计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20160427
54(7):1510-1524,2017

基于格的前向安全无证书数字签名方案

徐 潜 谭成翔 冯 俊 樊志杰 朱文烨
(同济大学电子与信息工程学院计算机科学与技术系 上海 201804)
(1062842783@qq.com)

Lattice-Based Forward Secure and Certificateless Signature Scheme

Xu Qian, Tan Chengxiang, Feng Jun, Fan Zhijie, and Zhu Wenye
(*Department of Computer Science and Technology, College of Electronics and Information Engineering, Tongji University, Shanghai* 201804)

Abstract Certificateless signature scheme has solved key escrow problems existing in traditional identity-based signature schemes. The secret key of the user in certificateless signature scheme consists of two parts, one is partial secret key, which is generated by key generation centre, and the other is secret value from user itself. However, there are still three points to be improved in such scheme. Firstly, although some lattice-based certificateless signature schemes based on the random oracle model have been proposed in order to achieve the post-quantum security, their standard model counterparts remain unrealized. Secondly, most of the existing lattice-based certificateless signature schemes only consider the outside attacker and neglect the threats from semi-trusted user. Thirdly, the existing certificateless signature schemes all rely on the security of the secret key, which cannot be satisfied due to the key exposure problem. In this paper, based on the forward secure and certificateless signature scheme in the random oracle model, we propose the first lattice-based certificateless signature scheme which is provably secure in the standard model to eliminate key exposure and key escrow problems without introducing a third party proxy. With the help of the small integer solution problem, we have proved that our schemes can guarantee the forward secure and strongly existential unforgeability against the adaptive chosen message and adaptive chosen identity attack.

Key words lattice-based signature scheme; certificateless; forward secure; random oracle model; standard model

摘 要 无证书签名方案利用密钥生成中心与用户共同生成签名密钥的方式,解决了传统的基于身份的数字签名方案中存在的密钥托管问题.目前,针对无证书签名方案的研究还存在3点可以改进的地方:1)已有的基于随机格构建的无证书签名方案,虽然具有后量子安全性,但都是建立在随机预言模型下,尚无针对标准模型的相关研究;2)已有的格基无证书签名方案大多只考虑外部敌手,缺乏抵御不诚实用户攻击的能力;3)已有的无证书签名方案均需要保证用户密钥是绝对安全的,无法解决密钥泄露问题.针对这3点不足,在随机预言模型下的前向安全的无证书格基签名方案的基础上,首次提出了标准模型下可证明安全的基于随机格的前向安全无证书数字签名方案,并在不引入第三方代理的前提下同时解

收稿日期:2016-06-13;**修回日期**:2016-08-23
基金项目:国家重点研发计划项目(2017YFB0802302)
This work was supported by the National Key Research and Development Program of China (2017YFB0802302)
通信作者:谭成翔(jerrytan@tongji.edu.cn)

决了密钥泄露和密钥托管问题.在面对不诚实的用户和恶意密钥生成中心2类强敌手的情况下,利用小整数解SIS假设证明了所提出的方案具有适应性选择消息、选择身份攻击下的前向安全强不可伪造性.

关键词　格基数字签名;无证书;前向安全;随机预言模型;标准模型

中图法分类号　TP309

传统的基于公钥基础设施(public key infrastructure, PKI)的公钥密码系统通过引入证书管理机构CA为用户颁发数字证书,并鉴权用户身份.然而,证书的更新、撤销等管理操作给系统带来较大的运行负荷.为了消除证书管理带来的昂贵开销,Shamir[1]于1984年提出了身份基加密的思想,利用用户唯一的公共标识ID作为用户的公钥,由密钥生成器(private key generator, PKG)为用户生成密钥.目前已有很多高效的身份基签名方案[2-5],如Yao等人[2]利用拉格朗日插值公式,在随机格的基础上构建了允许模糊身份验证的身份基签名方案.以及Wei等人[3]提出的门限身份基签名方案等.然而,由于用户密钥完全由PKG生成,对PKG可见,一旦PKG受到污染,整个系统中的用户都将不再安全,这就产生了密钥托管问题(key escrow).

Al-Riyami等人[6]在2003年首次定义了无证书公钥密码学的概念,用来解决密钥托管问题并消除证书管理的开销.无证书密码学的核心思想为:密钥生成中心(key generation centre, KGC)为用户派发部分密钥,用户自己负责剩余密钥,即私密值的生成,用户完整的签名密钥由部分密钥和私密值共同组成.由于KGC无法获取用户的私密值,也就无法知晓用户的完整密钥,从而消除了恶意KGC带来的安全隐患,解决了密钥托管问题.无证书密钥方案可以用于移动环境下用户敏感数据的保护或者高效的授权认证等领域.

基于Al-Riyami的思想,很多无证书数字签名方案被陆续提出[7-15].这些方案的安全性都是基于传统数论难题,如离散对数和大整数分解等.然而随着量子计算机的发展,基于传统数论难题的密码方案的安全性受到了挑战.事实上,早在1997年,Shor[16]就提出了多项式时间内解决离散对数和大整数素分解的量子算法.因此,构建能够抵御量子攻击的后量子安全的无证书签名方案就具有十分重要的意义.为此,Kim等人[17]和Tian等人[18]设计了基于格的无证书签名方案,并通过小整数解(short integer solution, SIS)问题证明了方案的安全性.但是他们的方案以及安全证明都是基于随机预言模型,在实际应用中,很难保证诸如Hash函数等对象可以按照在随机预言证明中所假设的那样,实现完全的随机化,从而难以保证系统的实际安全性[19].同时,他们的方案只考虑外部敌手,忽视了来自于内部不诚实签名用户的威胁.

更进一步地,在移动环境下特别是随着手机等移动端的大量使用,由于用户的不安全行为,一旦移动设备被攻击,存储在设备中的用户签名密钥将很容易被窃取,即存在密钥泄露问题.目前后量子安全的无证书签名方案[17-18]等均假设用户密钥是绝对安全的,缺乏有效解决密钥泄露问题的能力.同时,基于传统数论难题的无证书签名方案虽然考虑了密钥泄露问题,但主要通过引入第三方代理来更新用户密钥,不仅增加了系统的复杂度,而且,由于第三方代理的安全性无法保证,系统的安全隐患也随之增加.

综上所述,目前无证书签名方案存在3个问题:

1) 已有基于格的后量子安全的无证书签名方案仅仅基于随机预言模型,无法保证实际应用中的系统安全性;

2) 已有无证书签名方案的安全证明主要考虑外部敌手和恶意密钥生成中心,而对来自于不诚实的签名用户的威胁抵抗能力不足;

3) 目前无证书签名方案还无法在不引入第三方代理的前提下解决密钥泄露问题.

针对这3个主要问题,本文利用格基委派技术,基于随机格理论,首先在随机预言模型下引入了前向安全的无证书数字签名方案RO_LFC_SIG,并在此基础上,设计了第1个标准模型下可证安全的前向安全无证书ST_LFC_SIG方案.

本文的主要贡献有4个方面:

1) 针对不诚实的用户和内部恶意KGC攻击者,首次形式化定义了前向安全强不可伪造性的安全模型.与文献[8,18,20-21]中的安全模型相比,不仅增加了针对密钥泄露的前向安全性部分,而且将外部敌手增强为不诚实的签名用户,使得方案安全性更高.

2) 首次具体实现了基于格的前向安全无证书

签名方案,将前向安全与无证书方案基于随机格结合,在不引入第三方代理的条件下同时解决密钥泄露和密钥托管问题,且具有后量子安全性.

3) 提出的 ST_LFC_SIG 无证书签名方案不仅具有前向安全性,也是首个在标准模型下可证安全的格基无证书签名方案,与文献[17-18]中的格基签名方案相比,安全性更高.

4) 分别在随机预言模型和标准模型下,利用随机格的小整数解 SIS 难题,证明了提出的 2 个签名方案在面对 2 类强敌手时,具有适应性选择消息、选择身份攻击的前向安全强不可伪造性(forward secure and strongly existentially unforgeable against adaptive chosen message and adaptive chosen identity attack, FSU-AMAIA);通过与已有的格基签名方案和无证书签名方案进行安全性和效率的对比,证明本文方案在保证较低的渐近性复杂度的同时,达到了更好的安全性.

1 相关工作

无证书数字签名方案的研究目前已有很多,例如 Yu 等人[7]就是利用双线性对构造了无证书签名方案;Guan 等人[8]通过应用公钥替换攻击证明了 Yu 等人[7]方案并不是存在不可伪造的;Yeh 等人[9]通过椭圆曲线设计了无证书签名方案,但是只考虑了第三方敌手的攻击;陈虎等人[10]将无证书签名与群签名结合,基于双线性对设计了高效的无证书群签名方案,实现了群成员的动态更新;Choi 等人[12]基于计算性 Diffie-Hellman 假设(computational Diffie-Hellamn, CDH)构造了高效的无证书签名方案,但主要实现了存在不可伪造性而非强不可伪造;Huang 等人[13]构造了能够抵御 2 类强敌手的无证书签名方案,并基于提出的签名方案设计了身份鉴权协议;Tso 等人[14]基于 CDH 假设并针对公钥替换攻击问题设计了强不可伪造的无证书签名方案;同样基于 CDH 假设的还有 Chen 等人[15]的方案.以上的无证书签名方案[7-15]都是基于传统数论难题的,不具备后量子安全性;Kim 等人[17]和 Tian 等人[18]设计了基于格的随机预言模型下可证安全的无证书签名方案,并通过小整数解 SIS 问题证明了方案的存在不可伪造性;文献[17-18]的方案实现了后量子安全的无证书签名方案,但是随机预言模型无法保证方案的实际安全性,其安全证明也只考虑了外部敌手,没有针对不诚实用户的安全性分析.同时,文献[17-18]的签名方案依赖于绝对安全的用户密钥,因此存在密钥泄露问题.

解决密钥泄露问题的一种有效的方法是构建前向安全的公钥密码系统.针对密钥泄露的前向安全性是指,某一个时刻用户密钥的泄露不会危及之前任意时刻的方案的安全性.在前向安全的数字签名研究方面,目前采用的主要思想是构建不可逆的密钥更新算法.已有很多前向安全的签名方案[22-25],例如 Yu 等人[22]的方案;Ebri 等人[23]赋予用户指定密钥更新时间的能力;文献[24]则将前向安全与门限签名相结合,利用周期性密钥更新和群组门限同时保证密钥的安全性;文献[25]中利用时间序列树等实现了前向安全的细粒度属性控制.但同很多无证书密码方案一样,这些前向安全的签名方案仍然是基于双线性对等数学难题,不具有抗量子计算攻击的能力;Zhang 等人[20]设计了首个基于格的前向安全的签名方案 FSIBS,其主要的思路是建立在 Rückert[26]的分层的身份基签名方案的基础上,利用格基委派算法实现密钥的前向更新;然而同文献[17-18]中的方案一样,Zhang 等人[20]的方案也仅仅实现了随机预言模型下的证明;而且 Zhang 等人[20]的方案只考虑了外部敌手,不具备抵抗恶意 KGC 攻击的能力,安全模型也仅考虑了存在不可伪造性而缺乏针对前向安全性的形式化定义;Li 等人[27]仍然基于双线性对考虑了前向安全与无证书方案的结合问题,没有给出安全模型的形式化定义,而且文献[27]通过引入第三方代理实现前向安全性,增加了方案复杂度,也没有证明当第三方代理受到攻击时方案的可靠性.

2 预备知识

标识与记号:设 q 为正素数,$\mathbb{Z}_q$ 表示$[-\frac{q-1}{2},\frac{q-1}{2}]$范围内的整数.$\|\boldsymbol{v}\|$表示向量 $\boldsymbol{v}$ 的 l_2 范数.本文中使用标准的 O 记号表示函数的复杂度上界,即 $g(n)=O(f(n))$当且仅当存在正常数 c 和 n_0,使得对任意的 $n\geqslant n_0$ 有 $|g(n)|\leqslant c|f(n)|$成立.相应地,定义下界复杂度记号 ω,即 $g(n)=\omega(f(n))$当且仅当存在正常数 c 和 n_0,使得对任意的 $n\geqslant n_0$ 有 $|g(n)|\geqslant c|f(n)|$成立.定义关于 n 的可忽略函数 $negl(n)$,使得对任意多项式 $g(n)$,当 n 足够大时都有 $negl(n)\leqslant\frac{1}{g(n)}$.如果概率 $p=1-negl(n)$则称概

率是压倒性成立的,若 $p=negl(n)$,则称概率是可忽略的.

定义 1. 小整数解问题 SIS[28]:给定一个正整数 q,随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,实数 β,定义(q,m,β)上的 SIS 问题 $\mathcal{P}_{\mathrm{SIS}}(q,m,\beta)$是:找到非 0 向量 $\boldsymbol{v}\in\mathbb{Z}^m$,使得 $\boldsymbol{Av}=0 \bmod q$ 并且 $\|\boldsymbol{v}\|\leqslant\beta$. Micciancio 等人[29]已经证明,对任意多项式有界的 $m,\beta,q\geqslant\beta\omega(\sqrt{n\lg n})$,平均情况下的 $\mathcal{P}_{\mathrm{SIS}}(q,m,\beta)$问题与解决最坏情况下格上的近似独立向量问题是同等困难的.

引理 1[28]. 设 D_σ^m 表示参数为 σ 且中心为 0 的离散正态分布,向量 $\boldsymbol{x}\leftarrow D_\sigma^m$,则 $\|\boldsymbol{x}\|\leqslant 2\sigma\sqrt{m}$ 以压倒性概率成立. α 为正实数,$\boldsymbol{v}\in\mathbb{Z}^m$,如果 $\sigma=\alpha\|\boldsymbol{v}\|$,则 $Pr[\boldsymbol{x}\leftarrow D_\sigma^m:D_\sigma^m(\boldsymbol{x})/D_{\sigma,\boldsymbol{v}}^m(\boldsymbol{x})<\mathrm{e}^{12/\alpha+1/2\alpha^2}]>1-2^{-100}$,其中 D_σ^m 的概率密度为 $\rho_{\sigma,\boldsymbol{c}}^m(\boldsymbol{x})=(2\pi\sigma^2)^{-m/2}\mathrm{e}^{-(\|\boldsymbol{x}-\boldsymbol{c}\|^2/2\sigma^2)}$.

