小 型 微 型 计 算 机 系 统
Journal of Chinese Computer Systems
DOI:10.20009/j.cnki.21-1106/TP.2025-0015
2026 年 2 月 第 2 期
Vol.47 No.2 2026

理想格上的动态前向安全群签名方案研究

王 璐[1],朱晓军[1],王 龙[2],杨倩倩[2]

[1](太原理工大学 计算机科学与技术学院(大数据学院),太原 030000)
[2](晋中信息学院 大数据学院,山西 晋中 030800)
E-mail:wangluua@163.com

摘 要:针对现有的基于格的群签名方案的研究中存在的计算和存储开销大、成员加入与撤销不灵活和密钥暴露后安全性难保证等问题,提出了一种理想格上的动态前向安全群签名方案.首先,理想格的应用能够有效降低签名的计算和存储开销;其次,Ducas-Micciancio 签名方案和 VLR 机制相结合能够实现方案的完全动态性,支持成员灵活加入和撤销,其中针对 VLR 机制的存在的匿名性问题,利用 PKE 设置额外密钥对能够实现方案的完全匿名性;最后引入盆景树技术,通过周期性的密钥更新能够实现方案的前向安全性,保证密钥暴露后的安全性.在 RSIS 和 RLWE 困难假设下,证明了该方案的安全性.

关 键 词:群签名;理想格;完全动态性;前向安全性;完全匿名性
中图分类号:TP309 **文献标识码**:A **文 章 编 号**:1000-1220(2026)02-0458-10

Research on Dynamic Forward Secure Group Signature Scheme on Ideal Lattice

WANG Lu[1],ZHU Xiaojun[1],WANG Long[2],YANG Qianqian[2]
[1](School of Computer Science and Technology (Big Data College),Taiyuan University of Technology,Taiyuan 030000,China)
[2](School of Big Data,Jinzhong University of Information Technology,Jinzhong 030800,China)

Abstract:A dynamic forward secure group signature scheme on ideal lattice is proposed to address the problems of high computational and storage overhead,inflexible member enrollment and revocation,and difficulty in ensuring security after key exposure in existing lattice-based group signature schemes Firstly,the application of ideal lattices can effectively reduce the computational and storage costs associated with signatures. Secondly,the combination of the Ducas-Micciancio signature scheme and the VLR mechanism enables full dynamicity in the scheme,supporting flexible member enrollment and revocation. To address the anonymity issue inherent in the VLR mechanism,the use of an additional key pair set up through PKE ensures complete anonymity in the scheme. Finally,the introduction of the Merkle Tree technology,through periodic key updates,achieves forward security in the scheme,ensuring security even after key exposure. The security of this scheme is proven under the hardness assumptions of RSIS and RLWE.

Keywords:group signature;ideal-lattice;fully-dynamism;forward-security;fully-anonymity

0 引 言

群签名是 Chaum 和 van Heyst[1] 提出的一种数字签名方案,允许用户代表整个群组对消息进行签名,并设有追踪机构识别签名的用户身份,实现了可追溯性和匿名性的平衡.群签名适用于匿名在线通信、隐私保护、数字版权管理、电子政务和军事等多领域[2].但是传统群签名方案的安全性基于经典密码学的难度假设,这些假设可以在多项式时间内被量子计算攻破[3].相比之下,Regev[4] 等人提出的基于格的密码学展现了具有效的量子抵抗性.近些年来,越来越多的研究者将基于格的密码学引入群签名方案的设计中,以提高方案的量子安全性.由此可见,随着后量子时代的到来,基于格的群签名方案研究已成为新的研究趋势.

在基于格的群签名方案研究中,研究者们从方案的动态性、匿名性和安全性等角度深入探索.Ling[5] 等人通过引入理想格的概念,首次提出了签名大小恒定的群签名方案.Luo[6] 等人在此基础上采用签名混合加密方法代替零知识证明,构建出了更高效、更精准的群签名算法.Canard[7] 等人引入盆景树技术,在签名大小恒定的基础上为签名增添了前向安全性.然而,上述方案在成员加入或离开时需重新初始化群组,未能实现完全动态性.

针对方案不能灵活加入和撤销成员的问题,Ling[8] 等人引入了首个基于格的动态群签名方案,但是用户撤销时需更新 Merkle 哈希树,导致计算复杂且耗时.Perare[9] 等人引入了 VLR 机制,通过吊销令牌实现成员撤销.目前的 VLR 机制都只满足较弱的无私匿名,无法抵抗用户签名密钥的泄漏.Abhilash[10] 等人提出基于限时签名密钥的撤销技术,利用时间戳技术对 VLR 机制进行改进,但仍未实现完全匿名性.

综上所述,目前基于格的群签名方案中还没有能够同时兼顾动态性、匿名性、安全性和计算开销等多方面要素的方

收稿日期:2025-01-08 收修改稿日期:2025-02-24 基金项目:中央引导地方科技发展资金项目(YDZJSX2022C004)资助;国家自然科学基金项目(U21A20469)资助;山西省自然科学面上项目(202203021211144)资助. 作者简介:**王 璐**,女,1999 年生,硕士研究生,CCF 学生会员,研究方向为密码学技术;**朱晓军**(通信作者),男,1977 年生,博士,副教授,CCF 会员,研究方向为网络安全;**王 龙**,男,1988 年生,博士,副教授,研究方向为网络安全;**杨倩倩**,女,1988 年生,博士,副教授,研究方向为网络安全.

