doi:10.6043/j.issn.0438-0479.201705013

一个基于格的环签名方案的改进

热娜·艾合买提[1,2],张 娟[1],李 伟[1],曾吉文[1,2]*
(1.厦门大学数学科学学院,福建 厦门 361005;2.新疆师范大学数学科学学院,新疆 乌鲁木齐 830054)

摘要:针对 Wang 等提出的基于格中困难问题的环签名方案不满足不可伪造性的问题,提出了一种改进的环签名方案.该方案在随机谕言模型下满足全密钥暴露下的匿名性和内部攻击下的不可伪造性.而且使用一种强陷门生成算法,保证了新的签名方案简单、高效且容易实施.

关键词:环签名;格;不可伪造;强陷门
中图分类号:TP 309 **文献标志码**:A **文章编号**:0438-0479(2018)02-0238-05

2001 年,Rivest 等[1]在群签名的基础上提出了环签名.它是一种特殊的群签名,实现了签名者的完全匿名性,被广泛应用于网上投票、电子选举等领域.截止目前,大部分环签名方案本质上都是基于数学中的困难问题假设[2-4],安全性很大程度上依赖于安全参数的选取[5].并且,基于离散对数问题的签名无法抵抗量子攻击[6].因此,设计更加安全的环签名方案成为密码学发展的一个重要方向.

一个 n 维格是 $\mathbf{R}^n$ 上的离散子群,基于格中困难问题(如最短向量问题等)的密码构造可以抵抗量子攻击.Ajtai 等[5,7-9]证明了某些格中困难问题在一般情况和最坏情况下的困难性相当.因此,在基于格中困难问题的密码体制中,随机挑选实例[5]与最难实例的安全性相同.这个重要性质是大部分传统的密码体制所不具备的.而且,格中涉及的线性运算和模运算相比传统密码的指数运算速度快.

许多人对基于格的环签名方案进行了研究[10-14].2010 年,Cash 等[10]提出了格基派生技术来为用户产生公私钥,并设计了第一个基于格的环签名方案,但是此方案消息扩展较长,不利于实施.2011 年,Wang 等[11]提出一个新的环签名方案,并声称他们的方案可以满足全密钥暴露下的匿名性和内部攻击下的不可伪造性.然而,该方案在内部攻击条件下不满足不可伪造性.本研究改进了 Wang 的方案:新方案在随机谕言模型下,可以满足全密钥暴露下的匿名性和内部攻击下的不可伪造性;并且使用了 Micciancio 等[15]提出的一种新的陷门生成算法.由于这种新的陷门生成算法在计算方面简单、有效、容易实施,因此本研究的签名方案和其他方案相比也更高效.

1 预备知识

本文中系统参数为 n.对任意一个正整数 k,$[k]$ 表示集合$\{1,2,\cdots,k\}$.设矩阵 $\boldsymbol{A}=[\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m]$,其中 $\boldsymbol{a}_i$ 表示矩阵$\boldsymbol{A}$ 的第i 个列向量.$\|\boldsymbol{a}\|$ 表示 $\boldsymbol{a}$ 的欧几里得范数,且 $\|\boldsymbol{a}\|=\max_{x\in[m]}\|\boldsymbol{a}_i\|$.

1.1 格(Lattice)

一个格是 $\mathbf{R}^n$ 的离散子群,它由 $\mathbf{R}^n$ 中 n 个线性无关的向量生成,称其为基向量.设 $\boldsymbol{B}=[\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n]$ 是 $n\times n$ 矩阵,由 n 个线性无关的基(列)向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 组成.那么一个由 $\boldsymbol{B}$ 生成的 n 维格 Λ 定义如下:

$$\Lambda=L(\boldsymbol{B})=\{\boldsymbol{Bc}:\boldsymbol{c}\in\mathbf{Z}^n\},$$

这里 $\boldsymbol{B}$ 就是格 $\Lambda=L(\boldsymbol{B})$ 的一组基,设 $\widetilde{\boldsymbol{B}}$ 表示这组基的 Gram-Schmidt 正交化后的一组基

在密码应用中,通常将格(基底)限制到 $\mathbf{Z}^n$ 上.

本研究使用 q 模格,对 q 模格定义如下:对于一个奇偶校验矩阵 $\boldsymbol{A}\in\mathbf{Z}_q^{n\times m}$,$q$,$m$,$n$ 是一些整数.