引理 2[28]. 无抽样技术:若签名人从某个随机分布中抽取 $\boldsymbol{y}$,签名的目标分布为 $f(\boldsymbol{x})$,与签名人私钥 sk 无关,实际分布为 $g(\boldsymbol{x})$,可能与 sk 有关,且对于任意 $\boldsymbol{x}$ 及某个正实数 M 有 $f(\boldsymbol{x})\leqslant Mg(\boldsymbol{x})$. 则以概率 $f(\boldsymbol{y})/Mg(\boldsymbol{y})$输出签名 $\boldsymbol{y}$ 将使得 $\boldsymbol{y}$ 服从分布 $f(\boldsymbol{x})$.

由引理 1,若设 $M=\mathrm{e}^{12/\alpha+1/2\alpha^2}$,以 $\min(1,D_\sigma^m(\boldsymbol{y})/MD_{\sigma,\boldsymbol{v}}^m(\boldsymbol{y}))$输出签名 $\boldsymbol{y}$,则 $\boldsymbol{y}$ 服从于分布 D_σ^m 且以压倒性的概率满足 $\|\boldsymbol{y}\|\leqslant 2\sigma\sqrt{m}$.

引理 3. 陷门生成算法[30]:设 $q\geqslant 3$,$m\geqslant 5n\lg q$,存在有效的多项式时间算法 $TrapGen$ 在多项式时间内生成统计接近于 $\mathbb{Z}_q^{n\times m}$ 上随机分布的矩阵 $\boldsymbol{A}$ 以及整数格 $\Lambda^\perp(\boldsymbol{A})$的短基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$,设 Gram-Schmidt 正交化后为 $\tilde{\boldsymbol{T}}_{\boldsymbol{A}}$,则 $\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\leqslant L=O(\sqrt{n\lg q})$,$\|\boldsymbol{T}_{\boldsymbol{A}}\|\leqslant O(n\lg q)$以压倒性概率成立.

引理 4. 原像抽样算法[31]:设 $q\geqslant 3$,$m\geqslant O(n\lg q)$,随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 以及整数格 $\Lambda^\perp(\boldsymbol{A})$的短基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$,设高斯参数 $s\geqslant\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\omega(\sqrt{\lg n})$,那么对任意的 $\boldsymbol{u}\in\mathbb{Z}_q^n$,存在有效的多项式时间算法 $SamplePre(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},s,\boldsymbol{u})$,统计近似于从离散高斯分布 $G_{\Lambda^{\boldsymbol{u}}(\boldsymbol{A}),s}$ 中抽取向量 $\boldsymbol{v}\in\Lambda^{\boldsymbol{u}}(\boldsymbol{A})$. 由高斯分布的性质,$\boldsymbol{v}$ 将以压倒性的概率满足 $\|\boldsymbol{v}\|\leqslant s\sqrt{m}$. 其中 $\Lambda^{\boldsymbol{u}}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m:\boldsymbol{Ae}=\boldsymbol{u} \bmod q\}$. 可以很容易的扩展到矩阵的原像抽样算法,即:

对任意的矩阵 $\boldsymbol{U}\in\mathbb{Z}^{n\times k}$,其余参数与基本的原像抽样算法相同,存在扩展的多项式时间算法 $SamplePre(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},s,\boldsymbol{U})$,统计近似于从离散高斯分布 $G_{\Lambda^{\boldsymbol{U}}(\boldsymbol{A}),s}$ 中得到矩阵 $\boldsymbol{V}\in\Lambda^{\boldsymbol{u}}(\boldsymbol{A})$,且 $\boldsymbol{AV}=\boldsymbol{U} \bmod q$. 同时 $\|\boldsymbol{V}\|\leqslant s\sqrt{m}$ 以压倒性概率成立.

引理 5. 格基委派算法[32]:设 $\mathbb{Z}^q$ 上小范数可逆矩阵(按离散高斯分布独立抽取每一列)的集合为 $D_{m\times m}$,矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,整数格 $\Lambda^\perp(\boldsymbol{A})$的短基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$,高斯参数 $s\geqslant\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|m\omega(\lg^2 m)$,矩阵 $\boldsymbol{R}\leftarrow D_{m\times m}$,存在多项式时间算法 $BasicDel(\boldsymbol{A},\boldsymbol{R},\boldsymbol{T}_{\boldsymbol{A}},s)$输出格 $\Lambda^\perp(\boldsymbol{B}=\boldsymbol{AR}^{-1})$的短基 $\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}^{m\times m}$,$\|\tilde{\boldsymbol{T}}_{\boldsymbol{B}}\|\leqslant s/(\omega(\sqrt{\lg m}))$. 且不存在多项式时间 $BasicDel$ 的求逆运算. 存在多项式时间算法 $SampleRwithBasis(\boldsymbol{A})$输出矩阵 $\boldsymbol{R}\leftarrow D_{m\times m}$以及格 $\Lambda^\perp(\boldsymbol{B}=\boldsymbol{AR}^{-1})$的短基 $\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}^{m\times m}$,$\|\tilde{\boldsymbol{T}}_{\boldsymbol{B}}\|\leqslant O(\sqrt{n\lg q})$. 存在确定性的多项式算法 $ExtBasis(\boldsymbol{F}=\boldsymbol{A}|\boldsymbol{C},\boldsymbol{T}_{\boldsymbol{A}})$输出 $\boldsymbol{A}|\boldsymbol{C}$ 对应的整数格 $\Lambda^\perp(\boldsymbol{A}|\boldsymbol{C})$的基 $\boldsymbol{T}_{\boldsymbol{F}}$,且 $\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|=\|\tilde{\boldsymbol{T}}_{\boldsymbol{F}}\|$.

定义 2. 本文提出的数字签名方案包括 5 个多项式时间算法:

1) 系统建立 $Setup$. 由密钥生成中心 KGC 运行,输入安全参数 n,输出系统公共参数 PP 和主密钥 MSK.

2) 用户密钥提取 $KeyExtract$. 由 KGC 与用户交互完成,输入公共参数 PP、用户 ID、主密钥 MSK 以及当前时刻 t,输出用户公钥 pk_{ID}^t、用户私钥 sk_{ID}^t.

3) 密钥更新算法 $Update$. 输入用户当前 ID 与更新的时间区间,KGC 与用户交互完成密钥更新.

4) 签名算法 $Sign$. 输入系统公共参数、用户公钥与私钥、待签名消息、输出签名.

5) 验证算法 $Verify$. 输入系统公共参数、签名消息、用户公钥与用户 ID 以及签名,算法判断该签名是否是有效签名.

定义 3. 前向安全强不可伪造性 FSU-AMAIA:定义 2 类多项式时间强敌手:1)强敌手 $\mathcal{A}_1$ 模拟内部不诚实的用户,不诚实的用户指在签名过程中,会在未获得合法部分密钥的情况下尝试伪造自己或其他用户的签名,显然,伪造自身某一时刻的签名需要的安全性更高;2)强敌手 $\mathcal{A}_2$ 模拟恶意的密钥生成中心 KGC,在文献[8,18]中提出的安全模型的基础上,给出针对 2 类强敌手的安全游戏 $Game_1$ 与 $Game_2$,如果敌手 $\mathcal{A}_1$ 与 $\mathcal{A}_2$ 分别赢得 $Game_1$ 和 $Game_2$ 的概率是可忽略的,则称签名方案在适应性选择消息、选择身份攻击下对强敌手是前向安全强不可伪造的,游戏 $Game_b$,$b\in\{1,2\}$具体描述如下.

1) 系统建立 $Setup$. 输入安全参数 n,挑战者 C 生成系统公共参数 PP 与主密钥 MSK,如果 $b=1$,

C 将 PP 发送给敌手 $\mathcal{A}_1$,否则,将 PP 和 MSK 一起发给 $\mathcal{A}_2$.

2) 敌手适应性的进行如下问询.

① 公钥问询:敌手提交$\{ID,t\}$,挑战者返回相应的公钥回答问询.

② 密钥问询:敌手 $\mathcal{A}_b$ 提交$\{ID,t\}$,如果 $b=1$,挑战者 C 生成用户的部分签名密钥并发送给敌手.同时,敌手可以问询除自己之外的其他用户的私密值.注意如果$\{ID,t\}$对应的公钥发生过替换,挑战者返回⊥.如果 $b=2$,密钥问询只包括私密值问询,挑战者返回私密值给敌手.

③ 公钥替换问询:敌手可以替换任意身份下的公钥.

④ 密钥更新问询:敌手 $\mathcal{A}_b$ 提交更新时间区间与身份,挑战者返回更新后的密钥作为应答.

⑤ 签名问询:敌手 $\mathcal{A}_b$ 问询关于任意消息的签名,挑战者生成消息的签名并返回给敌手.注意如果相应的公钥被敌手替换过,则敌手需要提交对应的私密值.

敌手 $\mathcal{A}_b$ 可以选择变更用户身份或签名时刻并问询密钥和签名,也可以直接进入伪造阶段.

3) 伪造 $Forgery$.敌手 $\mathcal{A}_b$ 输出以身份 ID^*,时刻 t^* 下的关于消息 $\boldsymbol{\mu}^*$ 的签名 $\boldsymbol{e}^*$,敌手 $\mathcal{A}_b$ 赢得游戏当且仅当:

① $Verify(ID^*,\boldsymbol{e}^*,\boldsymbol{\mu}^*,t^*)=$Accept;

② 若 $b=1$,(ID^*,t^*)未作为密钥问询的输入;若 $b=2$,$(ID^*,t\leqslant t^*)$未作为私密值问询的输入;

③ 若 $b=1$,(ID^*,t_i,t^*)未作为密钥更新问询的输入;若 $b=2$,$(ID^*,t_i,t_j\leqslant t^*)$未作为密钥更新问询的输入;

④ 若 $b=2$,$(ID^*,t\leqslant t^*)$未作为公钥替换问询的输入;

⑤ $\boldsymbol{e}^*$ 未作为签名问询的应答返回给敌手.

若敌手 $\mathcal{A}_b$ 获胜的概率为 $Adv_{\mathcal{A}_b}=Pr[Forgery(ID^*,\boldsymbol{e}^*,\boldsymbol{\mu}^*,t^*)=\text{Success}]$,则当且仅当 $Adv_{\mathcal{A}_b}$ 关于安全参数 n 是可忽略的时,签名方案是适应性选择消息、选择身份攻击下前向安全强不可伪造FSU-AMAIA安全的.

3 随机预言模型下的签名方案 RO_LFC_SIG

本节给出随机预言模型下的前向安全的格基无证书数字签名方案 RO_LFC_SIG,作为构建标准模型下前向安全无证书签名方案的基础.RO_LFC_SIG 方案具体包括 5 个多项式时间的算法.

1) 系统建立 $Setup$.设 n 为安全参数,实数 $M>0$,$\alpha>0$,k,λ,T 为正整数,素数 $q\geqslant 3$.设正整数 $m\geqslant 5n\ \mathrm{lb}q$,$L=O(\sqrt{n\ \mathrm{lb}q})$,取 3 个抗碰撞的 Hash 函数:$H_1:\{0,1\}^*\rightarrow\mathbb{Z}_q^{n\times k}$;$H_2:\{0,1\}^*\rightarrow D_{m\times m}$;$H_3:\mathbb{Z}_q^{2n}\times\{0,1\}^*\rightarrow\{\boldsymbol{v},\boldsymbol{v}\in\{-1,0,1\}^k,\|\boldsymbol{v}\|\leqslant k\}$.

KGC 运行$\langle\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}}\rangle=TrapGen(n,q,m)$,得到近似随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$及整数格 $\Lambda^{\perp}(\boldsymbol{A})$的基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$,$\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\leqslant L=O(\sqrt{n\ \mathrm{lb}q})$.设高斯参数 $s\geqslant\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\omega(\sqrt{\mathrm{lb}n})$,参数序列$\{\sigma_0,\sigma_1,\cdots,\sigma_T\}$,其中 $\sigma_0=\omega(\mathrm{lb}m)$,$\sigma_i\geqslant m^{3i/2}\omega(\mathrm{lb}\ m)^{2i-1}$.设离散正态分布参数 $\delta\leqslant\alpha\lambda s\sqrt{6m}$.随机矩阵 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$.

KGC 公布公共参数 $PP=\{\boldsymbol{A},\boldsymbol{B},H_1,H_2,H_3\}$,主密钥 $MSK=\{\boldsymbol{T}_{\boldsymbol{A}}\}$.

2) 密钥提取 $KeyExtract$.给定 PP、ID、密钥生成时刻 $t_0\in[1,T]$,KGC 生成部分密钥:$\boldsymbol{T}_{\boldsymbol{A}}^{t_0}=BasicDel(\boldsymbol{A},H_2(ID|t_0),\boldsymbol{T}_{\boldsymbol{A}},\sigma_{t_0})$,其中 $\boldsymbol{T}_{\boldsymbol{A}}^{t_0}$ 为整数格 $\Lambda^{\perp}(\boldsymbol{A}H_2^{-1}(ID|t_0))$的短基,且有 $\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}^{t_0}\|\leqslant\sigma_{t_0}\sqrt{m}$.

KGC 选取从高斯分布 $G_{\mathbb{Z}_q^{m\times k},s}$ 中抽取随机矩阵 $\boldsymbol{C}_{ID}^{t_0}$,且 $\|\boldsymbol{C}_{ID}^{t_0}\|\leqslant s\sqrt{m}$.之后调用 $SamplePre(\boldsymbol{A}H_2^{-1}(ID|t_0),\boldsymbol{T}_{\boldsymbol{A}}^{t_0},s,H_1(ID|t_0)-\boldsymbol{A}\boldsymbol{C}_{ID}^{t_0})$得到 $\boldsymbol{S}_{ID}^{t_0}$,且满足 $\|\boldsymbol{S}_{ID}^{t_0}\|\leqslant s\sqrt{m}$.则用户 ID 在时刻 t_0 的部分密钥为 $\begin{bmatrix}\boldsymbol{S}_{ID}^{t_0}\\ \boldsymbol{C}_{ID}^{t_0}\end{bmatrix}\in\mathbb{Z}_q^{2m\times k}$.