案.因此本文提出了理想格上的动态前向安全群签名方案研究(Dynamic Forward-secure Group Signature,DFSGS),本文的主要贡献如下:

1) 提出一个基于理想格的群签名方案,其公钥、用户密钥和签名大小和用户数量无关,减少了存储开销.方案基于RSIS 和 RLWE 假设的难度,在量子计算攻击下是安全的.

2) 构建了一个完全动态的基于格的群签名方案,支持成员加入和撤销,提高了算法的灵活性.

3) 群组成员撤销采用 VLR 机制来实现,利用 PKE 为用户设置额外密钥对来添加撤销功能,底层 PKE 方案的密钥隐私性可以保证方案的完全匿名性.

4) 引入了盆景树技术,利用理想格上的 $TrapGen_{R_q}$算法、$SampleD_{R_q}$算法、$DelBasis_{R_q}$算法实现密钥生成和更新,在理想格的基础上为方案提供了前向安全性.

1　预备知识

1.1　格上相关知识

定义 1.(格):设 $b_1,b_2,\cdots,b_m$ 是 $\mathbb{R}^n$ 上线性无关向量的集合,则格定义为这些向量的整系数向量组合,即:$\Lambda=\{\sum_i^m b_i\cdot x_i : x_i\in\mathbb{Z}, i\in[m]\}$,$b_1,b_2,\cdots,b_m$ 为 Λ 的一组基.

定义 2.(系数映射 τ):将环元素 $v=v_0+v_1\cdot x+\cdots+v_{n-1}\cdot x^{n-1}\in R_q$ 映射到向量 $\tau(v)=(v_0,v_1,\cdots,v_{n-1})^{\mathrm{T}}\in\mathbb{Z}_q^n$.

定义 3.(环同态映射 rot):将环上的矩阵 $A=[a_1|\cdots|a_m]\in R_q^{1\times m}$ 映射到矩阵 $rot(A)=[rot(a_1)|\cdots|rot(a_m)]\in\mathbb{Z}_q^{n\times mn}$.

定义 4.(RSIS 问题[11,12]):给定一个随机均匀矩阵$A=[a_1|\cdots|a_m]\in R_q^{1\times m}$,找到一个非零向量 $x=(x_1,\cdots,x_m)^{\mathrm{T}}\in R^m$ 使得 $A\cdot x=a_1\cdot x_1+\cdots+a_m\cdot x_m=0$ 且 $\|x\|_\infty\leq\beta$.

定义 5.(RLWE 问题[13]):给定 $n,m\geq1,q\geq2$ 和 R 上的一个概率分布 χ,对于 $s\in R_q$,随机选取 $a\leftarrow R_q$ 和 $e\leftarrow\chi$,定义分布 $A_{s,\chi}$并输出$(a,a\cdot s+e)\in R^q\times R^q$.

1.2　整数分解

在签名方案中使用到了整数分解函数 $rdec$[5].对于任何 $B\in Z^+$,定义:

$$\delta_B=\lfloor\log_2 B\rfloor+1=\lceil\log_2(B+1)\rceil$$

则 $rdec_B: R_q\rightarrow R^{\delta_B}$是一个内射函数,将 $p\in R_q$ 映射到$\boldsymbol{p}\in R^{\delta_B}$,其中 $\|\boldsymbol{p}\|_\infty\leq B$, $\|p\|_\infty\leq1$. 当 $B=\frac{q-1}{2}$时,用 $rdec$ 来代替 $rdec_{\frac{q-1}{2}}$.

1.3　相关算法

最大奇异值 $s_1(R)$决定了陷门 R 的质量.给定安全参数 n,素数 $q=poly(n)$,$m\geq2n\log q$,存在算法:

引理 1.($TrapGen_{R_q}$算法[14,15]):给定一个均匀矩阵 $A'\in R_q^{1\times m}$,可逆标签 $I\in R_q$ 和 $\sigma=\omega(\sqrt{\log n})$,存在多项式时间算法 $TrapGen_{R_q}(A',I,\sigma)\rightarrow(A,R)$,其中 $A\in R_q^{1\times(m+k)}$,$R\in Rq_q^{m\times k}$,R 为矩阵 A 的 G-陷门.

引理 2.($SampleD_{R_q}$算法[16]):输入矩阵 $A\in R_q^{1\times(m+k)}$,A 的 G-陷门 $R\in Rq_q^{m\times k}$,任意向量 $z\in R_q$ 和参数 $\sigma>\omega(\sqrt{\log n})\cdot s_1(R)$,存在多项式时间算法 $SampleD_{R_q}(A,R,z,\sigma)$,输出在统计上接近分布 $D_{\Lambda^z(A),\sigma}$的向量 $b\in\Lambda^z(A)$.

引理 3.($DelBasis_{R_q}$算法[17]):输入矩阵 $A\in R_q^{1\times(m+k)}$,A 的 G-陷门 $R\in R_q^{m\times k}$ 和参数 $\sigma>\omega(\sqrt{\log n})\cdot s_1(R)$,令 $A'\in R_q^{1\times(m'+k)}$ 为包含矩阵 A 的任意矩阵,且 $m'\geq m+k$,存在多项式时间算法 $DelBasis_{R_q}(R,A')$,输出 A'的 G-陷门 $R'\in R^{m'\times k}$.