收稿日期:2017-05-08 **录用日期**:2017-03-12
基金项目:国家自然科学基金(11261060)
*通信作者:jwzeng@xmu.edu.cn
引文格式:热娜·艾合买提,张娟,李伟,等.一个基于格的环签名方案的改进[J].厦门大学学报(自然科学版),2018,57(2):238-242.
Citation:RE N,ZHANG J,LI W,et al.An improvement of a ring signature scheme based on lattices[J].J Xiamen Univ Nat Sci,2018,57(2):238-242.(in Chinese)

$$\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbf{Z}^m:\boldsymbol{Ae}=\boldsymbol{0} \bmod q\},$$

其中 n 和 q 是正整数,$\boldsymbol{0}\in Z_q^n$ 是一个零向量.下面定义一个 $\Lambda^{\perp}(\boldsymbol{A})$ 的陪集.对于一个校验值 $\boldsymbol{u}\in\mathbf{Z}_q^n$,$\Lambda^{\perp}(\boldsymbol{A})$ 的陪集定义如下:

$$\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbf{Z}^m:\boldsymbol{Ae}=\boldsymbol{u} \bmod q\},$$

也就是 $\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})=\boldsymbol{t}+\Lambda^{\perp}(\boldsymbol{A})$,这里 $\boldsymbol{t}$ 是方程 $\boldsymbol{At}\equiv u \bmod q$ 的任一特解.

对任何 $r>0$,$\mathbf{R}^n$ 上中心在 $\boldsymbol{c}$,偏差为 r 的高斯函数定义如下[8]:

$$\boldsymbol{x}\in\mathbf{R}^n,\rho_{r,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/r^2).$$

对任意 $\boldsymbol{c}\in\mathbf{R}^n$,$r>0$ 及 n 维格 Λ,Λ 上的离散高斯分布定义如下:

$$\boldsymbol{x}\in\Lambda,D_{\Lambda,r,\boldsymbol{c}}=\rho_{r,\boldsymbol{c}}(\boldsymbol{x})/\rho_{r,\boldsymbol{c}}(\Lambda),$$

其中 $\rho_{r,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{r,\boldsymbol{c}}(x)$ 为固定值.

1.2　格中困难问题假设

本研究环签名方案的安全性依赖于格中 SIS 问题(small integer solution problem)、ISIS 问题(inhomogeneous small integer solution problem)的困难性,定义如下[5]:

定义 1　(SIS 问题)设 q 是整数,$\beta(n)$ 是一个关于安全参数 n 的有界函数,矩阵 $\boldsymbol{A}\in\mathbf{Z}_q^{n\times m}$,即元素来自 $\mathbf{Z}_q$ 中的 $n\times m$ 矩阵,其中 $m=\mathrm{poly}(n)$,$\mathrm{SIS}_{q,\beta}$ 问题是寻找一个非零向量 $\boldsymbol{v}\in\mathbf{Z}^m$ 使得 $\boldsymbol{Av}=\boldsymbol{0}$;mod q 成立且满足 $\|\boldsymbol{v}\|\leqslant\beta$.

定义 2　(ISIS 问题)设 q 是整数,$\beta(n)$ 是一个关于安全参数 n 的有界函数,矩阵 $\boldsymbol{A}\in\mathbf{Z}_q^{n\times m}$,其中 $m=\mathrm{poly}(n)$.向量 $\boldsymbol{y}\in\mathbf{Z}_q^n$,$\mathrm{ISIS}_{q,\beta}$ 问题是寻找一个非零向量 $\boldsymbol{v}\in\mathbf{Z}^m$ 使得 $\boldsymbol{Av}=\boldsymbol{y} \bmod q$ 成立且满足 $\|\boldsymbol{v}\|\leqslant\beta$.

1.3　格的基本算法

本文中使用了 Micciancio 等[15]在 2012 年提出的一种新的陷门生成算法:

定义 3　设 $\boldsymbol{A}\in\mathbf{Z}_q^{n\times m}$,$\boldsymbol{G}\in\mathbf{Z}_q^{n\times w}$ 且 $m\geqslant w\geqslant n$,$\boldsymbol{A}$ 的 $\boldsymbol{G}$-陷门是一个矩阵 $\boldsymbol{T}\in\mathbf{Z}_q^{(m-w)\times w}$,满足 $\boldsymbol{A}\begin{bmatrix}\boldsymbol{T}\\ \boldsymbol{I}\end{bmatrix}=\boldsymbol{HG}$,其中 $\boldsymbol{H}\in\mathbf{Z}_q^{n\times n}$ 是一个可逆矩阵,则称 $\boldsymbol{H}$ 是陷门的一个标签.通常,陷门的质量由它的最大奇异值 $s_1(\boldsymbol{T})$ 来测量.其中 $s_1(\boldsymbol{T})=\|\boldsymbol{T}\|$.奇异值越小,陷门质量越好.为了简便起见,通常设 $\boldsymbol{H}=\boldsymbol{I}$.

陷门生成算法 GenTrap$(\bar{\boldsymbol{A}},\boldsymbol{H})$[15]:输出一个均匀随机矩阵 $\boldsymbol{A}\in\mathbf{Z}_q^{n\times m}$ 作为奇偶校验矩阵及其 $\boldsymbol{G}$-陷门 $\boldsymbol{T}\in\mathbf{Z}_q^{(m-w)\times w}$.