用户从离散高斯分布 $G_{\mathbb{Z}_q^{m\times k},s}$ 中随机采样矩阵 $\boldsymbol{X}_{ID}^{t_0}$ 作为私密值.

因此,用户 ID 在时刻 t_0 的完整密钥为 $sk_{ID}^{t_0}=[\boldsymbol{S}_{ID}^{t_0}\quad\boldsymbol{C}_{ID}^{t_0}\quad\boldsymbol{X}_{ID}^{t_0}]\in\mathbb{Z}_q^{m\times 3k}$.公钥为 $pk_{ID}^{t_0}=\boldsymbol{B}\boldsymbol{C}_{ID}^{t_0}+\boldsymbol{B}\boldsymbol{X}_{ID}^{t_0}\in\mathbb{Z}_q^{n\times k}$.

3) 密钥更新 $KeyUpdate$.假设密钥更新时间区间为 $\lfloor t_j,t_i\rfloor$,设矩阵 $\boldsymbol{A}_{t_j}=\boldsymbol{A}H_2^{-1}(ID|t_0)H_2^{-1}(ID|t_0+1)\cdots H_2^{-1}(ID|t_j)$.KGC 运行:$\boldsymbol{T}_{\boldsymbol{A}}^{t_i}=BasicDel(\boldsymbol{A}_{t_j},H_2(ID|t_i)H_2(ID|t_i-1)H_2(ID|t_i-2)\cdots H_2(ID|t_j+1),\boldsymbol{T}_{\boldsymbol{A}}^{t_j},\boldsymbol{\sigma}_{t_i})$,以及 $SamplePre(\boldsymbol{A}_{t_i},T_{\boldsymbol{A}}^{t_i},s,H_1(ID|t_i)-\boldsymbol{A}\boldsymbol{C}_{ID}^{t_i})$得到 $\boldsymbol{S}_{ID}^{t_i}$.则时刻 t_i 用户的密钥为 $sk_{ID}^{t_0}=[\boldsymbol{S}_{ID}^{t_i}\quad\boldsymbol{C}_{ID}^{t_i}\quad\boldsymbol{X}_{ID}^{t_i}]$,其中 $\boldsymbol{X}_{ID}^{t_i}$ 为用户从 $G_{\mathbb{Z}_q^{m\times k},s}$ 中随机采样得到.

关于高斯参数 σ_{t_i} 的选取:由引理 5,有 $\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}^{t_i-1}\|\leqslant\sigma_{t_i-1}\sqrt{m}$,$\sigma_{t_i}\geqslant\|\tilde{\boldsymbol{T}}_{ID}^{t_i-1}\|m\omega(\mathrm{lb}m)^2$,若取 $\sigma_0=\omega(\mathrm{lb}m)$,

则有 $\sigma_{t_i}\geqslant m^{3t_i/2}\omega(\mathrm{lb}\ m)^{2t_i+1}$. 由引理 1,可以得到 $\delta\leqslant\alpha\lambda s\sqrt{6m}$.

4) 签名算法 *Sign*. 设待签名消息为 $\boldsymbol{\mu}\in\{0,1\}^*$,用户公钥 pk_{ID}^t,私钥 sk_{ID}^t. 用户随机选取向量 $\boldsymbol{y}=\begin{bmatrix}\boldsymbol{y}_1\\ \boldsymbol{y}_2\\ \boldsymbol{y}_3\end{bmatrix}\in\mathbb{Z}^{3m}$,其中 $\boldsymbol{y}_1\leftarrow D_\delta^m,\boldsymbol{y}_2\leftarrow D_\delta^m,\boldsymbol{y}_3\leftarrow D_\delta^m$.

设 $\boldsymbol{h}=H_3\left(\begin{bmatrix}\boldsymbol{A}_t & \boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\boldsymbol{y},\boldsymbol{\mu}\right),\boldsymbol{x}=sk_{ID}^t\boldsymbol{h}\in\mathbb{Z}^{3m}$,$\boldsymbol{\varepsilon}=\boldsymbol{x}+\boldsymbol{y}$,以概率 $\min(1,D_\delta^{3m}(\boldsymbol{\varepsilon})/MD_{\delta,\boldsymbol{x}}^{3m}(\boldsymbol{\varepsilon}))$ 输出签名$(\boldsymbol{\varepsilon},\boldsymbol{h})$.

5) 验证算法 *Verify*. 输入$(ID,(\boldsymbol{\varepsilon},\boldsymbol{h}),\boldsymbol{\mu},t)$,算法输出 Accept 当且仅当:

① $\|\boldsymbol{\varepsilon}\|\leqslant 2\delta\sqrt{3m}$;

② $\boldsymbol{h}=H_3\left(\begin{bmatrix}\boldsymbol{A}_t & \boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\boldsymbol{\varepsilon}-\begin{bmatrix}H_1(ID\|t)\\ pk_{ID}^t\end{bmatrix}\boldsymbol{h},\boldsymbol{\mu}\right)$.

正确性:

① 由引理 2,签名统计不可区分于分布 D_δ^{3m},从而 $\|\boldsymbol{\varepsilon}\|\leqslant 2\delta\sqrt{3m}$ 以压倒性概率成立;

② $\begin{bmatrix}\boldsymbol{A}_t & \boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\boldsymbol{\varepsilon}-\begin{bmatrix}H_1(ID\|t)\\ pk_{ID}^t\end{bmatrix}\boldsymbol{h}=\begin{bmatrix}\boldsymbol{A}_t & \boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\boldsymbol{\varepsilon}-\begin{bmatrix}\boldsymbol{A}_t & \boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\begin{bmatrix}\boldsymbol{S}_{ID}^t\\ \boldsymbol{C}_{ID}^t\\ \boldsymbol{X}_{ID}^t\end{bmatrix}\boldsymbol{h}=\begin{bmatrix}\boldsymbol{A}_t & \boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}(\boldsymbol{\varepsilon}-\boldsymbol{x})=\begin{bmatrix}\boldsymbol{A}_t & \boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\boldsymbol{y}$.

4　RO_LFC_SIG 的安全性分析

本节基于 SIS 假设证明随机预言模型下方案的前向安全强不可伪造性. 不失一般性,设敌手的问询时刻为$[1,T]$区间上的连续值,时刻 $t_0=1$. 设 Q 为总的问询身份数,T_{Sam},T_{Bas},T_{Trap},$T_{\mathrm{SamRwithBas}}$,T_{Ext} 为算法,*BasicDel*,*TrapGen*,*SampleRwithBasis* 以及 *ExtBasis* 运行时间,T_{mul} 为一次 $m\times m$ 矩阵乘法的近似运行时间.

定理 1. RO_LFC_SIG 方案对于第 1 类强敌手的前向安全强不可伪造性 FSU-AMAIA 基于小整数解假设 $\mathcal{P}_{\mathrm{SIS}}(q,m,8\delta\sqrt{2m}+4s\lambda\sqrt{2m})$. 具体地,令 $\mathcal{A}_1$ 为第 1 类多项式时间敌手,若 $Adv_{\mathcal{A}_1}=\xi$ 为不可忽略的,则有多项式算法,在至多 $\tau'=\tau+TQ(T_{\mathrm{Sam}}+T_{\mathrm{SamRwithBas}}+(T+2)T_{\mathrm{mul}})+(T-t^*)T_{\mathrm{Bas}}$ 的时间内以概率 $Adv_B=\xi(1-2^{-\omega(\mathrm{lb}n)})/TQ$ 解决 $\mathcal{P}_{\mathrm{SIS}}(q,m,8\delta\sqrt{2m}+4s\lambda\sqrt{2m})$ 问题,其中 τ 为 $Game_1$ 运行时间.

证明. 假设存在敌手 $\mathcal{A}_1$ 可以伪造签名,则可以如下构造多项式算法.

1) 系统建立 *Setup*. 设安全参数为 n,实数 $M>0$,$\alpha>0$,正整数 k,λ,T,$\beta=8\delta\sqrt{2m}+4s\lambda\sqrt{2m}$,素数 $q\geqslant\beta\omega(\sqrt{n\ \mathrm{lb}\ n})$,$m\geqslant 5n\ \mathrm{lb}\ q$,$L=O(\sqrt{n\ \mathrm{lb}\ q})$. 取抗碰撞的 Hash 函数 $H_3:\mathbb{Z}_q^{2n}\times\{0,1\}^*\rightarrow\{\boldsymbol{v},\boldsymbol{v}\in\{-1,0,1\}^k,\|\boldsymbol{v}\|\leqslant k\}$. 高斯参数 $s,\delta,\{\sigma_0,\sigma_1,\cdots,\sigma_T\}$ 与 RO_LFC_SIG 方案中相同.

挑战者 $\mathcal{C}$ 随机选择 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$ 为 SIS 实例,随机矩阵 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$,维护 4 个 Hash 列表 L_{H_1},L_{H_2},L_{H_3},L_{sig}. $\mathcal{C}$ 从 $G_{\mathbb{Z}_q^m,s}$ 逐列采样选取 t^* 个可逆的小范数矩阵 $\boldsymbol{R}_i\in\mathbb{Z}_q^{m\times m}$,并设 $\boldsymbol{A}=\boldsymbol{A}_0\boldsymbol{R}_{t^*}\boldsymbol{R}_{t^*-1}\cdots\boldsymbol{R}_1$,$\gamma\in[1,Q]$.

$\mathcal{C}$ 将公共参数 $PP=\{\boldsymbol{A},\boldsymbol{A}_0,\boldsymbol{B},H_3\}$ 发送给敌手 $\mathcal{A}_1$.

2) 敌手可以适应性的进行如下问询.

① H_2 问询:敌手提交$\{ID,t_i\}$,$\mathcal{C}$ 查找列表 L_{H_2} 判断是否有对应的 Hash 值,若有,则直接作为敌手的应答返回敌手,否则,设 $D_{m\times m}$ 为 $\mathbb{Z}_q$ 上的小范数可逆阵集合. 若 ID 不为第 γ 次问询身份,$\mathcal{C}$ 调用多项式时间函数$\langle\boldsymbol{R},\boldsymbol{T}_{\boldsymbol{AR}}^{t_i}\rangle=SampleRwithBasis(\boldsymbol{A})$ 生成 $\boldsymbol{R}\leftarrow D_{m\times m}$ 以及 $\Lambda^\perp(\boldsymbol{AR}^{-1})$ 的基 $\boldsymbol{T}_{\boldsymbol{AR}}^{t_i}\in\mathbb{Z}^{m\times m}$,$\mathcal{C}$ 设置 $H_2(ID\|t_i)=\boldsymbol{R}$ 并将其返回给敌手作为应答. 同时,将$\{\boldsymbol{T}_{\boldsymbol{AR}}^{t_i},\boldsymbol{R}\}$插入到列表 L_{H_2} 中.

若 ID 为第 γ 次问询身份,$t_i\leqslant t^*$,$\mathcal{C}$ 直接令 $H_2(ID\|t_i)=\boldsymbol{R}_{t_i}$,$\boldsymbol{T}_{\boldsymbol{AR}}^{t_i}=\perp$,将 $H_2(ID\|t_i)=\boldsymbol{R}_{t_i}$ 返回给敌手,并将$\{\boldsymbol{T}_{\boldsymbol{AR}}^{t_i},\boldsymbol{R}_{t_i}\}$插入到 L_{H_2} 中.

若 ID 为第 γ 次问询身份,$t_i=t^*+1$,$\mathcal{C}$ 调用 $SampleRwithBasis(\boldsymbol{A}_0)$ 生成 $\boldsymbol{R}\leftarrow D_{m\times m}$,$\boldsymbol{T}_{\boldsymbol{AR}}^{t_i}\in\mathbb{Z}^{m\times m}$. $\mathcal{C}$ 设置 $H_2(ID\|t^*+1)=\boldsymbol{R}$ 并将其返回给敌手作为应答. 同时,将$\{\boldsymbol{T}_{\boldsymbol{AR}}^{t_i},\boldsymbol{R}\}$插入到列表 L_{H_2} 中.

若 ID 为第 γ 次问询身份,$t_i>t^*+1$,$\mathcal{C}$ 从 $D_{m\times m}$ 中随机采样得到 $H_2(ID\|t_i)$,由 *BasicDel*$(\boldsymbol{A}_0H_2^{-1}(ID\|t^*+1),H_2(ID\|t_i)H_2(ID\|t_i-1)\cdots H_2(ID\|t^*+2),\boldsymbol{T}_{\boldsymbol{AR}}^{t^*+1},\sigma_{t_i})$得到 $\boldsymbol{T}_{\boldsymbol{AR}}^{t_i}$. 之后将 $H_2(ID\|t_i)$返回给敌手并将$\{\boldsymbol{T}_{\boldsymbol{AR}}^{t_i},H_2(ID\|t_i)\}$插入到 L_{H_2} 中.

② H_1 问询:敌手提交$\{ID,t_i\}$,$\mathcal{C}$ 查找列表 L_{H_1} 判断是否有对应的 Hash 值,若有,则直接作为敌手的应答返回敌手,否则,$\mathcal{C}$ 从离散高斯分布 $G_{\mathbb{Z}_q^m,s}$ 中逐列采样得到 $\boldsymbol{C}_{ID}^{t_i}$,且 $\|\boldsymbol{C}_{ID}^{t_i}\|\leqslant s\sqrt{m}$ 以绝对优势成立.

若 ID 不为第 γ 次问询身份,$\mathcal{C}$ 查找列表 L_{H_2} 中的表项$\{\boldsymbol{T}_{\boldsymbol{AR}}^{t_i},H_2(ID\|t_i)\}$,若不存在,则首先进行 H_2 问询. 之后 $\mathcal{C}$ 调用 $SamplePre(\boldsymbol{A}H_2^{-1}(ID\|t_i),$

$\boldsymbol{T}_{\boldsymbol{AR}}^{t_i}, s, \boldsymbol{M}$)得到 $\boldsymbol{S}_{ID}^{t_i}$,其中 $\boldsymbol{M}\in\mathbb{Z}_q^{n\times k}$为随机矩阵.从而 $H_1(ID|t_i)=\boldsymbol{M}+\boldsymbol{AC}_{ID}^{t_i}$,$\mathcal{C}$将 $H_1(ID|t_i)$保存到 L_{H_1} 中并作为敌手的应答.同时,将部分密钥 $\begin{bmatrix}\boldsymbol{S}_{ID}^{t_i}\\ \boldsymbol{C}_{ID}^{t_i}\end{bmatrix}\in\mathbb{Z}_q^{2m\times k}$保存到 L_{sig}中.