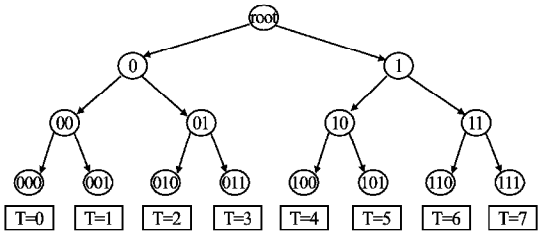

图 1　盆景树结构

Fig. 1　Bonsai tree structure

引理 4.(盆景树算法[18]):对于 $d\in\mathbb{Z}^+$,将整个过程的执行时间划分为 $T=2^d$ 个周期.当 $k\in[1,d+1]$,$t\in[0,T-1]$,定义深度 k 处的右兄弟节点 $Sibling(k,t)$.对于目标叶结点,求从根到叶结点的路径节点,生成节点集 $Nodes(t\rightarrow T-1)$,由$\{sibling(1,t),\cdots,sibling((d+1),t)\}$组成,如图 1 所示.

2　方案定义及安全模型

一个基于格的动态群签名方案包括 8 个算法:

1) $KeyGen(\lambda,T)$:给定安全参数 λ 和时间段 T,生成群公钥 gpk、群管理员密钥 ik 和追踪密钥 ok.将 ik 发给群管理员 GM,将 ok 发给追踪机构 TM,并将 gpk 公开.

2) $UKeyGen(\lambda)$:想要成为群成员的用户运行此算法以获得个人密钥对(usk,upk).

3) $<Join,Iss>$:新用户 U_p 运行此算法和 GM 交互来加入群.该算法在接收到输入 gpk、ik 和成员公钥 p 时,向新用户颁发证书 $cert_p$,并输出成员密钥 gsk_p 和撤销令牌 grt_p.然后将注册信息记录在注册表 reg 中.

4) $KeyUpdate(gpk,gsk_t[p],t+1)$:输入 $gpk,gsk_t[p]$和 $t+1$,其中 $gsk_t[p]$和是用户 U_p 在时间 t 时的签名密钥,输出 U_p 在时间 $t+1$ 时的签名密钥 $gsk_{t+1}[p]$.

5) $Revoke(gpk,ik,RU)$:输入 gpk,ik 和吊销用户列表 RU 时,算法根据列表 RU 中的用户更新吊销令牌列表 RL,输出吊销令牌列表 RL.

6) $Sign(gpk,gsk_t[p],M,t)$:输入 gpk、$gsk_t[p]$、消息 M 和当前时间 t,返回消息 M 上的用户签名 Σ.

7) $Verify(gpk,M,\Sigma,t)$:该算法输出 0/1,表示用群公钥 gpk 验证 Σ 是否是消息 M 上的有效签名.

8) $Open(gpk,ok,reg,M,\Sigma)$:输入 gpk、(M,Σ) 和 ok,TM 访问注册表 reg,获得成员身份 p.

2.1　正确性

正确性保证诚实的用户可以加入群组.验证算法接受其签名,追踪算法追踪到正确的签名者.即对于所有的$(gpk,ik,ok)\leftarrow KeyGen(\lambda,T)$和$(gsk_p,cert_p)\leftarrow Join$,以及所有的 $M\in\{0,1\}^*$,以下两个等式成立:

$$Verify(gpk,Sign(gpk,usk_t[i],t,M),M,t,RL))=1\Leftrightarrow(grt_p\notin RL)$$

$Open(gpk,ok,t,M,Sign(gpk,usk_t[i],t,M))=p$

2.2 安全性定义

本方案采用 Emura[19] 等人的安全模型，通过帧攻击（不可帧性）、跟踪攻击（前向安全可追溯性）和匿名性攻击（完全匿名性）3 种攻击定义方案中的安全概念. 首先描述敌手$\mathcal{A}$在不同的攻击中可能会访问的共享变量和预言机.

共享变量：

· H_u：该集合包含该群的诚实用户.

· C_u：此集合包含群中被受损用户.

· $Sigs$：此集合包含$\mathcal{A}$所做的所有签名查询.

预言机：

· Add_{user}：此预言机将诚实用户添加到群中. 输入用户 U_p 的身份 p，通过在本地运行 *Join* 算法来计算 gsk_p 和 $cert_p$，然后 p 被保存在 H_u 里.

· Q_{gm}：此预言机中，$\mathcal{A}$作为受损用户 U_p 运行 *Join* 算法进行注册. 最后$\mathcal{A}$会得到 gsk_p 和 $cert_p$. 之后将 p 保存在 C_u 集合中.

· Q_{user}：$\mathcal{A}$作为一个被破坏的 GM，与诚实用户 U_p 参与了 *Join* 协议，之后 p 被保存在 H_u 集合中.

· Get_{reg}：这个预言机将用户身份 p 作为输入并返回 grt_p. 如果在 *reg* 表中找不到 p，则返回 $\perp$.

· G_{sign}：此预言机以用户身份 p，消息 M 作为输入，并将 M 上的签名 Σ 返回给$\mathcal{A}$，然后将(M,Σ)保存在 *Sigs* 集合中.

· Get_{ik}：返回 *ik* 给$\mathcal{A}$.