引理 1　GenTrap$(\bar{\boldsymbol{A}},\boldsymbol{H})$ 输入一个矩阵 $\bar{\boldsymbol{A}}\in\mathbf{Z}_q^{n\times(m-w)}$,其中 $m-w\geqslant 1$,可逆矩阵 $\boldsymbol{H}\in\mathbf{Z}_q^{n\times n}$ 和某一分布 Ψ,选择一个矩阵 $\boldsymbol{T}\in\mathbf{Z}^{(m-w)\times w}$,$\boldsymbol{T}$ 的每一列向量服从分布 Ψ,然后输出 $\boldsymbol{A}=[\bar{\boldsymbol{A}}\,|\,\boldsymbol{HG}-\bar{\boldsymbol{A}}\boldsymbol{T}]\in\mathbf{Z}_q^{n\times m}$ 以及它对应的陷门 $\boldsymbol{T}\in\mathbf{Z}^{(m-w)\times w}$,且有 $\|\tilde{\boldsymbol{T}}\|\leqslant O(\sqrt{n\log q})$,其中:

1) GenTrap 使用了一个固定的本原矩阵 $\boldsymbol{G}\in\mathbf{Z}_q^{n\times w}$,它的列向量可以生成 $\mathbf{Z}_q^n$.

2) $\boldsymbol{A}$ 的分布与均匀之间的统计距离可忽略.

3) GenTrap$(\bar{\boldsymbol{A}})$指的是 GenTrap$(\bar{\boldsymbol{A}},\boldsymbol{I})$.

定义域中取原像算法 Sample $D(\boldsymbol{A},\boldsymbol{T},\boldsymbol{H},\boldsymbol{u},s)$:在给定函数值时,可以利用陷门信息取样得到较短的原像[15].

引理 2　假设存在一个概率多项式时间算法 Sample $D(\boldsymbol{A},\boldsymbol{T},\boldsymbol{H},\boldsymbol{u},s)$,输入奇偶校验矩阵 $\boldsymbol{A}\in\mathbf{Z}_q^{n\times m}$ 及其 $\boldsymbol{G}$-陷门 $\boldsymbol{T}\in\mathbf{Z}^{(m-w)\times w}$,一个可逆矩阵 $\boldsymbol{H}\in\mathbf{Z}_q^{n\times n}$,校验值 $\boldsymbol{u}\in\mathbf{Z}_q^n$,通过线性方程可求得 $\boldsymbol{At}=\boldsymbol{u} \bmod q$ 的一个特解 $\boldsymbol{t}\in\mathbf{Z}^m$,然后从分布 $D_{\Lambda^{\perp}(\boldsymbol{A}),s,-\boldsymbol{t}}$ 中取样 $\boldsymbol{e}$,输出 $\boldsymbol{v}=\boldsymbol{t}+\boldsymbol{e}$.因此,输出向量 $\boldsymbol{v}$ 满足 $\boldsymbol{Av}\equiv\boldsymbol{u} \bmod q$ 且 $\|\boldsymbol{v}\|\leqslant s\sqrt{m}$.

1) Sample D 使用了一个固定的本原矩阵 $\boldsymbol{G}\in\mathbf{Z}_q^{n\times w}$,它的列向量可以生成 $\mathbf{Z}_q^n$.

2) 向量 $\boldsymbol{v}$ 的分布与 $D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}),s}$ 之间的统计距离可忽略.

3) Sample $D(\boldsymbol{A},\boldsymbol{T},\boldsymbol{u},s)$指的是 Sample $D(\boldsymbol{A},\boldsymbol{T},\boldsymbol{I},\boldsymbol{u},s)$.

陷门派生算法可以由矩阵 $\boldsymbol{A}\in\mathbf{Z}_q^{n\times m}$ 的陷门得到扩充矩阵 $\boldsymbol{A}'\in\mathbf{Z}_q^{n\times(m+m')}$ 的陷门[15].

引理 3　DelTrap$(\boldsymbol{A}',\boldsymbol{A},\boldsymbol{T},\boldsymbol{H}',s')$输入 $\boldsymbol{A}$ 的扩充阵 $\boldsymbol{A}'=[\boldsymbol{A}\,|\,\boldsymbol{A}_1]\in\mathbf{Z}_q^{n\times(m+m')}$ 作为奇偶校验矩阵,$\boldsymbol{A}$ 及其 $\boldsymbol{G}$-陷门 $\boldsymbol{T}$,可逆矩阵 $\boldsymbol{H}'\in\mathbf{Z}_q^{n\times n}$,利用 $\boldsymbol{A}$ 的陷门 $\boldsymbol{T}$ 可以从 $\Lambda^{\perp}(\boldsymbol{A})$ 的适当陪集上独立取样得到 $\boldsymbol{T}'$,使得 $\boldsymbol{AT}'=\boldsymbol{H}'\boldsymbol{G}-\boldsymbol{A}_1$ 成立,其中 $\boldsymbol{T}'$ 的列向量服从离散高斯分布.