若 ID 为第 γ 次问询身份,$t_i\leqslant t^*$,$\mathcal{C}$ 从 $G_{\boldsymbol{\Lambda}_q^m,s}$ 中逐列采样得到 $\boldsymbol{S}_{ID}^{t_i}$,并将 $\begin{bmatrix}\boldsymbol{S}_{ID}^{t_i}\\ \boldsymbol{C}_{ID}^{t_i}\end{bmatrix}$保存到 L_{sig}中.同时将 $H_1(ID|t_i)=\boldsymbol{A}_0(\boldsymbol{S}_{ID}^{t_i}+\boldsymbol{C}_{ID}^{t_i})$作为应答,并保存到 L_{H_1}中.

若 ID 为第 γ 次问询身份,$t_i\geqslant t^*+1$,$\mathcal{C}$从列表 L_{H_2}中取得$\{\boldsymbol{T}_{\boldsymbol{AR}}^{t_i}, H_2(ID|t_i)\}$,由$(\boldsymbol{A}_0H_2^{-1}(ID|t^*+1)H_2^{-1}(ID|t^*+2)\cdots H_2^{-1}(ID|t_i), \boldsymbol{T}_{\boldsymbol{AR}}^{t_i}, s, \boldsymbol{M})$得到 $\boldsymbol{S}_{ID}^{t_i}$,$H_1(ID|t_i)=\boldsymbol{M}+\boldsymbol{A}_0\boldsymbol{C}_{ID}^{t_i}$,保存到 L_{H_1}中并返回给敌手,$\begin{bmatrix}\boldsymbol{S}_{ID}^{t_i}\\ \boldsymbol{C}_{ID}^{t_i}\end{bmatrix}$保存到 L_{sig}中.

③ 部分密钥问询:敌手提交$\{ID,t\}$,需要满足 H_1 问询已经执行,否则先执行 H_1 问询.若 ID 不为第 γ 次问询身份,或者 $t\neq t^*$,$\mathcal{C}$查找列表 L_{sig}并返回部分密钥 $\begin{bmatrix}\boldsymbol{S}_{ID}^{t}\\ \boldsymbol{C}_{ID}^{t}\end{bmatrix}$;否则 $\mathcal{C}$退出.

④ 私密值问询:敌手提交对应于其他用户的$\{ID,t\}$,$\mathcal{C}$从离散高斯分布 $G_{\boldsymbol{\Lambda}_q^m,s}$中逐列采样得到私密值 $\boldsymbol{X}_{ID}^t$,且 $\|\boldsymbol{X}_{ID}^t\|\leqslant s\sqrt{m}$以绝对优势成立.$\mathcal{C}$将 $\boldsymbol{X}_{ID}^t$插入 L_{sig}并作为 $\mathcal{A}_1$ 私密值问询的应答.

⑤ 公钥问询:敌手提交$\{ID,t,\boldsymbol{X}_{ID}^t\}$,其中 $\boldsymbol{X}_{ID}^t$为敌手自己选取的私密值或之前经过私密值问询获得的其他用户的私密值.$\mathcal{C}$验证 $\|\boldsymbol{X}_{ID}^t\|\leqslant s\sqrt{m}$是否成立,若不成立则拒绝敌手.否则,$\mathcal{C}$查询 L_{sig}并验证$\{ID,t\}$对应的部分密钥是否存在,若不存在,需提前进行部分密钥问询,并将$\{ID,t\}$作为部分密钥问询输入.之后挑战者 $\mathcal{C}$ 返回 $pk_{ID}^t=\boldsymbol{BC}_{ID}^t+\boldsymbol{BX}_{ID}^t\in\mathbb{Z}_q^{n\times k}$并将公钥和敌手提交的合法私密值 $\boldsymbol{X}_{ID}^t$保存到 L_{sig}中.

⑥ 密钥更新问询:敌手提交$[t_j,t_i]$和 ID,需要满足已经对$\{ID,t_i\}$进行 H_1 问询.若 ID 不为第 γ 次问询身份,或者 $t_i\neq t^*$,$\mathcal{C}$直接将 $\begin{bmatrix}\boldsymbol{S}_{ID}^{t_i}\\ \boldsymbol{C}_{ID}^{t_i}\end{bmatrix}$返回给敌手;否则,$\mathcal{C}$退出.

⑦ 公钥替换问询:敌手提交$\{ID,t\}$以及 pk_{ID}^t,$\mathcal{C}$查找表 L_{sig}并替换$\{ID,t\}$对应的公钥.

⑧ H_3 问询:$\mathcal{C}$ 查找列表 L_{H_3} 并判断 $\boldsymbol{h}=H_3\left(\begin{bmatrix}\boldsymbol{A}_t & \boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\boldsymbol{y},\boldsymbol{\mu}\right)$是否已经存在,若存在则直接作为敌手的应答,否则,从$\{\boldsymbol{v},\boldsymbol{v}\in\{-1,0,1\}^k,\|\boldsymbol{v}\|\leqslant k\}$中随机选取 $\boldsymbol{h}$ 作为应答并保存到 L_{H_3}中.

⑨ 签名问询:敌手 $\mathcal{A}_1$ 提交$\{ID,t,\boldsymbol{\mu}\}$,$\mathcal{C}$查找 L_{H_3},L_{sig}得到对应的密钥与 $\boldsymbol{h}$,之后正常签名并应答敌手.如果$\{ID,t\}$对应的公钥发生过替换,则 $\mathcal{A}_1$ 需要提交对应的私密值.

3) 伪造 *Forgery*. $\mathcal{A}_1$ 输出消息 $\boldsymbol{\mu}^*$ 在$\{ID^*,t^*\}$下的伪造签名$(\boldsymbol{\varepsilon}^*,\boldsymbol{h}^*)$,当且仅当 ID^* 为第 γ 次问询身份且 $Verify(ID^*,(\boldsymbol{\varepsilon}^*,\boldsymbol{h}^*),\boldsymbol{\mu}^*,t^*)=$ Accept 时敌手成功.根据一般分叉引理[21],敌手可以以不可忽略的概率输出另一个有效伪造签名$(\boldsymbol{\varepsilon}',\boldsymbol{h}')$,因此有 $\begin{bmatrix}\boldsymbol{A}_{t^*} & \boldsymbol{A}_0 & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\boldsymbol{\varepsilon}^*-\begin{bmatrix}H_1(ID^*|t^*)\\ pk_{ID^*}^{t^*}\end{bmatrix}\boldsymbol{h}^*=\begin{bmatrix}\boldsymbol{A}_{t^*} & \boldsymbol{A}_0 & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B}\end{bmatrix}\boldsymbol{\varepsilon}'-\begin{bmatrix}H_1(ID^*|t^*)\\ pk_{ID^*}^{t^*}\end{bmatrix}\boldsymbol{h}'$,且 $\boldsymbol{A}_{t^*}=\boldsymbol{A}_0$.即:$\boldsymbol{A}_0(\boldsymbol{\varepsilon}_1^*+\boldsymbol{\varepsilon}_2^*-\boldsymbol{\varepsilon}_1'-\boldsymbol{\varepsilon}_2'+(\boldsymbol{S}_{ID^*}^{t^*}+\boldsymbol{C}_{ID^*}^{t^*})(\boldsymbol{h}'-\boldsymbol{h}^*))=\boldsymbol{0}$.由于$\|\boldsymbol{\varepsilon}_1^*\|,\|\boldsymbol{\varepsilon}_2^*\|,\|\boldsymbol{\varepsilon}_1'\|,\|\boldsymbol{\varepsilon}_2'\|\leqslant 2\delta\sqrt{3m},\boldsymbol{h}^*,\boldsymbol{h}'\leqslant\lambda$,因此 $\|\boldsymbol{\varepsilon}_1^*+\boldsymbol{\varepsilon}_2^*-\boldsymbol{\varepsilon}_1'-\boldsymbol{\varepsilon}_2'+(\boldsymbol{S}_{ID^*}^{t^*}+\boldsymbol{C}_{ID^*}^{t^*})(\boldsymbol{h}'-\boldsymbol{h}^*)\|\leqslant 8\delta\sqrt{2m}+4s\lambda\sqrt{2m}$以压倒性概率成立.

由原像抽样函数与最小熵性质[31],$\boldsymbol{\varepsilon}_1^*+\boldsymbol{\varepsilon}_2^*-\boldsymbol{\varepsilon}_1'-\boldsymbol{\varepsilon}_2'+(\boldsymbol{S}_{ID^*}^{t^*}+\boldsymbol{C}_{ID^*}^{t^*})(\boldsymbol{h}'-\boldsymbol{h}^*)=\boldsymbol{0}$ 的概率至多为 $1-2^{-\omega(\text{lb}n)}$,因此,算法 B 成功解决 $\mathcal{P}_{\text{SIS}}(q,m,8\delta\sqrt{2m}+4s\lambda\sqrt{2m})$问题的概率为 $Adv_B=\xi(1-2^{-\omega(\text{lb}n)})/TQ$,总时间为 $\tau'=\tau+TQ(T_{\text{Sam}}+T_{\text{SamRwithBas}}+(T+2)T_{\text{mul}})+(T-t^*)T_{\text{Bas}}$. 证毕.

定理 2. RO_LFC_SIG 方案对于第 2 类强敌手的前向安全强不可伪造性 FSU-AMAIA 基于小整数解假设 $\mathcal{P}_{\text{SIS}}(q,m,8\delta\sqrt{2m}+4s\lambda\sqrt{2m})$.具体地,令 $\mathcal{A}_2$ 为第 2 类多项式时间敌手,若 $Adv_{\mathcal{A}_2}=\xi$ 为不可忽略的,则有多项式算法 B,在至多 $\tau'=\tau+TQ(T_{\text{Sam}}+2T_{\text{mul}})$的时间内以概率 $Adv_B=\xi(1-2^{-\omega(\text{lb}n)})/TQ$ 解决 $\mathcal{P}_{\text{SIS}}(q,m,8\delta\sqrt{2m}+4s\lambda\sqrt{2m})$问题,其中 τ 为 $Game_2$ 运行时间.

证明. 假设存在敌手 $\mathcal{A}_2$ 可以伪造签名,则构造多项式算法步骤如下.

1) 系统建立 *Setup*. 设 $n,k,\lambda,T,M,\alpha,m,L,s,t^*,\gamma,\beta,q,\delta$ 以及参数序列$\{\sigma_0,\sigma_1,\cdots,\sigma_T\}$与定理 1 中一样. 3 个抗碰撞的 Hash 函数 H_1,H_2,H 与

RO_LFC_SIG 方案中一样.$\langle \boldsymbol{A}, \boldsymbol{T}_A \rangle = TrapGen(n, q, m)$. 随机矩阵 $\boldsymbol{B} \in \mathbb{Z}_q^{n \times m}$ 为 SIS 实例,维护 2 个 Hash 列表 $L_{H_3}, L_{\text{sig}}, L_{\text{sig}}$ 中的表项为 $\{ID, t, \boldsymbol{X}_{ID}^t\}$.

挑战者 $\mathcal{C}$ 将公共参数 $PP = \{\boldsymbol{A}, \boldsymbol{B}, H_1, H_2, H_3\}$ 与主密钥 $MSK = \{\boldsymbol{T}_A\}$ 发送给敌手 $\mathcal{A}_2$.

2) 敌手可以适应性的进行如下问询.

① 私密值问询:敌手提交 $\{ID, t\}$,$\mathcal{C}$ 查找列表 L_{sig},若 $\{ID, t\}$ 对应的私密值已经存在,直接将其返回给敌手,否则,$\mathcal{C}$ 从离散高斯分布 $G_{\mathbf{Z}_q^m, s}$ 中逐列采样得到私密值 $\boldsymbol{X}_{ID}^t$,且 $\| \boldsymbol{X}_{ID}^t \| \leqslant s\sqrt{m}$ 以绝对优势成立. $\mathcal{C}$ 将 $\boldsymbol{X}_{ID}^t$ 插入 L_{sig}. 若 ID 不为第 γ 次问询,或 ID 为第 γ 次问询但 $t \neq t^*$,$\boldsymbol{X}_{ID}^t$ 作为 $\mathcal{A}_2$ 问询的应答. 若 ID 为第 γ 次问询且 $t = t^*$,$\mathcal{C}$ 退出.

敌手 $\mathcal{A}_2$ 已知主密钥 MSK,因此不需要进行部分密钥问询. 部分密钥的更新也可以由敌手自己完成.

② 公钥问询:敌手提交 $\{ID, t\}$,若 $\{ID, t\}$ 对应的私密值不存在,则先进行私密值问询. 之后,挑战者 $\mathcal{C}$ 返回 $\boldsymbol{B}\boldsymbol{X}_{ID}^t$,敌手 $\mathcal{A}_2$ 可以生成完整的公钥 $pk_{ID}^t = \boldsymbol{B}\boldsymbol{C}_{ID}^t + \boldsymbol{B}\boldsymbol{X}_{ID}^t \in \mathbb{Z}_q^{n \times k}$.

③ 公钥替换问询:敌手提交 $\{ID, t\}$ 以及 pk_{ID}^t,挑战者查找表 L_{sig} 并替换 $\{ID, t\}$ 对应的公钥. 若 ID 为第 γ 次问询且 $t = t^*$,$\mathcal{C}$ 退出.

④ H_3 问询:与定理 1 相同.

⑤ 签名问询:敌手 $\mathcal{A}_2$ 提交 $\{ID, t, \boldsymbol{S}_{ID}^t, \boldsymbol{C}_{ID}^t, \boldsymbol{\mu}\}$,$\mathcal{C}$ 可以通过 $\boldsymbol{A}, \boldsymbol{S}_{ID}^t = H_1(ID \| t) - \boldsymbol{A}\boldsymbol{C}_{ID}^t$ 以及 $\| \boldsymbol{S}_{ID}^t \| \leqslant s\sqrt{m}$,$\| \boldsymbol{C}_{ID}^t \| \leqslant s\sqrt{m}$ 验证 $\boldsymbol{S}_{ID}^t, \boldsymbol{C}_{ID}^t$ 的合法性. 若提交的部分密钥合法,$\mathcal{C}$ 查找 L_{H_3}, L_{sig} 得到对应的 $\boldsymbol{h}, \boldsymbol{X}_{ID}^t$,之后正常签名并应答敌手.