· Get_{ok}：返回 *ok* 给$\mathcal{A}$.

· $Revoke$：$\mathcal{A}$使用此预言机撤销诚实用户. 预言机输入用户身份 p，并将 grt_p 保存在 *RL* 中.

· Get_{gsk}：这个预言机将用户身份 p 作为输入并将$(gsk_p, cert_p)$返回给$\mathcal{A}$. p 也保存在 C_u 中. 如果这样的 p 不存在，它将返回 $\perp$.

给定安全参数 λ 和时间段 T，定义以下的安全实验：

定义 6.（前向安全可追溯性）：如果在实验 $Exp_{\mathcal{A}}^{FS-trace}(\lambda,T)$，所有 PPT 敌手$\mathcal{A}$最多以可忽略不计的优势赢得前向安全可追溯性挑战，即 $Adv_{DFSGS,\mathcal{A}}^{FS-trace}=Pr[Exp_{\mathcal{A}}^{FS-trace}(\lambda,T)=1]$，则 DFSGS 方案满足前向安全可追溯性要求，如表 1 所示.

定义 7.（不可帧性）：如果在实验 $Exp_{\mathcal{A}}^{non-frame}(\lambda,T)$，所有 PPT 敌手$\mathcal{A}$ 最多以可忽略不计的优势赢得不可帧性挑战，即 $Adv_{DFSGS,\mathcal{A}}^{non-frame}=Pr[Exp_{\mathcal{A}}^{non-frame}(\lambda,T)=1]$，则 DFSGS 方案满足不可帧性要求，如表 2 所示.

定义 8.（完全匿名性）：如果在实验 $Exp_{\mathcal{A}}^{anon-b}(\lambda,T)$，所有 PPT 敌手$\mathcal{A}$最多以可忽略不计的优势赢得完全匿名性挑战，即 $Adv_{DFSGS,\mathcal{A}}^{non-frame}=\left|Pr[Exp_{\mathcal{A}}^{anon-b}(\lambda,T)=1]-\frac{1}{2}\right|$，则 DFSGS 方案满足完全匿名性要求，如表 3 所示.

2.3 基于格的动态群签名

$KeyGen(\lambda,T)$：给定安全参数 λ，进行如下操作：

1. 选择正整数 k、$n=\tilde{\mathcal{O}}(\lambda)$、模数且 $q=\tilde{\mathcal{O}}(n^4)$ 且 $q=3^k$、$m\geqslant 2\lceil\log q\rceil+2$，$\tilde{m}=m+k$，$\ell=\lfloor\log\frac{q-1}{2}\rfloor+1$，对于 $d_0\in\mathbb{Z}_+$，总时间段数 $T=2^{d_0}$，给定多项式环$\mathcal{R}=\mathbb{Z}[X]/(X^n+1)$，$\mathcal{R}_q=\mathcal{R}/q\mathcal{R}$. 并选择整数界 $\beta=\tilde{\mathcal{O}}(n)$ 和 $B=\tilde{\mathcal{O}}(n^{5/4})$，设$\chi$是$\mathcal{R}$上以 B 为边界的分布.

表 1 前向安全可追溯性定义

Table 1 Definition of forward security traceability

前向安全可追溯性：$Exp_{\mathcal{A}}^{FS-trace}(\lambda,T)$
$(gpk,ik,ok)\leftarrow KeyGen(\lambda,T);C_u,Sigs\leftarrow\varnothing;$
$(t^*,M^*,\Sigma^*,RL_{t^*}{}^*)\leftarrow\mathcal{A}(Get_{ok},Q_{gm},Get_{usk},Get_{reg},Update_{key},Revoke,G_{sign});$
if $Verify(gpk,M^*,\Sigma^*,t^*,RL_{t^*}{}^*)=0$ *or* $(M^*,\Sigma^*)\in Sigs$,
then output 0;
$p^*\leftarrow Open(gpk,ok,M^*,\Sigma^*,reg);$
if $(p^*\notin C_u)$ *or* $(p^*\in C_u$ *and* $\mathcal{A}$ *only queried* $gsk_t[p^*]$ *for* $t>t^*)$,
then output 1, *else output* 0;

表 2 不可帧性定义

Table 2 Definition of unframeability

不可帧性：$Exp_{\mathcal{A}}^{non-frame}(\lambda,T)$
$(gpk,ik,ok)\leftarrow KeyGen(\lambda,T);H_u,C_u,Sigs\leftarrow\varnothing;$
$(t^*,M^*,\Sigma^*,RL_{t^*}^*,p^*)\leftarrow\mathcal{A}(Q_{user},Get_{ik},Get_{usk},Get_{reg},G_{sign});$
if $Verify(gpk,M^*,\Sigma^*,t^*,RL_{t^*}^*)=0$ *or* $(M^*,\Sigma^*)\in Sigs$,
then output 0;
$p^*\leftarrow Open(gpk,ok,M^*,\Sigma^*,reg);$
if $p^*\in H_u$ *and* $p^*\notin C_u$; *then output* 1, *else output* 0;