1) DelTrap 使用了一个固定的本原阵 $\boldsymbol{G}\in\mathbf{Z}_q^{n\times w}$,它的列向量可以生成 $\mathbf{Z}_q^n$.

2) $\boldsymbol{T}'$的分布与离散高斯分布之间的统计距离可忽略.

3) 随机变换 $\boldsymbol{A}'$的列向量不影响算法的实施.

4) DelTrap$(\boldsymbol{A}',\boldsymbol{A},\boldsymbol{T},s')$指的是 DelTrap$(\boldsymbol{A}',\boldsymbol{A},\boldsymbol{T},\boldsymbol{I},s')$.

2　环签名

2.1　环签名的定义

一个环签名由 3 个概率多项式时间算法[4]构成:

KeyGen,Ringsign,Ringverify.

1) KeyGen(1^n):输入安全参数 n,该算法为每个成员输出签名密钥 sk_i 和验证密钥 vk_i.

2) Ringsign(sk_i,R,M):输入环 R,签名者的私钥 sk_i,消息 $M\in\{0,1\}^*$,该算法输出环 R 对消息 M 的签名 $\boldsymbol{v}$.

3) Ringverify(R,M,$\boldsymbol{v}$):输入环 R,消息 M 及环签名 $\boldsymbol{v}$,如果签名合理,算法回答接受,否则拒绝.

正确性:对所有的 $l\in N$,所有的$\{(vk_i,sk_i)_{i=1}^l\}$及任意的消息 $M\in\{0,1\}^*$,环 R 对消息 M 的签名是 $\boldsymbol{v}$,满足 Ringverify(R,M,Ringsign(sk_i,R,M))=1,则环签名方案正确.

2.2 环签名方案的匿名性

一般的环签名方案抗全密钥暴露下的匿名性证明定义如下:

假设攻击者 A 攻击环签名方案在全密钥暴露下的匿名性,挑战者 C 来响应 A 的攻击环境.通过挑战响应模式来进行如下游戏:C 运行 KeyGen 算法 l 次生成公私钥对$\{(vk_i,sk_i)_{i=1}^l\}$,其中 l 是游戏的参数.C 将公钥发送给 A,允许它进行私钥询问、签名询问.私钥询问的形式是一个指数 i,挑战者 C 将其私钥 sk_i 返回给 A.环签名询问的形式是(i.R,M),表示询问环 R 中成员 i 对消息 M 的签名,挑战者 C 执行算法 $\boldsymbol{v}\leftarrow$ Ring-sign(sk_i,R,M),将 $\boldsymbol{v}$ 返回给 A.最终 A 发出挑战(i_0,i_1,R^*,M^*)给 C,表示环 R^* 对消息 M^* 签名,i_0,i_1是 R^* 中的两个成员.C 选择 $b^*\leftarrow\{0,1\}$,C 执行算法得到 $\boldsymbol{v}^*\leftarrow$ Ringsign(sk_{ib^*},R^*,M^*),将 $\boldsymbol{v}^*$ 给 A,最终 A 输出它的猜测 $b'\leftarrow\{0,1\}$.如果 $b'=b^*$,则 A 赢得这个游戏.

用$\mathrm{Adv}_{RS,l}^{\mathrm{anno}}(\mathrm{A})$表示 A 以大于 1/2 的概率赢得这个游戏,即

$$\mathrm{Adv}_{RS,l}^{\mathrm{anno}}(\mathrm{A})=|\Pr(\mathrm{A}-\mathrm{win})-1/2|.$$

如果 $\mathrm{Adv}_{RS,l}^{\mathrm{anno}}(\mathrm{A})$是可忽略的,则环签名方案是匿名的.

2.3 环签名方案的不可伪造性

一般的环签名方案在内部攻击下不可伪造证明定义如下:

敌手 A 对环签名方案内部攻击下的不可伪造性,挑战者 C 响应 A 的攻击环境.通过挑战响应模式来进行如下游戏.C 运行 KeyGen 算法 l 次,生成公私钥对$\{(vk_i,sk_i)_{i=1}^l\}$,其中 l 是游戏的参数.C 将公钥发送给 A,允许它进行私钥询问、签名询问.询问形式同匿名性定义.最终 A 输出伪造签名(R^*,M^*,$\boldsymbol{v}^*$),如果 R^* 中的成员都没有被询问过私钥,(R^*,M^*)没有进行过签名询问且 Ringverify(R^*,M^*,$\boldsymbol{v}^*$)=1,Accept,则 A 赢得这个游戏.

