钥	公钥	签名	困难问题
RBS	$n\log(t\sigma+1)$	n	$n\log(ts+1)$	哈希碰撞
qTESLA	$n(k+1)\log(t\sigma+1)$	$kn\log q$	$n\log(ts+1)$	RLWE
本文	$2n\log(t\sigma+1)$	$kn\log q$	$n\log(ts+1)$	RLWE RSIS

4 结 语

本文通过对 qTESLA 方案以及 RBS 方案的研究和分析,给出了一个随机预言模型下安全的基于格的盲签名方案,证明了方案的盲性,并基于格上的困难问题证明了方案具备强 one-more 不可伪造性。

参 考 文 献

[1] Chaum D, Rivest R L, Sherman A T. Blind signatures for untraceable payments[J]. Advances in Cryptology, 1983, 10(18): 199 - 203.

[2] Baldimtsi F, Lysyanskaya A. Anonymous credentials light [C]//ACM SIGSAC Conference on Computer & Communications Security, 2013: 1087 - 1098.

[3] Kumar M, Katti C P, Saxena P C. A secure anonymous E-voting system using identity-based blind signature scheme [C]//International Conference on Information Systems Security, 2017: 29 - 49.

[4] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]//40th Annual ACM Symposium on Theory of Computing, 2008: 197 - 206.

[5] Rückert M. Lattice-based blind signatures[C]//International Conference on the Theory and Application of Cryptology and Information Security, 2010: 413 - 430.

[6] Lyubashevsky V. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures [C]//International Conference on the Theory and Application of Cryptology and Information Security, 2009: 598 - 616.

[7] Gu C X, Chen L, Zheng Y H. ID-based signatures from lattices in the random oracle model[C]//International Conference on Web Information Systems and Mining, 2012: 222 - 230.

[8] Gao W, Hu Y P, Wang B C, et al. Identity-based blind signature from lattices in standard model [C]//International Conference on Information Security and Cryptology, 2017: 205 - 218.

(下转第 332 页)

分析表6得到,随着样本数量的提升,不同方法在识别研究对象攻击类型过程中的 DCP 值均有所提升。其中本文方法在的 DCP 值最高达到 0.006 3%,与两种对比方法相比明显下降,由此说明本文方法在实际应用过程中具有较低的能耗。本文方法能耗较低的原因是在对攻击类型识别之前,构建了安全态势监测模型,充分利用该模型的优势,即通过数据融合技术实现态势感知分析,数据融合将来自多个信息源的数据收集起来,进行过滤、归并、关联,提升数据的有效性和精确度,减少数据中心内关键设备直接用于数据信息计算、处理、存储、传输、交换的能源能耗。

3 结 语

本文研究基于安全态势监测模型的泛在终端种类攻击自动识别方法,基于泛在终端安全态势监测结果,利用支持向量机模型识别泛在终端攻击种类,测试结果显示本文方法具有较高的识别精度与能耗。

参 考 文 献

[1] Cherpakov A V, Shlyakhova E A, Egorochkina I O, et al. Identification of concrete properties in beam-type structures with defects based on dynamic methods[J]. Materials Ence forum, 2018, 931(1):373 - 378.

[2] 王兴涛,赵训威,付海旋,等. 基于嵌入式系统的电力无线专网远程通信终端研制[J]. 电子技术应用,2020,46(1):108 - 112.

[3] 戚湧,郭诗炜,李千目. 电网融合泛在网信息平台设计及安全威胁分析[J]. 计算机科学,2017,44(3):150 - 152.

[4] 曲朝阳,董运昌,刘帅,等. 基于生物免疫学方法的泛在电力物联网安全技术[J]. 电力系统自动化,2020,44(2):1 - 12.

[5] 余洋,朱少敏,卞超轶. 基于知识图谱的泛在电力物联网安全可视化技术[J]. 电信科学,2019,35(11):132 - 139.

[6] Yang L, Liu J, Zhang Y. An intelligent security defensive model of SCADA based on multi-agent in oil and gas fields [J]. International Journal of Pattern Recognition and Artificial Intelligence, 2020, 34(1):1 - 13.

[7] 钱斌,蔡梓文,肖勇,等. 基于模糊推理的计量自动化系统网络安全态势感知[J]. 南方电网技术,2019,13(2):51 - 58.

[8] 韩晓露,刘云,张振江,等. 基于 IFS-NARX 模型的网络安全态势预测[J]. 吉林大学学报(工学版),2019,49(2):592 - 598.

[9] 丁华东,许华虎,段然,等. 基于贝叶斯方法的网络安全态势感知模型[J]. 计算机工程,2020,514(6):136 - 141.

[10] Kotenko I, Doynikova E. Selection of countermeasures against network attacks based on dynamical calculation of security metrics[J]. Journal of Defense Modeling and Simulation, 2018, 15(2):181 - 204.

[11] 冯英伟,王庆福,吕国,等. 基于改进证据理论的物联网安全态势评估[J]. 西安理工大学学报,2018,34(4):121 - 127.

[12] 何金栋,王宇,赵志超,等. 智能变电站嵌入式终端的网络攻击类型研究及验证[J]. 中国电力,2020,53(1):81 - 91.

[13] 胡彬,王春东,胡思琦,等. 基于机器学习的移动终端高级持续性威胁检测技术研究[J]. 计算机工程,2017,43(1):241 - 246.

[14] 刘远龙,潘筠,王玮,等. 用于泛在电力物联网的配电变压器智能感知终端技术研究[J]. 电力系统保护与控制,2020,48(16):140 - 146.

[15] 姚琳元,董平,张宏科. 基于对象特征的软件定义网络分布式拒绝服务攻击检测方法[J]. 电子与信息学报,2017,39(2):381 - 388.

(上接第 326 页)

[9] Alkadri N A, Bansarkhani R E, Buchmann J. BLAZE: Practical lattice-based blind signatures for privacy-preserving applications [C]//International Conference on Financial Cryptography and Data Security,2020:484 - 502.

[10] Bouaziz-Ermann S, Canard S, Eberhart G, et al. Lattice-based (partially) blind signature without restart [EB/OL]. [2020 - 12 - 07]. https://eprint.iacr.org/2020/260.

[11] Alkim E, Barreto P, Bindel N, et al. The lattice-based digital signature scheme qTESLA[C]//International Conference on Applied Cryptography and Network Security,2020:441 - 460.

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

[13] Ducas L, Durmus A. Ring-LWE in polynomial rings[C]// International Workshop on Public Key Cryptography,2012:34-51.

[14] Lyubashevsky V. Lattice signatures without trapdoors[C]// 31st Annual International Conference on Theory and Applications of Cryptographic Techniques,2011:738 - 755.

[15] Boneh D, Freeman D M. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures [C]//14th International Conference on Practice and Theory in Public Key Cryptography,2011:1 - 16.

[16] Bellare M, Neven G. Multi-signatures in the plain public-key model and a general forking lemma[C]//13th ACM Conference on Computer and Communications Security,2006:390 - 399.