表 3 完全匿名性定义

Table 3 Definition of complete anonymity

完全匿名性：$Exp^{anon-b}(\lambda,T)$
$(gpk,ik,ok)\leftarrow KeyGen(\lambda,T);$
$(aux,M^*,p_o,p_1,t^*)\leftarrow\mathcal{A}(play;Add_{user},G_{sign},Get_{usk},Revoke);$
if $(p_0\in C_u)$ or $(p_1\in C_u)$,
then output 0;
$b\leftarrow\{0,1\},\Sigma^*\leftarrow Sign(gpk,M^*,t^*,gsk_{p_b});$
$b'\leftarrow\mathcal{A}(guess,aux,\Sigma^*:Add_{user},G_{sign},Get_{usk},Revoke);$
if $b=b'$, *then return* 1, *else output* 0;

2. 选择实数 $c>1$，$\alpha_0>\frac{1}{c-1}$，整数 $d\geqslant log_c(\omega(\log n))$，对于 $i\in[d]$，计算 $c_0=0$，$c_i=\lfloor\alpha_0 c^i\rfloor$ 的严格递增序列 $\{c_1,c_2,\cdots,c_d\}$. 定义 $\tau_i=\{0,1\}^{c_i}$，将可将任意标签 $h\in\tau_d$ 与环元素关联为 $h(X)=\sum_{j=0}^{c_d-1}h_jX^j\in\mathcal{R}_q$. 令 $h_{[i]}=(h_{c_{i-1}},\cdots,h_{c_i-1})^{\mathrm{T}}$，则 $h=(h_{[1]}\|h_{[2]}\|\cdots\|h_{[d]})$.

3. 设$\mathcal{H}_{FS}:\{0,1\}^*\rightarrow\{1,2,3\}^\kappa$，其中 $\kappa=\omega(\log\lambda)$，$\mathcal{H}_1=\{0,1\}^*\rightarrow\mathcal{R}_q^\ell$，是抗碰撞的哈希函数，在 Fiat-Shamir 变换中被建模为一个随机预言机.

4. 设 COM 为统计隐藏和计算绑定承诺方案，用于方案的零知识论证系统.

5. 采样一个均匀随机矩阵 $\mathbf{B}\in\mathcal{R}_q^{1\times m}$.

6. 对于所有的 $i\in[d_0]$ 和 $j\in\{0,1\}$，选择 $u_0\in\mathcal{R}_q$，$A_i^j\in\mathcal{R}_q^{1\times m}$.

7. 设高斯参数 $s_{d_0}=\tilde{\mathcal{O}}(\sqrt{nd_0\log q})\cdot\omega(\sqrt{\log n})$，用于生成短样本向量.

8. 生成验证密钥 $A, F_0 \in \mathcal{R}_q^{1\times\bar{m}}; A_{[0]}, \cdots, A_{[d]} \in \mathcal{R}_q^{1\times k}; F, F_1 \in \mathcal{R}_q^{1\times\ell}; u \in \mathcal{R}_q$. 均匀选择 $A' \in \mathcal{R}_q^{1\times m}, I \in \mathcal{R}_q$ 是可逆标签, $o = \omega(\sqrt{\log n})$, 运行陷门算法 $(A, R) \leftarrow TrapGen_{\mathcal{R}_q}(A', I, \sigma)$, 其中 $A \in \mathcal{R}_q^{1\times\bar{m}}, R \in \mathcal{R}_q^{m\times k}$, 则 R 为 Ducas-Micciancio 签名方案的签名密钥.

9. 采样 $s_1, s_2 \leftarrow \chi, e_1, e_2 \leftarrow \chi^{\ell}$, $a \in \mathcal{R}_q^{\ell}$ 并计算 $b_1 = a \cdot s_1 + e_1 \in \mathcal{R}_q^{\ell}$; $b_2 = a \cdot s_2 + e_2 \in \mathcal{R}_q^{\ell}$, 其中, χ、χ' 分别为 $\mathcal{R}_q$、$\mathcal{R}_q^{\ell}$ 上的分布.

10. 设置公共参数 pp、组公钥 gpk、GM 密钥 ik 和 TM 密钥 ok 如下所示:

$$pp = \{n, q, k, \mathcal{R}, \mathcal{R}_q, \ell, m, \bar{m}, \chi, d, d_0, c_0, \cdots, c_d, B, \beta, \kappa, \mathbf{B}, s_{d_0}\}$$

$$gpk = \{pp, A, \{A_{[i]}\}_{i=0}^{d}, \{A_j^0, A_j^1\}_{j=1}^{d_0}, F, F_0, F_1, u, u_0, a, b_1, b_2\}$$

$$ik = R; ok = (s_1, e_1)$$

可信方将 gpk 公开, 并发送 ik 到 GM, 发送 ok 给 TM. GM 收到 ik 后, 初始化其内部状态 $S = 0$ 和注册表 reg.

$UKeyGen(gpk)$: 用户 U_p. 采样 $x \in \mathcal{R}^{m}$, 其系数在集合 $\{-1, 0, 1\}$ 中随机均匀选择. 然后计算 $p = \mathbf{B} \cdot x \in \mathcal{R}_q$. 设置 $upk = p$ 和 $usk = x$.

$<Join, Iss>$: 当接收到公钥为 $upk = p$ 的用户 U_p 的加入请求时, GM 验证 upk 之前是否被注册过, 若没有被使用过, 则进行如下操作.