A 在上述游戏中取胜的优势定义如下:

$$\mathrm{Adv}_{RS,l}^{\mathrm{unfor}}(\mathrm{A})=\Pr(\mathrm{A}-\mathrm{win}),$$

如果$\mathrm{Adv}_{RS,l}^{\mathrm{unfor}}(\mathrm{A})$是可忽略的,那么环签名方案是不可伪造的.

3 本研究提出的方案

设 n 是一个安全参数,β 是 SIS 问题中短向量的上界.$\boldsymbol{G}\in\mathbf{Z}_q^{n\times w}$是一个本原矩阵,即它的列可以张成整个 $\mathbf{Z}_q^n$.Params=$\{\boldsymbol{G},\bar{\boldsymbol{A}},\boldsymbol{u},\boldsymbol{H}(\cdot,\cdot)\}$是公开的参数,其中

$$\bar{\boldsymbol{A}}\leftarrow\mathbf{Z}_q^{n\times(m-w)},\boldsymbol{u}\leftarrow\mathbf{Z}_q^l,$$

$$\boldsymbol{H}(\cdot,\cdot):\{0,1\}^*\times\{0,1\}^m\rightarrow\{0,1\}^n.$$

是一个安全的 Bash 函数.安全性分析时将视 $H(\cdot,\cdot)$为一个随机器.为了方便起见,令其中的可逆矩阵 $\boldsymbol{H}=\boldsymbol{I}$.

1) KeyGen(1^n):输入安全参数 n,可信中心运行陷门生成算法 GenTrap($\bar{\boldsymbol{A}}$),为每个用户 i 选择一个随机矩阵 $\boldsymbol{T}_i\in\mathbf{Z}^{(m-w)\times w}$,它的列向量服从分布 Ψ,计算 $\boldsymbol{A}_i=[\bar{\boldsymbol{A}}\,|\,\boldsymbol{HG}-\bar{\boldsymbol{A}}\boldsymbol{T}_i]\in\mathbf{Z}_q^{n\times m}$,得到验证密钥 $vk_i=\boldsymbol{A}_i$ 及相应的签名密钥 $sk_i=\boldsymbol{T}_i$,($i=1,2,\cdots,L$).

2) Ringsign(i,R,M):设 $R=\{1,2,\cdots,L\}$表示环成员的集合,每个成员 i 的公钥 $\boldsymbol{A}_i\in\mathbf{Z}_q^{n\times m}$,下面用户 i 做如下工作对消息 $M\in\{0,1\}^*$进行签名.

(i) 设 $\boldsymbol{A}_R=[\boldsymbol{A}_1\,\|\,\boldsymbol{A}_2\,\|\cdots\boldsymbol{A}_L]\in\mathbf{Z}_q^{n\times Lm}$,$\boldsymbol{y}=H(R,M)\bmod q\in\mathbf{Z}_q^n$.

(ii) 利用算法 DelTrap($\boldsymbol{A}_R$,$\boldsymbol{A}_i$,$\boldsymbol{T}_i$,s') 派生出 $\boldsymbol{A}_R$的陷门 $\boldsymbol{T}_R$.

(iii) 利用算法 Sample $D(\boldsymbol{A}_R,\boldsymbol{T}_R,\boldsymbol{y})$ 取样得到 $\boldsymbol{v}\in\mathbf{Z}^{Lm}$,显然满足 $\boldsymbol{A}_R\boldsymbol{v}=\boldsymbol{y}\bmod q$.

(iv) 最后输出用户 i 对消息 M 的签名 $\boldsymbol{v}$.

3) Ringverify(R,$\boldsymbol{v}$,M):给定一个环 R,消息 M,签名 $\boldsymbol{v}$,当下述两个条件满足时,验证者接受这个签名:

(i) $0\leqslant\|\boldsymbol{v}\|\leqslant r\sqrt{Lm}$;

(ii) $\boldsymbol{A}_R\boldsymbol{v}=\boldsymbol{H}(R,M)\bmod q$.

否则,验证者不接受.

正确性:环签名 $\boldsymbol{v}$ 的分布与 $D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}_R),s}$ 统计距离可以忽略,满足 $\boldsymbol{A}_R\boldsymbol{v}=\boldsymbol{H}(R,M)\bmod q$ 且 $\|\boldsymbol{v}\|\leqslant r\sqrt{Lm}$ 以压倒性的概率成立.因此本研究的环签名方

案是正确的.

3.1　全密钥暴露下的匿名性

定理 1　若将 $\boldsymbol{H}(\cdot,\cdot)$视为一个随机谕言模型,假设 $\mathrm{ISIS}_{q,lm}$是困难的,则本研究的环签名方案在全密钥暴露下是匿名的.