3) 伪造 $Forgery$. 敌手输出消息 $\boldsymbol{\mu}^*$ 在 $\{ID^*, t^*\}$ 下的伪造签名 $(\boldsymbol{\varepsilon}^*, \boldsymbol{h}^*)$,当且仅当 ID^* 为第 γ 次问询身份且 $Verify(ID^*, (\boldsymbol{\varepsilon}^*, \boldsymbol{h}^*), \boldsymbol{\mu}^*, t^*) =$ Accept 时敌手成功. 同定理 1 一样,根据一般分叉引理[21],敌手可以以不可忽略的概率输出另一个有效伪造签名 $(\boldsymbol{\varepsilon}', \boldsymbol{h}')$,因此有 $\begin{bmatrix} \boldsymbol{A}_{t^*} & \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B} \end{bmatrix} \boldsymbol{\varepsilon}^* - \begin{bmatrix} H_1(ID^* \| t^*) \\ pk_{ID^*}^{t^*} \end{bmatrix} \boldsymbol{h}^* = \begin{bmatrix} \boldsymbol{A}_{t^*} & \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{B} \end{bmatrix} \boldsymbol{\varepsilon}' - \begin{bmatrix} H_1(ID^* \| t^*) \\ pk_{ID^*}^{t^*} \end{bmatrix} \boldsymbol{h}'$,即:$\boldsymbol{B}(\boldsymbol{\varepsilon}_2^* + \boldsymbol{\varepsilon}_3^* - \boldsymbol{\varepsilon}_2' - \boldsymbol{\varepsilon}_3' + (\boldsymbol{S}_{ID^*}^{t^*} - \boldsymbol{X}_{ID^*}^{t^*})(\boldsymbol{h}' - \boldsymbol{h}^*)) = \boldsymbol{0}$. 与定理 1 一样,$\| \boldsymbol{\varepsilon}_2^* + \boldsymbol{\varepsilon}_3^* - \boldsymbol{\varepsilon}_2' - \boldsymbol{\varepsilon}_3' + (\boldsymbol{S}_{ID^*}^{t^*} - \boldsymbol{X}_{ID^*}^{t^*})(\boldsymbol{h}' - \boldsymbol{h}^*) \| \leqslant 8\delta\sqrt{2m} + 4s\lambda\sqrt{2m}$ 以不可忽略的概率成立.

由原像抽样函数与最小熵性质[31],$\boldsymbol{\varepsilon}_2^* + \boldsymbol{\varepsilon}_3^* - \boldsymbol{\varepsilon}_2' - \boldsymbol{\varepsilon}_3' + (\boldsymbol{S}_{ID^*}^{t^*} - \boldsymbol{X}_{ID^*}^{t^*})(\boldsymbol{h}' - \boldsymbol{h}^*) = \boldsymbol{0}$ 的概率至多为 $1 - 2^{-\omega(\text{lb}n)}$,因此,算法 B 成功解决 $\mathcal{P}_{\text{SIS}}(q, m, 8\delta\sqrt{2m} + 4s\lambda\sqrt{2m})$ 问题的概率为 $Adv_B = \xi(1 - 2^{-\omega(\text{lb}n)})/TQ$,总时间为 $\tau' = \tau + TQ(T_{\text{Sam}} + 2T_{\text{mul}})$.

证毕.

5　标准模型下的签名方案 ST_LFC_SIG

随机预言模型下 RO_LFC_SIG 签名方案的安全性依赖于方案所采用的 Hash 函数的完全随机性,这在实际应用中可能无法满足. 因此,为了增强格基前向安全的无证书签名方案的应用性与安全性,我们在 RO_LFC_SIG 的基础上,研究了基于标准模型的 ST_LFC_SIG 方案. 本节给出方案的具体实现.

需要注意的是,本文提出的 ST_LFC_SIG 方案是第 1 个标准模型下基于格的无证书数字签名方案,方案具体由 5 个多项式时间的算法构成.

1) 系统建立 $Setup$. 设安全参数为 n,实数 $M > 0, \alpha > 0$,设正整数 k, b, d, l, T,素数 $q \geqslant 3, m \geqslant 5n\,\text{lb}q$,$L = O(\sqrt{n\,\text{lb}q})$. 高斯参数 s,参数序列 $\{\sigma_0, \sigma_1, \cdots, \sigma_T\}$ 以及矩阵 $\langle \boldsymbol{A}, \boldsymbol{T}_A \rangle$ 与 RO_LFC_SIG 方案相同. 离散正态分布参数 $\delta \leqslant \alpha s\sqrt{m}$. 设抗碰撞的 Hash 函数:$H_1: \{0,1\}^* \to \{0,1\}^d$ 与 $H_2: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^l$.

取 $2Td$ 个矩阵 $\boldsymbol{R}_{i,j}^b \leftarrow D_{m \times m}$,其中 $i \in [1, d], j \in [1, T], b \in \{0, 1\}$. 设随机均匀小范数矩阵 $\boldsymbol{C}_i \in \mathbb{Z}_q^{n \times k}, i \in [1, d]$;$F_i \in \mathbb{Z}_q^{n \times m}, i \in [1, l]$.

公共参数 $PP = \{\boldsymbol{A}, \langle \boldsymbol{C}_i \rangle, \langle \boldsymbol{F}_i \rangle, \langle \boldsymbol{R}_{i,j}^b \rangle\}$;主密钥 $MSK = \{\boldsymbol{T}_A\}$.

2) 密钥提取 $KeyExtract$. 给定用户身份 ID,起始时刻 $t_0 \in [1, T]$. KGC 运行 $\boldsymbol{h} = H_1(ID \| t_0)$,$\boldsymbol{C}_{ID\|t_0} = \sum_{i=0}^{d-1} (-1)^{h[i]} \boldsymbol{C}_{i+1}$. 由 $\boldsymbol{T}_{\boldsymbol{AC}} = ExtBasis(\boldsymbol{A} | \boldsymbol{C}_{ID\|t_0}, \boldsymbol{T}_A)$ 得到 $[\boldsymbol{A} | \boldsymbol{C}_{ID\|t_0}]$ 的短基 $\boldsymbol{T}_{\boldsymbol{AC}}$. KGC 调用 $\boldsymbol{S}_{ID}^{t_0} = (\boldsymbol{A} | \boldsymbol{C}_{ID\|t_0}, \boldsymbol{T}_{\boldsymbol{AC}}, s, \boldsymbol{0})$ 得到 $\boldsymbol{S}_{ID}^{t_0} \in \mathbb{Z}^{(m+k) \times m}$,$\| \boldsymbol{S}_{ID}^{t_0} \| \leqslant s\sqrt{m+k}$. KGC 将 $\boldsymbol{S}_{ID}^{t_0}$ 发送给用户作为部分密钥.

用户验证 $[\boldsymbol{A} | \boldsymbol{C}_{ID\|t_0}] \boldsymbol{S}_{ID}^{t_0} = \boldsymbol{0} \bmod q$ 且 $\| \boldsymbol{S}_{ID}^{t_0} \| \leqslant s\sqrt{m + k + 2d^2 s^2 mk}$ 是否成立.

若用户 ID 为第 1 次生成密钥,运行 $\langle \boldsymbol{B}, \boldsymbol{T}_B \rangle = TrapGen(n, q, m)$ 得到密钥根矩阵 $\langle \boldsymbol{B}, \boldsymbol{T}_B \rangle$.

用户计算 $\boldsymbol{R}_{ID|t_0}=\boldsymbol{R}_{d,t_0}^{\boldsymbol{h}[d-1]}\boldsymbol{R}_{d-1,t_0}^{\boldsymbol{h}[d-2]}\cdots\boldsymbol{R}_{1,t_0}^{\boldsymbol{h}[0]}$,由 $\boldsymbol{X}_{ID}^{t_0}=BasicDel(\boldsymbol{B},\boldsymbol{R}_{ID|t_0},\boldsymbol{T}_{\boldsymbol{B}},\sigma_{t_0})$得到时刻 t_0 公钥 $pk_{ID}^{t_0}=\boldsymbol{B}\boldsymbol{R}_{ID|t_0}^{-1}\in\mathbb{Z}_q^{n\times m}$和私密值 $\boldsymbol{X}_{ID}^{t_0}$.

用户时刻 t_0 私钥 $sk_{ID}^{t_0}=\begin{bmatrix}\boldsymbol{S}_{ID}^{t_0}\\ \boldsymbol{X}_{ID}^{t_0}\end{bmatrix}\in\mathbb{Z}^{(2m+k)\times m}$.

3) 密钥更新 *KeyUpdate*. 假设密钥更新时间区间为 $\lfloor t_j,t_i\rfloor$. KGC 计算 $\boldsymbol{h}=H_1(ID|t_i)$和 $\boldsymbol{C}_{ID|t_i}=\sum_{i=0}^{d-1}(-1)^{\boldsymbol{h}[i]}\boldsymbol{C}_{i+1}$,之后调用 *KeyExtract* 算法得到 $\boldsymbol{S}_{ID}^{t_i}\in\mathbb{Z}^{(m+k)\times m}$作为时刻 t_i 的部分密钥并发送给用户.

用户计算 $\boldsymbol{h}=H_1(ID|t)$,对 $t\in[t_j+1,t_i]$,有 $\boldsymbol{R}_{ID|t}=\boldsymbol{R}_{d,t}^{\boldsymbol{h}[d-1]}\boldsymbol{R}_{d-1,t}^{\boldsymbol{h}[d-2]}\cdots\boldsymbol{R}_{1,t}^{\boldsymbol{h}[0]}$,并代入到公式 $\boldsymbol{X}_{ID}^{t_i}=BasicDel(pk_{ID}^{t_j},\boldsymbol{R}_{ID|t_j}\boldsymbol{R}_{ID|t_j-1}\cdots\boldsymbol{R}_{ID|t_j+1},\boldsymbol{X}_{ID}^{t_j},\sigma_{t_i})$中得到时刻 t_i 的私密值 $\boldsymbol{X}_{ID}^{t_i}$以及公钥 $pk_{ID}^{t_i}=pk_{ID}^{t_j}\boldsymbol{R}_{ID|t_j+1}^{-1}\boldsymbol{R}_{ID|t_j+2}^{-1}\cdots\boldsymbol{R}_{ID|t_i}^{-1}$.

4) 签名算法 *Sign*. 输入用户公钥 pk_{ID}^{t},私钥 sk_{ID}^{t}、待签名消息 $\boldsymbol{\mu}\in\{0,1\}^*$. 随机选取向量 $\boldsymbol{r}\in D_\delta^m$. 设 $\boldsymbol{v}=H_2(ID,t,\boldsymbol{\mu})$,$F_{ID|t}^{\boldsymbol{\mu}}=\sum_{i=0}^{l-1}(-1)^{\boldsymbol{v}[i]}\boldsymbol{F}_{i+1}$,用户计算 $\boldsymbol{v}_2=SamplePre(pk_{ID}^{t},\boldsymbol{X}_{ID}^{t},s,\boldsymbol{F}_{ID|t}^{\boldsymbol{\mu}}\boldsymbol{r})$,并设 $\boldsymbol{v}_1=\boldsymbol{S}_{ID}^{t}\boldsymbol{v}_2=\begin{bmatrix}\boldsymbol{S}_{ID}^{t'}\\ \boldsymbol{S}_{ID}^{t''}\end{bmatrix}\boldsymbol{v}_2\in\mathbb{Z}^{m+k}$,$\boldsymbol{x}=\begin{bmatrix}\boldsymbol{S}_{ID}^{t'}\boldsymbol{v}_2\\ \boldsymbol{S}_{ID}^{t''}\boldsymbol{v}_2\\ \boldsymbol{v}_2\end{bmatrix}=\begin{bmatrix}\boldsymbol{x}_1\\ \boldsymbol{x}_2\\ \boldsymbol{x}_3\end{bmatrix}$,$\boldsymbol{\varepsilon}=\boldsymbol{r}+\boldsymbol{v}_2$.

以概率 $\min(1,D_\delta^m(\boldsymbol{\varepsilon})/MD_{\delta,\boldsymbol{v}_2}^m(\boldsymbol{\varepsilon}))$输出签名 $(\boldsymbol{\varepsilon},\boldsymbol{x})$.

5) 验证算法 *Verify*. 输入$(ID,(\boldsymbol{\varepsilon},\boldsymbol{h}),\boldsymbol{\mu},t)$,算法输出 Accept 当且仅当:

① $\|\boldsymbol{\varepsilon}\|\leqslant 2\delta\sqrt{m}$;

② $\|\boldsymbol{x}\|\leqslant s\sqrt{m+s^2(2m^2+2mk+4d^2s^2m^2k)}$;

③ 验证者计算 $\boldsymbol{C}_{ID|t}$ 与 $\boldsymbol{F}_{ID|t}^{\boldsymbol{\mu}}$并代入验证等式 $\begin{bmatrix}\boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & pk_{ID}^{t}\end{bmatrix}\begin{bmatrix}\boldsymbol{x}_1\\ \boldsymbol{x}_3\end{bmatrix}=\begin{bmatrix}-\boldsymbol{C}_{ID|t}\boldsymbol{x}_2\\ \boldsymbol{F}_{ID|t}^{\boldsymbol{\mu}}(\boldsymbol{\varepsilon}-\boldsymbol{x}_3)\end{bmatrix}$.

正确性:由引理 5,签名$(\boldsymbol{\varepsilon},\boldsymbol{x})$统计不可区分于离散正态分布 D_δ^m,从而 $\|\boldsymbol{\varepsilon}\|\leqslant 2\delta\sqrt{m}$ 以压倒性概率成立;由引理 4,$\|\boldsymbol{x}_3\|\leqslant s\sqrt{m}$,且 $\boldsymbol{v}_1=\boldsymbol{S}_{ID}^{t}\boldsymbol{x}_3$,则②成立. 根据$[\boldsymbol{A}|\boldsymbol{C}_{ID|t}]\boldsymbol{S}_{ID}^{t}=\boldsymbol{0}\bmod q$ 以及 $pk_{ID}^{t}\boldsymbol{v}_2=\boldsymbol{F}_{ID|t}^{\boldsymbol{\mu}}\boldsymbol{r}$ 可以代入 *Verify* 中验证③成立.