1. 采样 $\bar{s} \leftarrow \chi, \bar{e} \leftarrow \chi^{\ell}$, $\bar{a} \in \mathcal{R}_q^{\ell}$, 并计算 $\bar{b} = \bar{a} \cdot \bar{s} + \bar{e} \in \mathcal{R}_q^{\ell}$, 设置吊销令牌 $grt_p = (\bar{s}, \bar{e}, p)$.

2. 确定节点集确定节点集 $Nodes(0 \rightarrow T-l)$, 对于 $Nodes(0 \rightarrow T-1)$, 如果 $z = \perp$, 则令 $usk_0[z] = \perp$. 否则用 d_z, 表示 z 的长度, $d_z \leqslant d_0$, 计算矩阵:

$$A_z = [A \mid A_1^{z[1]} \mid A_2^{z[2]} \mid \cdots \mid A_{d_z}^{z[d_z]}] \in \mathcal{R}_q^{1\times((d_z+l)m+k)}$$

(i) 如果 z 的长度为 d_0:

$v_2 \leftarrow SampleD_{\mathcal{R}_q}(DelBasis_{\mathcal{R}_q}(R, A_z), u_0, s_{d_0})$, 设:

$$usk_0[p][z] = v_z$$

(ii) 如果 z 的长度小于 d_0:

$R_z \leftarrow DelBasis_{\mathcal{R}_q}(R, A_z)$, 设 $usk_0[p][z] = R_z$

令 $usk_0[p] = \{usk_0[p][z], z \in Nodes(0 \rightarrow T-1)\}$.

3. 设置标签 $h = (h_0, h_1, \cdots, h_{c_d-1})^{\mathrm{T}} \in \tau_d$, $S = \sum_{j=0}^{c_d-1} 2^j \cdot h_j$, 计算:

$$A_h = [A \mid A_{[0]} + \sum_{i=1}^{d} h_{[i]} A_{[i]}] \in \mathcal{R}_q^{1\times(m+k)}$$

4. 用签名密钥 R 在消息 $rdec(p) \in \mathcal{R}^{\ell}$ 上生成 Ducas-Micciancio 签名 (h, r, v):

(i) 采样 $r \in \mathcal{R}^{\bar{m}}$ 且 $\| r \|_{\infty} \leqslant \beta$ 并计算:

$$w = F \cdot rdec(F_0 \cdot r + F_1 \cdot rdec(p)) \in \mathcal{R}_q$$

(ii) 运行算法:

$$SampleD_{\mathcal{R}_q}(DelBasis_{\mathcal{R}_q}(R, A_h), w + u, \sigma)$$

生成 $v \in \mathcal{R}^{(\bar{m}+k)}$ 使得:

$$A_h \cdot v = w + u, \text{且} \| v \|_{\infty} \leqslant \beta, \| r \|_{\infty} \leqslant \beta$$

5. GM 设成员证书 $cert_p = (h, r, v)$, 并发送给用户. 群用户的签名密钥设置为 $gsk_0[p] = (usk_0[p], x, \bar{a}, \bar{b}, cert_p)$, GM 存储 $reg[S] = (grt_p, p)$, 并将 S 更新为 $S+1$.

KeyUpdate$(gpk, gsk[p], t+l)$: 根据 U_p 在时刻 t 的密钥 $usk_t[p] = \{usk_t, [p][z], z \in Nodes(t \rightarrow T-1)\}$ 确定节点集 $Nodes(t+l \rightarrow T-l)$. 对于 $z' \in Nodes(t+l \rightarrow T-1)$, 如果 $z' = \perp$, 设置 $usk_{t+1}[p][z'] = \perp$. 如果 $z' \neq \perp$, 其前缀恰好存在一个 $z \in Nodes(t \rightarrow T-1)$, 例如对于某个后缀 y, $z' = z \| y$, 考虑以下两种情况:

1. 若 $z' = z$, 令 $usk_{t+1}[p][z'] = usk_t[p][z]$.

2. 若 $z' = z \| y$ 且 y 非空, 令 $usk_t[p][z] = R_z$. 则:

(i) 如果 z' 长度为 d_0:

$v_2, \leftarrow SampleD_{\mathcal{R}_q}(DelBasis_{\mathcal{R}_q}(R_z, A_z), u_0, s_{d_0})$, 设

$$usk_{t+1} + [p][z'] = v_{z'}$$

(ii) 如果 z' 长度小于 d_0:

$R_{z'}, \leftarrow DelBasi_{\mathcal{R}_q}(R_z, A_{z'})$, 设 $usk_{t+1}[p][z'] = R_{z'}$, $usk_{t+1}[p] = \{usk_{t+1}[p][z'], z' \in Nodes(t+l \rightarrow T-1)\}$.

输出更新后的成员密钥:

$$gsk_{t+1}[p] = (usk_{t+1}[p], x, \bar{a}, \bar{b}, cert_p)$$

$Revoke(gpk, ik, RU)$: GM 从撤销成员列表 RU 中获得已撤销成员的吊销令牌 grt_p. 将 grt_p. 添加到成员吊销令牌列表 RL, 并将其更新为非活动状态. 返回 RL. $Sign(gpk, gsk_t[p], M)$: 拥有公钥 $p \in \mathcal{R}_q$. 的群成员按照如下步骤进行签名.