证明　假设存在一个自适应的敌手 A 攻击环签名方案在全密钥暴露下的匿名性,挑战者构造一个多项式时间算法 C 来响应 A 的攻击环境.设 A 的询问次数是 q_E.为了响应 A 的询问,存储两个列表 $\boldsymbol{H}$ 和 $\boldsymbol{K}$,他们在初始状态下都是空的.

1) setup 阶段:C 运行算法 GenTrap q_E 次,生成 $A_i\in\mathbf{Z}_q^{n\times m}$及相应的私钥 $\boldsymbol{T}_i\in\mathbf{Z}^{(m-w)\times w}$,其中 $1\leqslant i\leqslant q_E$.$C$ 将三元组$\langle i,\boldsymbol{A}_i,\boldsymbol{T}_i\rangle$存储在列表 $\boldsymbol{K}$ 中,记 $R=\{1,2,\cdots,q_E\}$,是这 q_E 个成员组成的环.C 将环 R 的公钥集合$\langle\boldsymbol{A}_1\parallel\boldsymbol{A}_2\parallel\cdots\boldsymbol{A}_{q_E}\rangle$发送给 A.

2) 询问阶段:C 分别回答 A 的 hash 询问、私钥询问及签名询问如下:其中 R_i表示环 R 的含有 l 个成员的任一子环,M_j 为任一消息.

(i) 对 $\boldsymbol{H}(R_i,M_j)$的 Hash 询问:C 返回一个随机值 $\boldsymbol{y}_{ij}\in\mathbf{Z}_q^n$给 A,然后将$\langle R_i,M_j,\boldsymbol{y}_{ij}\rangle$存入列表 $\boldsymbol{H}$;

(ii) R_i中用户 i_1的私钥询问阶段:C 查找列表$\boldsymbol{K}$,返回 $\boldsymbol{T}_{i1}$给 A.

(iii) 询问环 R_i 中的成员 i_1 对消息 M_j 的签名$\langle i_1,R_i,M_j\rangle$:可以假设 $\boldsymbol{H}(R_i,M_j)$已经被 A 询问过了,C 查询 $\boldsymbol{H}$ 列表$\langle R_i,M_j,\boldsymbol{y}_{ij}\rangle$得到 $\boldsymbol{y}_{ij}$,执行算法 Sample D 得到$\boldsymbol{v}_{ij}$,并将 $\boldsymbol{v}_{ij}$返回给 A.

A 发出挑战$\langle k_0,k_1,R^*,M^*\rangle$,使环 R^*对消息 M^*签名,k_0,k_1 是 R^*中的两个成员.C 选择$b^*\leftarrow\{0,1\}$,检查列表 $\boldsymbol{H}$ 中元组$\langle R^*,M^*,\boldsymbol{y}^*\rangle$,运行算法 DelTrap 得到$\boldsymbol{A}_{R^*}$的陷门 $\boldsymbol{T}_{R^*}$,然后计算挑战签名 $\boldsymbol{v}^*\leftarrow$Sample $D(\boldsymbol{A}_{R^*},\boldsymbol{T}_{R^*},\boldsymbol{y}^*)$,将 $\boldsymbol{v}^*$给 A,最终 A 输出它的猜测$b'\leftarrow\{0,1\}$.

从上述的模拟过程容易得出 v_{k0} 和 v_{k1} 分布与 $D_{\Lambda_{\boldsymbol{y}}^{\perp}(\boldsymbol{A}R),s}$统计距离都可以忽略,因此两者之间统计距离也可忽略,也就是 A 猜测两者的概率相同,即猜测的优势是可忽略的.所以本研究的环签名方案在全密钥暴露下是匿名的.

3.2　内部攻击下的不可伪造性

定理 2　若将 $\boldsymbol{H}(\cdot,\cdot)$视为一个随机谕言模型,假设 $\mathrm{SIS}_{q,lm}$是困难的,则本研究的环签名方案在内部攻击下是安全的.

证明　假设存在一个自适应的敌手 A 攻击环签名方案内部攻击下的不可伪造性,挑战者构造一个多项式时间算法 C 来模拟 A 的攻击环境,解决 SIS 问题.设询问次数是 q_E,A 和 C 进行如下游戏.为了响应 A 的询问,C 存储两个列表 $\boldsymbol{H}$ 和 $\boldsymbol{K}$,他们在初始状态下都是空的.