6 ST_LFC_SIG 的安全性分析

定理 3. ST_LFC_SIG 方案对于第 1 类强敌手的 FSU-AMAIA 安全性基于小整数解假设 $\mathcal{P}_{\mathrm{SIS}}(q,m,(1+ds\sqrt{2m})s^2\sqrt{2m^2+2mk+4d^2s^2m^2k})$. 具体地,令 $\mathcal{A}_1$ 为第 1 类多项式时间敌手,若 $Adv_{\mathcal{A}_1}=\xi$ 为不可忽略的,则有多项式算法 B,在至多 $\tau'=\tau+TQ(2T_{\mathrm{Sam}}+T_{\mathrm{Bas}}+T_{\mathrm{Trap}}+T_{\mathrm{SamRwithBas}}+(Td+2)T_{\mathrm{mul}})$的时间内以概率 $Adv_B=\xi(1-2^{-\omega(\mathrm{lb}n)})/TQ$ 解决 $\mathcal{P}_{\mathrm{SIS}}(q,m,(1+ds\sqrt{2m})s^2\sqrt{2m^2+2mk+4d^2s^2m^2k})$ 问题,其中 τ 为 $Game_1$ 运行时间,k,d 定义与 ST_LFC_SIG 中相同.

证明. 假设存在敌手 $\mathcal{A}_1$ 可以伪造签名,则构造多项式算法步骤如下.

1) 系统建立 *Setup*. 设 $n,M,\alpha,k,b,d,l,T,q,m,L,\delta,H_1,H_2$,参数序列$\{\sigma_0,\sigma_1,\cdots,\sigma_T\}$以及 $2Td$ 个矩阵 $\boldsymbol{R}_{i,j}^{b}$与 ST_LFC_SIG 方案相同,$s\geqslant L\omega\sqrt{\mathrm{lb}n}$.

对 $i\in[1,d]$,从分布 $G_{\boldsymbol{Z}^m,s}$中逐列采样得到小范数矩阵 $\boldsymbol{D}_i\in\mathbb{Z}_q^{m\times k}$,且 $\|\boldsymbol{D}_i\|\leqslant s\sqrt{m}$ 以压倒性概率成立. 设正整数 p_i,$\langle\boldsymbol{E},\boldsymbol{T}_{\boldsymbol{E}}\rangle=TrapGen(n,q,k)$,$\boldsymbol{C}_i=\boldsymbol{A}\boldsymbol{D}_i+p_i\boldsymbol{E}$,其中随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$为 SIS 实例. 则 $\boldsymbol{C}_i$ 统计不可区分于$\mathbb{Z}_q^{n\times k}$上的随机均匀矩阵. 对 $i\in[1,l]$,设 $\boldsymbol{F}_i\in\mathbb{Z}_q^{n\times m}$为随机均匀矩阵.

维护 Hash 表 L_{sig},表项为$\{\langle ID,t\rangle,pk_{ID}^{t},\boldsymbol{S}_{ID}^{t},\boldsymbol{X}_{ID}^{t},b\}$,其中 $b\in\{0,1\}$为标记位,初始化为 0.

挑战者 $\mathcal{C}$将 $PP=\{\boldsymbol{A},\langle\boldsymbol{C}_i\rangle,\langle\boldsymbol{F}_i\rangle,\langle\boldsymbol{R}_{i,j}^{b}\rangle\}$发给敌手 $\mathcal{A}_1$.

2) 敌手可以适应性地进行如下问询.

① 部分密钥问询:敌手提交$\{ID,t\}$,挑战者计算 $\boldsymbol{h}=H_1(ID|t)$,$\boldsymbol{C}_{ID|t}=\sum_{i=0}^{d-1}(-1)^{\boldsymbol{h}[i]}\boldsymbol{C}_{i+1}=\boldsymbol{A}\boldsymbol{D}+p\boldsymbol{E}$,其中 $\boldsymbol{D}=\sum_{i=0}^{d-1}(-1)^{\boldsymbol{h}[i]}\boldsymbol{D}_{i+1}$,$p=\sum_{i=0}^{d-1}(-1)^{\boldsymbol{h}[i]}p_{i+1}$.

如果 $p=0\bmod q$ 第 1 次出现,$\mathcal{C}$ 随机生成 $\mathbb{Z}^{(m+k)\times m}$上的矩阵$\boldsymbol{S}_{ID}^{t}$并返回给敌手作为部分密钥应答,设置 L_{sig}中$\{ID,t\}$对应表项的 $b=1$. 若 $p=0$ 不为第 1 次出现,$\mathcal{C}$终止游戏.

若 $p\neq 0$,挑战者 $\mathcal{C}$从$G_{\boldsymbol{Z}^m,s}$中逐列采样得到矩阵 $\boldsymbol{S}_{ID}^{t''}\in\mathbb{Z}^{m\times m}$. 由于 $\boldsymbol{T}_{\boldsymbol{E}}$ 为 $\Lambda^{\perp}(p\boldsymbol{E})$的短基,$\mathcal{C}$ 可由$(p\boldsymbol{E},\boldsymbol{T}_{\boldsymbol{E}},s,-\boldsymbol{A}\boldsymbol{S}_{ID}^{t''})$得到 $\boldsymbol{S}_{ID}^{t'}\leftarrow G_{\boldsymbol{Z}^{k\times m},s}$,从而 $\boldsymbol{S}_{ID}^{t''}=\boldsymbol{S}_{ID}^{t''}-\boldsymbol{D}\boldsymbol{S}_{ID}^{t''}\in\mathbb{Z}^{m\times m}$. 将 $\boldsymbol{S}_{ID}^{t}=\begin{bmatrix}\boldsymbol{S}_{ID}^{t'}\\ \boldsymbol{S}_{ID}^{t''}\end{bmatrix}$作为部分密钥应答返回敌手. 显然 $\|\boldsymbol{S}_{ID}^{t}\|\leqslant s\sqrt{m+k+2d^2s^2mk}$,将 $\boldsymbol{S}_{ID}^{t}$保存于 L_{sig}中.

② 公钥和私密值问询:敌手提交$\{ID,t\}$,挑战者可以调用方案的$KeyExtract$的正常计算pk_{ID}^t和$\boldsymbol{X}_{ID}^t$并回答敌手(若$t>1$需要运行$KeyUpdate$的公钥和私密值更新部分).同时将公钥pk_{ID}^t和私密值$\boldsymbol{X}_{ID}^t$保存到L_{sig}中.注意敌手仅需要对其他用户进行公钥和私密值问询,其自己的公钥和私密值可以由敌手自己生成.

③ 密钥更新问询:敌手提交$[t_j,t_i]$和ID,挑战者$\mathcal{C}$调用部分密钥问询并以$\{ID,t_i\}$作为输入进行部分密钥更新.如果游戏没有终止,且ID对应于敌手之外的用户,则挑战者$\mathcal{C}$调用$KeyUpdate$算法完成公钥和私密值更新.

④ 公钥替换问询:敌手提交$\{ID,t\}$以及pk_{ID}^t,挑战者查找表L_{sig}并替换$\{ID,t\}$对应的公钥.

⑤ 签名问询:敌手提交$\{ID,t,\boldsymbol{\mu},pk_{ID}^t,\boldsymbol{X}_{ID}^t\}$,$\mathcal{C}$验证$\|\boldsymbol{X}_{ID}^t\|\leqslant\frac{s}{\omega(\sqrt{\mathrm{lb}\,m})}$是否成立且$\boldsymbol{X}_{ID}^t$是否为$pk_{ID}^t$对应的整数格的基,若不是,则拒绝敌手.否则,如果$L_{sig}$中$\{ID,t\}$的表项存在且$b=0$,则$\mathcal{C}$将$L_{sig}$中保存的$\boldsymbol{S}_{ID}^t$代入$Sign$算法对消息$\mu$进行签名并回答敌手.若$\{ID,t\}$对应表项不存在,$\mathcal{C}$先以$\{ID,t\}$为输入跳转到部分密钥问询,更新$L_{sig}$中的$\{ID,t\}$表项之后再进行签名问询.同时,$\mathcal{C}$将公钥$pk_{ID}^t$和私密值$\boldsymbol{X}_{ID}^t$保存到$L_{sig}$对应表项中.

若$\{ID,t\}$表项存在,但$b=1$,$\mathcal{C}$终止游戏.

3) 伪造$Forgery$.敌手输出消息$\boldsymbol{\mu}^*$在$\{ID^*,t^*\}$下的伪造签名$(\boldsymbol{\varepsilon}^*,\boldsymbol{x}^*)$,敌手成功当且仅当$\{ID^*,t^*\}$恰为$L_{sig}$中的标记项$b=1$且$Verify(ID^*,(\boldsymbol{\varepsilon}^*,\boldsymbol{x}^*),\boldsymbol{\mu}^*,t^*)=$Accept.将$\boldsymbol{C}_{ID^*|t^*}=\boldsymbol{AD}$代入到$Verify$算法中可以得到方程:$\boldsymbol{Ax}_1^*=-\boldsymbol{ADx}_2^*$,即$\boldsymbol{A}(\boldsymbol{x}_1^*+\boldsymbol{Dx}_2^*)=\boldsymbol{0}$.如果$(\boldsymbol{\varepsilon}^*,\boldsymbol{x}^*)$为正确的伪造,那么$\|\boldsymbol{x}_1^*\|\leqslant s^2\sqrt{2m^2+2mk+4d^2s^2m^2k}$和$\|\boldsymbol{x}_2^*\|\leqslant s^2\sqrt{2m^2+2mk+4d^2s^2m^2k}$以压倒性概率成立,同时$\|\boldsymbol{D}\|\leqslant ds\sqrt{m}$,因此有$\|\boldsymbol{x}_1^*+\boldsymbol{Dx}_2^*\|\leqslant(1+ds\sqrt{2m})s^2\sqrt{2m^2+2mk+4d^2s^2m^2k}$以压倒性概率成立.游戏模拟的时间上限为$\tau'=\tau+TQ(2T_{\mathrm{Sam}}+T_{\mathrm{Bas}}+T_{\mathrm{Trap}}+T_{\mathrm{SamRwithBas}}+(Td+2)T_{\mathrm{mul}})$.由原像抽样函数和最小熵性质,$\boldsymbol{x}_1^*+\boldsymbol{Dx}_2^*\neq\boldsymbol{0}$的概率至多为$1-2^{-\omega(\mathrm{lb}\,n)}$,因此算法$B$成功解决$\mathcal{P}_{\mathrm{SIS}}(q,m,(1+ds\sqrt{2m})s^2\sqrt{2m^2+2mk+4d^2s^2m^2k})$问题的概率为$Adv_B=\xi(1-2^{-\omega(\mathrm{lb}\,n)})/TQ$.　　证毕.

定理 4. ST_LFC_SIG 方案对于第 2 类强敌手的 FSU-AMAIA 安全性基于小整数解假设$\mathcal{P}_{\mathrm{SIS}}(q,m,s\sqrt{m}+\sqrt{2}lsm(2\delta+s))$.具体地,令$\mathcal{A}_2$为第 2 类多项式时间敌手,若$Adv_{\mathcal{A}_2}=\xi$为不可忽略的,则有多项式算法$B$,在至多$\tau'=\tau+TQ(T_{\mathrm{Sam}}+T_{\mathrm{Bas}}+T\times T_{\mathrm{SamRwithBas}}+(Td+2)T_{\mathrm{mul}})$的时间内以概率$Adv_B=\xi(TQ-t^*)(1-2^{-\omega(\mathrm{lb}\,n)})/TQ(TQ-1)$解决$\mathcal{P}_{\mathrm{SIS}}(q,m,s\sqrt{m}+\sqrt{2}lsm(2\delta+s))$问题,其中$\tau$为$Game_2$运行时间.

证明. 假设存在敌手$\mathcal{A}_2$可以伪造签名,则构造多项式算法步骤如下.

1) 系统建立$Setup$.设设$n,M,\alpha,k,b,d,l,T,q,m,L,\delta,H_1,H_2$,参数序列$\{\sigma_0,\sigma_1,\cdots,\sigma_T\}$,参数$s,\delta$与定理 3 中一样.$\langle\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}}\rangle=TrapGen(n,q,m)$.设$i\in[1,d]$,随机均匀小范数矩阵$\boldsymbol{C}_i\in\mathbb{Z}_q^{n\times k}$.对$i\in[1,l]$,逐列从$G_{\mathbb{Z}^m,s}$中采样得到$\boldsymbol{D}_i\in\mathbb{Z}_q^{m\times m}$,则$\boldsymbol{F}_i=\boldsymbol{B}_0\boldsymbol{D}_i$统计不可区分于$\mathbb{Z}_q^{n\times m}$上的随机均匀分布,其中随机矩阵$\boldsymbol{B}_0$为 SIS 实例.

维护 Hash 表L_{sig},表项为$\{\langle ID,t\rangle,pk_{ID}^t,\boldsymbol{X}_{ID}^t,\boldsymbol{X},\boldsymbol{T}_{\boldsymbol{X}}\}$,其中$\boldsymbol{X}$为用户$ID$的密钥根矩阵,$\boldsymbol{T}_{\boldsymbol{X}}$为$\Lambda^{\perp}(\boldsymbol{X})$的基.

算法 1. 生成Td个矩阵$\boldsymbol{R}_{i,j}^b$算法.