1. 对于消息 $M \in \{0,1\}^{*}$, 令 $\delta = \mathcal{H}_1(M) \in \mathcal{R}_q^{\ell}$, 采样 $\bar{g} \leftarrow \chi, e_3 \leftarrow \chi^{\ell}$ 和 $e_4 \leftarrow \chi^{\ell}$ 并对 δ 进行加密:

$$\bar{c} = (\bar{c_1}, \bar{c_2}) = (\bar{a} \cdot \bar{g} + e_3, \bar{b} \cdot \bar{g} + e_4 + \lfloor q/4 \rfloor \cdot \delta) \in \mathcal{R}_q^{\ell} \times \mathcal{R}_q^{\ell}$$

2. 为环向量 $rdec(p) \in \mathcal{R}_q^{\ell}$. 进行两次加密, 即对于每个 $i \in \{1,2\}$, 采样 $g_i \leftarrow \chi, e_{i,1} \leftarrow \chi^{\ell}$ 和 $e_{i,2} \leftarrow \chi^{\ell}$ 进行采样并计算:

$$c_i = (c_{i,1}, c_{i,2}) = (a \cdot g_i + e_{i,1}, b_i \cdot g_i + e_{i,2} + \lfloor q/4 \rfloor \cdot rdec(p)) \in \mathcal{R}_q^{\ell} \times \mathcal{R}_q^{\ell}$$

3. 生成一个 NIZKAoKΠ_{gs}来证明拥有有效元组:

$$\zeta = (h, r, v, x, p, \bar{g}, g_1, g_2, e_3, e_4, e_{1,1}, e_{2,1}, e_{1,2}, e_{2,2}, \nu_z)$$

使以下条件成立:

(i) 成员证书是在用户身份上的正确签名.

(ii) $\mathbf{B} \cdot x = p$ 并且 $\| x \|_{\infty} \leqslant 1$.

(iii) 密文 $\bar{c}$ 是 $\mathcal{H}_1(M)$ 的正确加密.

(iv) 密文 c_1, c_2 是 $rdec(p)$ 分别在 $g_1, e_{1,1}, e_{1,2}$ 和 $g_2, e_{2,1}, e_{2,2}$ 下的正确加密.

(v) 签名密钥根据时间正确更新.

该协议是 Ducas-Micciancio 签名协议的扩展, 其中证明者额外证明了声明(iii)和(v). 该协议重复 $\kappa = \omega(\log\lambda)$ 次以实现可忽略的可靠性误差, 并通过 Fiat-Shamir 将其转换为非交互式:

$$\Pi_{gs} = (\{CMT_i\}_{i=1}^{\kappa}, CH, \{RSP_i\}_{i=1}^{k})$$

其中:

$$CH = (ch_1, \cdots, ch_{\kappa},) = \mathcal{H}_{FS}(\{CMT_i\}_{i=1}^{\kappa}, M, \xi)$$

$$\xi = (A, \{A_{[i]}\}_{i=0}^{d}, \{A_j^0, A_j^1\}_{j=1}^{d_0}, F, F_0, F_1, u_0, u, \mathbf{B}, t, \bar{c}, c_1, c_2, a, b_1, b_2, \bar{a}, \bar{b})$$

输出群签名 $\sum = (\bar{c}, c_1, c_2, \prod_{gs})$.

$Verify(gpk, M, \sum, t)$: 给定输入, 该算法进行如下操作.

1. 把签名 $\sum$ 解析为:

$\sum = (\bar{c}, c_1, c_2, \{CMT_i\}_{i=1}^{\kappa}, (Ch_1, \cdots, Ch_{\kappa}), \{RSP_i\}_{i=1}^{\kappa})$.

如果 $(Ch_1, \cdots, Ch_{\kappa}) \neq \mathcal{H}_{FS}(M, \{CMT_i\}_{i=1}^{\kappa}, \xi)$ 则返回 0.

2. 对于每个 $i \in [\kappa]$, 运行零知识协议的验证阶段, 检查 RSP_i 相对于 CMT_i, 和 Ch_i, 的有效性. 如果任何条件不成立, 则返回 0.

3. 返回 1.

$Open(gpk,ok,reg,M,\Sigma)$:输入 $ok=(s_1,e_1)$ 和签名 $\Sigma=(\bar{c},c_1,c_2,\prod_{gs})$. 然后,该算法执行以下操作:

1. 使用 s_1 对 $c_1=(c_{1,1},c_{1,2})$ 进行如下解密:

(a)计算 $p''=\dfrac{c_{1,2}-c_{1,1}\cdot s_1}{\lfloor q/4\rfloor}$

(b)对于 p''的每个系数:

(1)如果它更接近于 0 而不是 -1 和 1,则将其四舍五入为 0;

(2)如果它更接近于 -1 不是 0 和 1,则将其四舍五入到 -1;

(3)如果它更接近于 1 而不是 0 和 -1,则将其四舍五入为 1.

(c)将处理后的 p''记为 $p'\in\mathcal{R}_q^{\ell}$,系数为 $\{-1,0,1\}$.

(d)令 $p'\in\mathcal{R}_q$ 使得 $\tau(p')=H\cdot\tau(p')$. $\mathbf{H}\in\mathbb{Z}_q^{n\times n\ell}$ 是 $\mathcal{R}_q$. 中的元素的分解矩阵.

2. 如果 reg 不包含 p',则返回上.

3. 返回 p'.