1) setup 阶段:C 选择 $l\in[q_E]$,l 是猜测的挑战环中成员个数.C 获取一个 SIS 实例 $\boldsymbol{A}_{R_t}\in\mathbf{Z}_q^{n\times lm}$,将这个 $n\times lm$ 矩阵分块为 l 个 $n\times m$ 矩阵.记为 $\boldsymbol{A}_{R_t}=[\boldsymbol{A}_{1*}\boldsymbol{A}_{2*}\cdots\boldsymbol{A}_{l*}]$,其中 $\boldsymbol{A}_{ist}\in\mathbf{Z}_q^{n\times m}$.$C$ 随机挑选 $t_i\in[q_E]$,$i\in\{1,2,\cdots,l\}$,记 $R_t=\{t_1,t_2,\cdots,t_l\}$,然后将 SIS 实例 $\boldsymbol{A}_{R_t}$的每个子块$\boldsymbol{A}_{i*}$分别作为 R_t 中每个成员的公钥,即 $\boldsymbol{A}_{ti}=\boldsymbol{A}_{i*}$,对$[q_E]$中除 R_t之外的其他成员(q_E-l 个),C 运行算法 GenTrap 为它们生成公钥 $\boldsymbol{A}_i\in\mathbf{Z}_q^{n\times m}$及相应的私钥 $\boldsymbol{T}_i\in\mathbf{Z}^{(m-w)\times w}$,然后将$\langle i,\boldsymbol{A}_i,\boldsymbol{T}_i\rangle$存储在列表 K 中,记 $R=\{1,2,\cdots,q_E\}$,是这 q_E个成员组成的环.C 将环 R 的公钥集合$\langle\boldsymbol{A}_1\parallel\boldsymbol{A}_2\parallel\cdots\boldsymbol{A}_{q_E}\rangle$发送给 $\boldsymbol{A}$.

2) 询问阶段:C 分别回答 A 的 Hash 询问、私钥询问及签名询问如下:其中 R_i表示环 R 的含有 l 个成员的任一子环,M_j 为任一消息.

(i) 对 $\boldsymbol{H}(R_i,M_j)$的 Hash 询问:C 返回一个随机值 $e_{ij}\leftarrow\mathbf{Z}^{lm}$,服从高斯分布 $D_{\mathbf{Z}^{lm},r}$,返回 $\boldsymbol{y}_{ij}\leftarrow\boldsymbol{A}_{R_t}e_{ij}\bmod q$ 给 A,然后将$(R_i,M_j,e_{ij},\boldsymbol{y}_{ij})$存储在列表中 $\boldsymbol{H}$.

(ii) 对 k 私钥询问:如果 $k\notin R_t$,C 在列表 K 中寻找$\langle k,\boldsymbol{A}_k,\boldsymbol{T}_k\rangle$,然后将 $\boldsymbol{T}_k$ 返回给 A.否则中止.

(iii)询问环 R_i 中的成员 i_1 对消息 M_j 的签名$\langle i_1,R_i,M_j\rangle$:可以假设 $\boldsymbol{H}(R_i,M_j)$已经被 A 询问,如果 $R_i=R_t$,C 查找列表$\boldsymbol{H}(R_i,M_j,e_{ij},\boldsymbol{y}_{ij})$,将 e_{ij}返回给 A.若 $R_i\neq R_t$,分两种情况:

情况 1:$i_1\in R_i-R_t$,此时$\langle i_1,\boldsymbol{A}_{i1},\boldsymbol{T}_{i1}\rangle$包含在列表 $\boldsymbol{K}$ 中,那么 C 运行 DelTrap 算法获得 $\boldsymbol{A}_{R_i}$的陷门$\boldsymbol{T}_{R_i}\leftarrow\mathrm{DelTrap}(\boldsymbol{A}_{R_i},\boldsymbol{A}_{i1},\boldsymbol{T}_{i1})$,检查 $\boldsymbol{H}$ 列表中的$(R_i,M_j,e_{ij},\boldsymbol{y}_{ij})$,计算挑战签名 $\boldsymbol{v}_{ij}\leftarrow\mathrm{Sample}\ D(\boldsymbol{A}_{R_i},\boldsymbol{T}_{R_i},\boldsymbol{y}_{ij})$,并将 $\boldsymbol{v}_{ij}$返回给 A.

情况 2:$i_1\in R_i\cap R_t$,C 寻找一个 $i_2\in R_i-R_t$,使得$\langle i_2,\boldsymbol{A}_{i2},\boldsymbol{T}_{i2}\rangle$包含在列表 $\boldsymbol{K}$ 中,运行 DelTrap 算法获得 $\boldsymbol{A}_{R_i}$的陷门$\boldsymbol{T}_{R_i}\leftarrow\mathrm{DelTrap}(\boldsymbol{A}_{R_i},\boldsymbol{A}_{i2},\boldsymbol{T}_{i2})$,$C$ 重新在列表 $\boldsymbol{H}$ 中获得$(R_i,M_j,e_{ij},\boldsymbol{y}_{ij})$,然后计算挑战签名 $\boldsymbol{v}_{ij}\leftarrow\mathrm{Sample}\ D(\boldsymbol{A}_{R_i},\boldsymbol{T}_{R_i},\boldsymbol{y}_{ij})$ 并将 $\boldsymbol{v}_{ij}$返回给 A.