① Set $\gamma\in[1,Q],t^*\in[1,T]$ / * ID^*为第r次秘钥问询对应的身份 * /

② Foreach $t\leqslant t^*$ do

③　$\boldsymbol{h}=H_1(ID^*|t)$;

④　$R_{i,j}^{\boldsymbol{h}[i-1]}\leftarrow D_{m\times m}$, where $i\in[1,d],j\in[1,t^*]$;

⑤　$\boldsymbol{R}_{ID^*|t}=\boldsymbol{R}_{d,t}^{\boldsymbol{h}[d-1]}\boldsymbol{R}_{d-1,t}^{\boldsymbol{h}[d-2]}\cdots\boldsymbol{R}_{1,t}^{\boldsymbol{h}[0]}$;

⑥ End Foreach

⑦ $\boldsymbol{B}=\boldsymbol{B}_0\boldsymbol{R}_{ID^*|t^*}\boldsymbol{R}_{ID^*|t^*-1}\cdots\boldsymbol{R}_{ID^*|1}$;

　/ * $\boldsymbol{B}$为ID^*对应的秘钥根矩阵 * /

⑧ $\boldsymbol{B}'=\boldsymbol{B}_0$;

⑨ For $j=t^*+1$ to T

⑩　$\boldsymbol{h}=H_1(ID^*|j-1)$;

⑪　$\boldsymbol{R}_{ID^*|j-1}=\boldsymbol{R}_{d,j-1}^{\boldsymbol{h}[d-1]}\boldsymbol{R}_{d-1,j-1}^{\boldsymbol{h}[d-2]}\cdots\boldsymbol{R}_{1,j-1}^{\boldsymbol{h}[0]}$;

⑫　If $j\geqslant t^*+2$ then

⑬　　$\boldsymbol{B}'=\boldsymbol{B}'\boldsymbol{R}_{ID^*|j-1}^{-1}$;

⑭　End If

⑮　For $i=0$ to $d-1$

⑯　　If $i=0$ then

⑰　　$\langle\boldsymbol{R}_{i+1,j}^{\boldsymbol{h}[i]},\boldsymbol{T}_{ID^*|j}\rangle=SampleRwithBasis(\boldsymbol{B}')$;

⑱ Else $\boldsymbol{R}_{i+1,j}^{\boldsymbol{h}[i]} \leftarrow D_{m\times m}$;

⑲ End If

⑳ End For

㉑ End For

剩余 dT 个 $\boldsymbol{R}_{i,j}^{b}$ 为 $D_{m\times m}$ 上的随机均匀矩阵.

$\mathcal{C}$ 公布 $PP=\{\boldsymbol{A},\boldsymbol{B}_0,\langle\boldsymbol{C}_i\rangle,\langle\boldsymbol{F}_i\rangle,\langle\boldsymbol{R}_{i,j}^{b}\rangle\}$,并将主密钥 $MSK=\{\boldsymbol{T}_A\}$ 一起发给敌手 $\mathcal{A}_2$.

2) 敌手可以适应性地进行如下问询.

① 公钥问询:敌手提交 $\{ID,t\}$,若 ID 不为第 γ 次问询身份,挑战者 $\mathcal{C}$ 首先查询表 L_{sig} 看是否有对应于身份 ID 的密钥根矩阵. 如果没有,由 $SampleRwithBasis(\boldsymbol{B})$ 得到 $\boldsymbol{R}\leftarrow D_{m\times m}$ 和 $\Lambda^{\perp}(\boldsymbol{BR}^{-1})$ 的基 $\boldsymbol{T}_{\boldsymbol{BR}}$,$\mathcal{C}$ 将 $\boldsymbol{BR}^{-1}$ 作为当前身份 ID 的密钥根矩阵,并将其和 $\boldsymbol{T}_{\boldsymbol{BR}}$ 一起保存到 L_{sig} 中. $\mathcal{C}$ 调用签名方案的 $KeyExtract$ 和 $KeyUpdate(t>1)$ 算法正常计算用户的公钥应答.

若 ID 为第 γ 次问询身份且 $t\leqslant t^*$,设 $pk_{ID^*}^{t}=\boldsymbol{BR}_{ID^*|1}^{-1}\boldsymbol{R}_{ID^*|2}^{-1}\cdots\boldsymbol{R}_{ID^*|t}^{-1}$,将 $pk_{ID^*}^{t}$ 作为敌手的公钥问询应答.

若 ID 为第 γ 次问询身份且 $t\geqslant t^*+1$,设 $\boldsymbol{h}=H_1(ID^*|t)$,$\boldsymbol{B}'=\boldsymbol{B}_0\boldsymbol{R}_{ID^*|t^*+1}^{-1}\boldsymbol{R}_{ID^*|t^*+2}^{-1}\cdots\boldsymbol{R}_{ID^*|t-1}^{-1}$,$BasicDel(\boldsymbol{B}'(\boldsymbol{R}_{1,t}^{\boldsymbol{h}[0]})^{-1},\boldsymbol{R}_{d,t}^{\boldsymbol{h}[d-1]}\boldsymbol{R}_{d-1,t}^{\boldsymbol{h}[d-2]}\cdots\boldsymbol{R}_{2,t}^{\boldsymbol{h}[1]},\boldsymbol{T}_{ID^*|t},\sigma_t)$ 得到 $\Lambda^{\perp}(\boldsymbol{B}'\boldsymbol{R}_{ID^*|t}^{-1})$ 的基 $\boldsymbol{X}_{ID^*}^{t}$. 将 $pk_{ID^*}^{t}=\boldsymbol{B}'\boldsymbol{R}_{ID^*|t}^{-1}$ 作为公钥返回敌手,并与私密值 $\boldsymbol{X}_{ID^*}^{t}$ 一起保存到 L_{sig} 中. 可以看出,$pk_{ID^*}^{t}=\boldsymbol{B}'\boldsymbol{R}_{ID^*|t}^{-1}=\boldsymbol{BR}_{ID^*|1}^{-1}\boldsymbol{R}_{ID^*|2}^{-1}\cdots\boldsymbol{R}_{ID^*|t}^{-1}$,$ID^*$ 的密钥根矩阵依然为 $\boldsymbol{B}$.

② 私密值问询:敌手提交 $\{ID,t\}$,若 ID 不为第 γ 次问询身份或 $t\geqslant t^*+1$,需要满足敌手已经进行过公钥问询,并得到私密值,否则先进行公钥问询,之后 $\mathcal{C}$ 从表 L_{sig} 中取出 $\boldsymbol{X}_{ID^*}^{t}$ 返回敌手. 若 ID 为第 γ 次问询身份且 $t\leqslant t^*$,$\mathcal{C}$ 退出.

敌手 $\mathcal{A}_2$ 已知主密钥 MSK,因此不需要进行部分密钥问询. 部分密钥的更新也可以由敌手自己完成.

③ 私密值更新问询:若 ID 不为第 γ 次问询身份时,敌手公钥和私密值均正常生成,因此挑战者 $\mathcal{C}$ 可以直接调用 $KeyUpdate$ 算法完成更新.

若 ID 为第 γ 次问询身份,设更新区间 $[t_j,t_i]$,若 $t_j\geqslant t^*$ 或 $t_i>t^*\geqslant t_j$,$\mathcal{C}$ 可以查表 L_{sig} 得到时刻 $t'=\max(t_j,t^*+1)$ 的公钥和私密值,之后可以调用 $KeyUpdate$ 算法在 $[t',t_i]$ 上完成更新. 若 $t^*\geqslant t_i$,$\mathcal{C}$ 退出.

④ 公钥替换问询:敌手提交 $\{ID,t\}$ 以及 pk_{ID}^{t},挑战者 $\mathcal{C}$ 查找表 L_{sig} 并替换 $\{ID,t\}$ 对应的公钥. 若 ID 为第 γ 次问询且 $t\leqslant t^*$,$\mathcal{C}$ 退出.

⑤ 签名问询:敌手提交 $\{ID,t,\boldsymbol{S}_{ID}^{t},\boldsymbol{\mu}\}$,若 ID 不为第 γ 次问询,或 ID 为第 γ 次问询但 $t\geqslant t^*+1$,$\mathcal{C}$ 拥有合法的公钥和私密值,可以直接为敌手进行签名应答并生成合法签名. 否则,$\mathcal{C}$ 退出.

3) 伪造 $Forgery$. 敌手输出消息 $\boldsymbol{\mu}^*$ 在 $\{ID^*,t^*\}$ 下的伪造签名 $(\boldsymbol{\varepsilon}^*,\boldsymbol{x}^*)$,敌手成功时有 $Verify(ID^*,(\boldsymbol{\varepsilon}^*,\boldsymbol{x}^*),\boldsymbol{\mu}^*,t^*)=\text{Accept}$. 设 $\boldsymbol{v}=H_2(ID^*,t^*,\boldsymbol{\mu}^*)$,$D=\sum_{0}^{l-1}(-1)^{\boldsymbol{v}[i]}\boldsymbol{D}_{i+1}$,将 $\boldsymbol{F}_{ID^*|t^*}^{\boldsymbol{\mu}}=\boldsymbol{B}_0\boldsymbol{D}$ 代入到 $Verify$ 算法中,注意到 $pk_{ID^*}^{t^*}=\boldsymbol{B}_0$,可以得到方程:$\boldsymbol{B}_0\boldsymbol{x}_3^*=\boldsymbol{B}_0\boldsymbol{D}(\boldsymbol{\varepsilon}^*-\boldsymbol{x}_3^*)$,即 $\boldsymbol{B}_0(\boldsymbol{x}_3^*-\boldsymbol{D}(\boldsymbol{\varepsilon}^*-\boldsymbol{x}_3^*))=\boldsymbol{0}$. 如果 $(\boldsymbol{\varepsilon}^*,\boldsymbol{x}^*)$ 为正确的伪造,那么 $\|\boldsymbol{\varepsilon}^*\|\leqslant 2\delta\sqrt{m}$ 和 $\|\boldsymbol{x}_3^*\|\leqslant s\sqrt{m}$ 以压倒性概率成立,同时 $\|\boldsymbol{D}\|\leqslant ls\sqrt{m}$ 以压倒性概率成立,因此有 $\|\boldsymbol{x}_3^*-\boldsymbol{D}(\boldsymbol{\varepsilon}^*-\boldsymbol{x}_3^*)\|\leqslant s\sqrt{m}+\sqrt{2}lsm(2\delta+s)$ 以压倒性概率成立. 游戏模拟的时间上限为 $\tau'=\tau+TQ(T_{\text{Sam}}+T_{\text{Bas}}+T\times T_{\text{SamRwithBas}}+(Td+2)T_{\text{mul}})$. 同定理 3,$\|\boldsymbol{x}_3^*-\boldsymbol{D}(\boldsymbol{\varepsilon}^*-\boldsymbol{x}_3^*)\|\neq\boldsymbol{0}$ 的概率至多为 $1-2^{-\omega(\text{lb}n)}$,因此算法成功解决 $\mathcal{P}_{\text{SIS}}(q,m,s\sqrt{m}+\sqrt{2}lsm(2\delta+s))$ 的概率为 $Adv_B=\xi(TQ-t^*)(1-2^{-\omega(\text{lb}n)})/TQ(TQ-1)$. 证毕.

由于用户的密钥由 KGC 和用户一同完成,而 KGC 生成的部分私钥依赖于主密钥 $\boldsymbol{T}_A$ 和当前时刻下的 $H_1(ID|t)$ 值,由 H_1 的抗碰撞性可知,在未知 $\boldsymbol{T}_A$ 的情况下,不诚实的用户获得时刻 $t'<t$ 的部分密钥 $\boldsymbol{S}_{ID}^{t'}$ 的难度不会小于破解 $\mathcal{P}_{\text{SIS}}(q,m+k,s\sqrt{m+k})$ 问题的难度. 同时,用户私密值为用户公钥对应的整数格的基. 由引理 5,即使恶意 KGC 获取 t 时刻的私密值 $\boldsymbol{X}_{ID}^{t}$,也无法获取任意时刻 $t'<t$ 的 $\boldsymbol{X}_{ID}^{t'}$. 而敌手在未知 $\boldsymbol{X}_{ID}^{t}$ 的情况下伪造签名组件 $\boldsymbol{v}_2$ 的难度不会小于破解 $\mathcal{P}_{\text{SIS}}(q,m,s\sqrt{m})$ 问题的难度. 根据定义 1,破解 SIS 问题的概率是可忽略的,综合定理 3 和定理 4,本文提出的标准模型下的 ST_LFC_SIG 签名方案对于不诚实的用户和恶意 KGC 均满足适应性选择消息、选择身份攻击的 FSU-AMAIA 前向安全强不可伪造性.

7 方案安全性与效率对比分析

文献[33]对无证书签名方案的安全模型进行了分析,并依据签名问询与私密值问询,对第 1 类强敌手和第 2 类强敌手分别给出了 8 种和 4 种不同能力

的敌手攻击等级,归纳如表 1 和表 2 所示. N-Sign 表示在签名问询,若身份 ID 对应的公钥发生过替换,则拒绝应答. S-Sign 表示无论公钥是否发生替换,都响应敌手的签名问询.

Table 1　Eight Different Attack Levels of Type 1 Adversary

表 1　敌手 1 对应的 8 种攻击等级

Name	Sign Oracle	(ID^*, μ^*)→Sign Oracle	ID^* to Secret Value Oracle
N-Type 1	N-Sign	No	No
SU-Type 1	N-Sign	Yes	No
SV-Type 1	N-Sign	No	Yes
SS-Type 1	S-Sign	No	No
SV-SU-Type 1	N-Sign	Yes	Yes
SS-SV-Type 1	S-Sign	No	Yes
SS-SU-Type 1	S-Sign	Yes	No
S-Type 1	S-Sign	Yes	Yes

Table 2　Four Different Attack Levels of Type 2 Adversary

表 2　敌手 2 对应的 4 种攻击等级

Name	Sign Oracle	(ID^*, μ^*)→Sign Oracle
N-Type 2	N-Sign	No
SU-Type 2	N-Sign	Yes
SS-Type 2	S-Sign	No
S-Type 2	S-Sign	Yes

由表 1 和表 2 可以看出,S-Type 1 和 S-Type 2 类型的 S-Type 敌手具有最强的攻击能力. 表 3 将本文提出的随机预言模型下的 RO_LFC_SIG 方案与标准模型下的 ST_LFC_SIG 方案,以及 Kim 等人[17]和 Tian 等人[18]的格基无证书签名方案,和文献[12-15]中的无证书签名方案进行安全性对比.

由表 3 可以看出,本文提出的无证书签名方案不仅具有抗量子攻击的能力,具有前向安全性,同时所基于的敌手模型攻击等级较高,因此方案具有较好的安全性. 更进一步地,本文提出的 ST_LFC_SIG 方案是第 1 个基于格的标准模型下的无证书签名方案,较之文献[12-15,17-18]中以及 RO_LFC_SIG 随机预言模型下的签名方案,在实际应用中的安全性更高.

Table 3　Comparison of Security

表 3　方案安全性对比

Schemes	Post Quantum	Key Exposure	Security Model	Threat Model
Ref[12]	No	No	Random	SU-Type
Ref[13]	No	No	Random	SU-Type
Ref[14]	No	No	Random	SS-SU-Type
Ref[15]	No	No	Random	S-Type
Ref[17]	Yes	No	Random	SS-SU-Type
Ref[18]	Yes	No	Random	SV-SU-Type
RO_LFC_SIG	Yes	Yes	Random	S-Type
ST_LFC_SIG	Yes	Yes	Standard	S-Type

在效率对比方面,本文除了选择文献[17-18]中的随机预言模型下的格基无证书签名方案外,还选择了 Yao 等人[2]和 Zhang 等人[20]的 FSIBS 以及 Rückert[26]的随机格签名方案,虽然后 3 种方案并不是无证书签名方案,但由于其均基于随机格,因此可以作为时间和空间复杂度对比的参照.

设参数与第 3 节方案中定义的相同,n 为安全参数,$m \geqslant 5n \text{ lb } q$,$k$ 为正整数. T_{Sam}, T_{Bas}, T_{Trap}, T_{Rand}, T_{Ext} 分别为算法 $SamplePre$, $BasicDel$, $TrapGen$, $RandBasis$, $ExtBasis$ 运行时间. T_{mul} 为一次标量乘法耗费时间. 7 种方案的渐近性复杂度对比如表 4 所示.

Table 4 Comparison of Asymptotic Complexity

表 4 渐近复杂度对比

Schemes	Public Key	Secret Key	Signature	Key Generation	Sign	Verify
Ref[2]	$O(ID)2mn\text{lb}(pq)$	$O(ID)\sqrt{2m}$	$O(ID)\sqrt{2m}$	$O(ID)(T_{\text{Rand}}+T_{\text{Ext}})$	$O(ID)T_{\text{Sam}}$	$(mn+n)T_{\text{mul}}$
Ref[17]	nm	$3m^2$	$3m$	$T_{\text{Sam}}+T_{\text{Trap}}$	$6mnT_{\text{mul}}+T_{\text{Sam}}$	$6mnT_{\text{mul}}$
Ref[18]	nm	$2m^2$	$4m$	T_{Sam}	$4mnT_{\text{mul}}$	$4mnT_{\text{mul}}$
Ref[20]	nm	m^2	$m+n/2$	$T_{\text{Bas}}+nm^2T_{\text{mul}}$	T_{Sam}	$(m^2+mn)T_{\text{mul}}$
Ref[26]	$3n^2m+m+n$	$4m^2$	$4m+n/2$	$T_{\text{Bas}}+T_{\text{Rand}}+T_{\text{Ext}}$	$T_{\text{Sam}}+T_{\text{Ext}}+n^2m^2T_{\text{mul}}$	$2nmT_{\text{mul}}$
RO_LFC_SIG	nk	$3km$	$3m+k$	$T_{\text{Bas}}+T_{\text{Sam}}+nmkT_{\text{mul}}$	$3mkT_{\text{mul}}$	$6mnT_{\text{mul}}$
ST_LFC_SIG	nm	$m(2m+k)$	$2m+k$	$T_{\text{Bas}}+T_{\text{Sam}}+T_{\text{Ext}}$	$T_{\text{Sam}}+(m+k)mT_{\text{mul}}$	$4mnT_{\text{mul}}$

设 $k\leqslant n/4$,则由表 4 可以看出,在保证安全性的基础上,本文方案的公钥尺寸优于其他的格基或身份基签名方案.标准模型下的 ST_LFC_SIG 签名方案的签名长度优于除文献[20]以外的其他方案.在私钥长度方面,本文方案优于文献[17,26]的方案,比 Yao 等人[2]、Tian 等人[18]和 Zhang 等人[20]的 FSIBS 方案略大.这主要是由于无证书签名方案需要利用部分密钥和私密值 2 个子部分来构造基于随机格的 2 个 $\mathcal{P}_{\text{SIS}}$ 等式,从而实现对不诚实用户和恶意 KGC 的前向安全强不可伪造性,而 Zhang 等人[20]的方案只考虑了随机预言模型下的外部敌手.此外,本文通过引入变量 k 降低了签名长度,并通过密钥根矩阵保证了较小的公钥长度以及安全证明中正确的敌手视角,而文献[20]中的安全证明由于缺少与身份绑定的密钥根矩阵的定义,将导致敌手关于同一挑战身份与挑战时刻的 2 次公钥问询产生不同的应答结果.而 Yao 等人[2]和 Tian 等人[18]的方案则不具备前向安全性.因此与文献[2,18,20]相比,本文方案的安全性更高.

时间复杂度方面,根据文献[30-31],有 $T_{\text{Ext}}<T_{\text{Sam}}<nm^2T_{\text{mul}}<T_{\text{Rand}}<T_{\text{Rand}}+nm^2T_{\text{mul}}<T_{\text{Bas}}<T_{\text{Trap}}$,在忽略采样时间的情况下,$T_{\text{Sam}}\approx n^2T_{\text{mul}}$.因此本文提出的 2 个签名方案的签名算法时间复杂度较文献[2,17,26]等方案均有优势.ST_LFC_SIG 方案在验证算法方面也基本优于其他方案.在密钥生成算法方面,本文优于 Yao 等人[2]和 Rückert[26]的方案,与文献[17,20]的方案基本持平.略大于 Tian 等人[18]的方案,这主要是由于为实现前向安全性,本文方案调用了 BasicDel 函数,增加了密钥生成算法时间.一种改进的方法是利用理想格构建前向安全的无证书签名方案,也是下一步的研究目标.

由以上分析可知,本文提出的 RO_LFC_SIG 和 ST_LFC_SIG 无证书签名方案首次在不引入第三方代理的条件下基于随机格实现了前向安全性与无证书的结合.同时,ST_LFC_SIG 方案也是第 1 个基于格的标准模型下可证安全的无证书签名方案,并解决了密钥泄露问题.通过以上安全性与效率的对比分析可知,在保证相对较低的时空复杂度的基础上,随机预言模型下 RO_LFC_SIG 方案和标准模型下的 ST_LFC_SIG 方案均可以达到较好的安全性与实用性.

8 结束语

本文基于格基委派技术,针对密钥泄露的前向安全性,在提出随机预言模型下 RO_LFC_SIG 方案的基础上,设计了标准模型下前向安全的无证书签名方案 ST_LFC_SIG,并给出了 2 个方案的具体构造.同时,基于随机预言模型和标准模型,证明了所提出的方案面对 2 类强敌手在适应性选择消息、选择身份攻击下的前向安全强不可伪造性 FSU-AMAIA.本文方案的安全性建立在不诚实用户和恶意密钥生成中心的基础上,较之已有方案中的外部敌手模型,安全性更高.最后,通过对比分析,证明了本文提出的前向安全无证书签名方案具有较好的安全性与实用性.

本文提出的 ST_LFC_SIG 签名方案是第 1 个基于随机格的标准模型下可证安全的无证书数字签名方案,并结合了前向安全性以抵御密钥泄露的威胁.

由于本文提出的 2 个无证书签名方案主要是基于随机格进行方案构造,因此依然存在改进的空间,一个潜在的思路是采用理想格替代随机格优化存储空间,但是标准模型下基于理想格的签名方案的安全性证明是目前一个研究难点.因此我们下一步的研究目标将集中在设计基于理想格的前向安全无证书签名方案,以提高方案的整体效率.

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [G] //LNCS 196: Proc of the CRYPTO 1984. Berlin: Springer, 1985: 47-53

[2] Yao Yanqing, Li Zhoujun. A novel fuzzy identity based signature scheme based on the short integer solution problem [J]. Computers and Electrical Engineering, 2014, 40(6): 1930-1939

[3] Wei Baodian, Du Yusong, Zhang Huang, et al. Identity-based threshold ring signature from lattices [G] //LNCS 8792: Proc of the 8th Int Conf on Network and System Security. Berlin: Springer, 2014: 233-245

[4] Tian Miaomiao. Identity-based proxy re-signatures from lattices [J]. Information Processing Letters, 2015, 115(4): 462-467

[5] Kim K S, Hong D W, Jeong I R. Identity-based proxy signature from lattices [J]. Journal of Communications and Networks, 2013, 15(1): 1-7

[6] Al-Riyami S, Paterson K G. Certificateless public key cryptography [G] //LNCS 2894: Proc of the ASIACRYPT 2003. Berlin: Springer, 2003: 452-473

[7] Yu Yong, Mu Yi, Wang Guilin, et al. Improved certificateless signature scheme provably secure in the standard model [J]. Information Security IET, 2012, 6(2): 102-110

[8] Guan Chaowen, Weng Jian, Deng R H, et al. Unforgeability of an improved certificateless signature scheme in the standard model [J]. Information Security IET, 2014, 8(5): 273-276

[9] Yeh K H, Tsai K Y, Fan C Y. An efficient certificateless signature scheme without bilinear pairings [J]. Multimedia Tools and Applications, 2015, 74(16): 6519-6530

[10] Chen Hu, Zhu Changjie, Song Rushun. Efficient certificateless signature and group signature schemes [J]. Journal of Computer Research and Development, 2010, 47(2): 231-237 (in Chinese)
(陈虎, 朱昌杰, 宋如顺. 高效的无证书签名和群签名方案[J]. 计算机研究与发展, 2010, 47(2): 231-237)

[11] Du Hongzhen, Wen Qiaoyan. Security analysis of two certificateless short signature schemes [J]. Information Security IET, 2014, 8(4): 230-233

[12] Choi K, Park J H, Lee D H. A new provably secure certificateless short signature scheme [J]. Computers & Mathematics with Applications, 2011, 61(7): 1760-1768

[13] Huang X, Mu Y, Susilo W, et al. Certificateless signatures: New schemes and security models [J]. Computer Journal, 2012, 55(4): 457-474

[14] Tso R, Huang X, Susilo W. Strongly secure certificateless short signatures [J]. Journal of System & Software, 2012, 85(6): 1409-1417

[15] Chen Yuchi, Tso R, Horng G, et al. Strongly secure certificateless signature: Cryptanalysis and improvement of two schemes [J]. Journal of Information Science and Engineering, 2015, 31(1): 283-296

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

[17] Kim K S, Jeong I R. A new certificateless signature scheme under enhanced security models [J]. Security and Communication Networks, 2015, 8(5): 801-810

[18] Tian Miaomiao, Huang Liusheng. Certificateless and certificate-based signatures from lattices [J]. Security and Communication Networks, 2015, 8(8): 1575-1586

[19] Bellare M, Boldyreva A, Palacio A. An uninstantiable random oracle-model scheme for a hybrid-encryption problem [G] //LNCS 3027: Proc of the EUROCRYPT 2004. Berlin: Springer, 2004: 171-188

[20] Zhang Xiaojun, Xu Chunxiang, Jin Chunhua, et al. Efficient forward secure identity-based shorter signature from lattice [J]. Computers and Electrical Engineering, 2013, 40(6): 1963-1971

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

[22] Yu Jia, Hao Rong, Kong Fanyu, et al. Forward-secure identity-based signature: Security notions and contribution [J]. Information Sciences, 2011, 181(3): 648-660

[23] Ebri N, Baek J, Shou F A. Forward-secure identity-based signature: New generic constructions and their applications [J]. Journal of Wireless Mobile Network, 2013, 4(1): 32-54

[24] Yu Jia, Kong Fanyu, Hao Rong, et al. A note on a forward secure threshold signature scheme from bilinear pairings [J]. Journal of Computer Research and Development, 2010, 47(4): 605-612 (in Chinese)
(于佳, 孔凡玉, 郝蓉, 等. 一个基于双线性映射的前向安全门限签名方案的标注[J]. 计算机研究与发展, 2010, 47(4): 605-612)

[25] Wei Jianghong, Liu Wenfen, Hu Xuexian. Forward-secure ciphertext-policy attribute-based encryption scheme [J]. Journal on Communications, 2014, 35(7): 38-45 (in Chinese)
(魏江宏, 刘文芬, 胡学先. 前向安全的密文策略基于属性加密方案[J]. 通信学报, 2014, 35(7): 38-45)

[26] Rückert M. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles [G] //LNCS 6061: Post-Quantum Cryptography. Berlin: Springer, 2010: 182-200

[27] Li Jiguo, Li Yanqiong, Zhang Yichen. Forward secure certificateless proxy signature scheme [G] //LNCS 7873: Proc of the 7th Int Conf on Network and System Security. Berlin: Springer, 2013: 350-364

[28] Lyubashevsky V. Lattice signatures without trapdoors [G] // LNCS 7237: Proc of the EUROCRYPT 2012. Berlin: Springer, 2012: 738-755

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

[30] Alwen J, Peikert C, et al. Generating shorter bases for hard random lattices [J]. Theory of Computer Systems, 2011, 48(3): 535-553

[31] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions [C] //Proc of the 14th Annual ACM Int Symp on Theory of Computing. New York: ACM, 2008: 197-206

[32] Agrawal S, Boneh D, Boyen X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE [G] //LNCS 6223: Advances in Cryptology (CRYPTO 2010). Berlin: Springer, 2010: 98-115

[33] Yu Chichen, Tso R. A survey on security of certificateless signature schemes [J]. IETE Technical Review, 2016, 33(2): 115-121

Xu Qian, born in 1986. PhD candidate. His main research interests include cryptography, cloud computing security and industrial control safety.

Tan Chengxiang, born in 1965. Professor and PhD supervisor. His main research interests include information security, cloud computing security and applied cryptography (Jerrytan@tongji.edu.cn).

Feng Jun, born in 1985. PhD candidate. His main research interests include security measure, security audit and mobile security (109056396@qq.com).

Fan Zhijie, born in 1982. PhD candidate. His main research interests include cyber security, cloud computing security and mobile security (1310898@tongji.edu.cn).

Zhu Wenye, born in 1991. PhD candidate. His main research interests include information security, security measure and mobile security (1549160994@qq.com).