3) 挑战阶段,A 输出一个伪造$\langle i^*,R^*,M^*,\boldsymbol{\sigma}^*\rangle$,如果 $R^*\neq R_t$,C 失败,否则 C 寻找列表 H 中的$\langle R^*,M^*,\boldsymbol{e}^*,\boldsymbol{y}^*\rangle$,然后输出 $\boldsymbol{v}=\boldsymbol{\sigma}^*-\boldsymbol{e}^*$,即为 SIS 问题实例 $f_{A_{Rt}}$的解.

分析:设敌手 A 输出一个合理的伪造的概率是

ε,挑战者 C 成功解决 SIS 问题实例主要取决于私钥询问阶段和挑战阶段.

(i)在私钥询问阶段,R 中有 l 个成员的私钥是未知的,被询问到的概率为 $1/q_E$,因此询问成功即 $i \notin R_t$,C 询问成功的概率是 $1-1/q_E$.

(ii)在挑战阶段,$R^* = R_t$,的概率为 $1/C_{q_E}^l$.其中 $C_{q_E}^l$ 为组合数.

因此,挑战者 C 成功解决 SIS 问题的概率至少为 $\varepsilon(1-1/q_E)/C_{q_E}^l$.

4 结 论

本文中提出的新的环签名方案在随机谕言模型下是可以满足全密钥暴露下的匿名性和内部攻击下的不可伪造性.而且使用一种强陷门生成算法,保证了新的签名方案简单、高效且容易实施.

参考文献:

[1] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a sercret[C]// Proceedings of the ASIACRYPT 2001. Berlin: Springer-Verlag, 2001: 552-565.

[2] ZENG S, JIANG S, QIN Z. An efficient conditionally anonymous ring signature in the random oracle model [J]. Theoretical Computer Science, 2012, 461: 106-114.

[3] SHIM K A. An efficient ring signature scheme from pai-rings[J]. Information Sciences, 2015, 300: 63-69.

[4] BENDER A, KATZ J, MORSELLI R. Ring signatures: stronger definitions, and construction without random oracles[J]. Journal of Cryptology, 2009, 22(1): 114-138.

[5] AJTAI M. Generating hard instances of lattice problems (extended abstract)[C]// STOC. Philadelphia: ACM, 1996: 99-108

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

[7] DWORK C. A public-key cryptosystem with worst-case and/average-case equivalence[C]// Proceeding of Twenty-ninth ACM Symposium on Theory of Computing. [S. l.]: ACM, 1997: 284-293.

[8] MICCIANCIO D, ROSEN O. Worst-case to average-case reductions based on Gaussian measures[J]. SIAM Journal on Computing, 2007, 37: 267-302.

[9] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48 (3): 535-553.

[10] CASH D, HOFHEINZ D, KILTZ D, et al. Bonsai trees, or how to delegate a lattices basis[J]. Eurocrypt, 2010, 6110: 523-552.

[11] WANG J, SUN B. Ring signature schemes from lattice basis delegation[J]. Lecture Notes in Computer Science, 2011, 7043: 15-28.

[12] NOH G, CHUNJ Y, JEONG I R. Strongly unforgeable ring signature scheme from lattices in the standard model[J]. Journal of Applied Mathematics, 2014(2014): 1-12.

[13] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]// Proceedings of the 40th Annual ACM Symposium on the Theory of computing (STOC′08). [S.l.]: ACM, 2008: 197-206.

[14] MELCHOR C A, BETTAIEB S, BOYEN X, et al. Adapting Lyubashevsky′s signature schemes to ring signature setting[J]. Progress in Cryptology, 2013, 7918: 1-25.

[15] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[J]. Lecture Notes in Computer Science, 2012, 7237: 700-718.

An Improvement of a Ring Signature Scheme Based on Lattices

RENA Ehmet[1,2], ZHANG Juan[1], LI Wei[1], ZENG Jiwen[1,2]*

(1. School of Mathematical Sciences, Xiamen University, Xiamen 361005, China;
2. Scool of Mathematical Sciences, Xinjiang Normal University, Urumqi 830054, China)

Abstract: Wang has proposed a ring signature scheme based on difficult problem in lattices, but it does not satisfy unforgeability against insider corruption. Hereby we present a ring signature scheme which is anonymous against full key exposure and unforgeable against insider corruption in the random oracle model. In our new signature schemes, we use strong trapdoor generation algorithms. Consequently, it is simple and efficient for proposed algorithms to be implemented.

Key words: ring signature; lattice; unforgeability; strong trapdoor