2.4 零知识论证系统基础

类 stern 协议:设 $q\geqslant 2,D,L$ 为正整数,使得 $L\geqslant D$ 且 $VALID$ 是 $\{-1,0,1\}^L$ 的子集. 设 $\mathcal{S}$ 是一个有限集合,使得每个 $\phi\in\mathcal{S}$ 与 L 个元素的一个排列 Γ_ϕ 相关联,满足条件:

$$\begin{cases} w\in VALID\Leftrightarrow\Gamma_\phi(w)\in VALID \\ w\in VALID\ and\ \phi\ is\ uniform\ in\ \mathcal{S}\Rightarrow\Gamma_\phi,\ is\ uniform\ in\ VALID \end{cases} \tag{1}$$

从而为以下抽象关系构造一个统计的 ZKAok:

$$R_{abstract}=\{(A,u);x\in\mathbb{Z}_q^{D\times L}\times\mathbb{Z}_q^{D}\times VALID;A=u\ mod\ q\} \tag{2}$$

Libert[20] 等人为关系 $R_{abstract}$ 构建了一个 IZK 协议,通过 R'将转换为其抽象形式,得到关系 R'的 IZK 协议.

Ling[5] 等人定义了两个扩展函数 enc、mix 在转换中得到广泛应用,具体定义如下:

1) enc:给定任意一个向量 $a\in\mathbb{Z}^m$,符号 $[a]_3$;用于表示向量 $a'\in\{-1,0,1\}^m$,使得 $a'=a\ mod\ 3$. 对于向量 $z=\{z_1,\cdots,z_m\}\in\{-1,0,1\}^m$,定义了函数:

$$enc(z):z\mapsto u,\text{其中 } u\in\{-1,0,1\}^{3m}$$

给定 $z,e\in\{-1,0,1\}^m$,则具备以下性质:

$$u=enc(z)\Leftrightarrow\pi_e(u)=enc([z+e]_3)$$

其中 π_e. 是定义在向量 u 上的置换.

2) mix:对于任意 $z=\{z_1,\cdots,z_m\}\in\{-1,0,1\}^m$,且 $t=(t_0,t_1,\cdots,t_{c_d-1})\in\{0,1\}^{c_d}$,令:

$$y=(z\parallel t_0\cdot z\parallel\cdots\parallel t_{c_c-1}\cdot z)\in\{0,1\}^{m+mc_d}$$

定义了函数:

$$mix(t,z):y\mapsto v$$

其中:

$$v=\{-1,0,1\}^{3m+6mc_d}$$

令 $t,b\in\{0,1\}^{c_d}$,且 $z,e\in\{-1,0,1\}^m$,则具备以下性质:

$$v=mix(t,z)\Leftrightarrow\Psi_{b,e}(v)=mix(t\oplus b,[z+e]_3)$$

其中 $\Psi_{b,e}$是定义在向量 v 上的置换.

2.5 交互式零知识协议

签名者在生成群签名时将调用统计 IZK. 该协议是 Du-cas-Micciancio 签名协议的扩展,证明者必须证明以下事实,以使验证者相信他是有效的组成员:

1. 签名者 U_p 拥有在用户身份上的签名,即证书 (h,r,v).

2. 签名者 U_p 拥有公钥 $p\in\mathcal{R}_q$ 对应的秘钥 $x\in\mathcal{R}^m$,满足 $\|x\|_\infty\leqslant 1$ 且 $\mathbf{B}\cdot x=p$.

3. 签名者 U_p 正确地将 $\mathcal{H}_1(M)\in\mathcal{R}_q^{\ell}$ 加密为密文 $\bar{c}$.

4. 签名者 U_p 正确加密 $rdec(p)\in\mathcal{R}^{\ell}$ 为密文 c_1 和 c_2.

5. 签名者 U_p 的签名密钥根据时间正确更新.

上述 5 个条件可以定义为关系 R'.

定义 9.

$$R'=(A,\{A_{[i]}\}_{i=0}^{d},\{A_j^0,A_j^l\}_{j=1}^{d_0},F,F_0,F_1,\mathbf{B},x,r,u_0,u,v,h,\bar{c},c_1,c_2,a,b_1,b_2,\bar{a},\bar{b})$$

其中:

$A;F_0\in\mathcal{R}_q^{1\times\bar{m}};A_{[0]},\cdots,A_{[d]}\in\mathcal{R}_q^{1\times k};F,F_1\in\mathcal{R}_q^{1\times\ell}$;

$a,b_1,b_2,\bar{a},\bar{b}\in\mathcal{R}_q^{\ell}$;$u_0,u\in\mathcal{R}_q$;$\mathbf{B}\in\mathcal{R}_q^{1\times m}$;$x\in\mathcal{R}^m$;

$h=(h_0,\cdots,h_{c_1-1},\cdots,h_{c_{d-1}},\cdots,h_{c_{d-1}})\in\{0,1\}^{c_d}$;$r\in[-\beta,\beta]^{\bar{m}}$;

$v\in[-\beta,\beta]^{(\bar{m}+k)}$;$g_1,g_2\in[-B,B]$;

$e_{11},e_{12},e_{21},e_{22}\in[-B,B]^{\ell}$.

满足以下条件:

$$A_h\cdot v=F\cdot rdec(F_0\cdot r+F_1\cdot rdec(p))+u \tag{3}$$

$$B\cdot x=p \tag{4}$$

$$\begin{cases} c_1=(c_{11},c_{12})=(a\cdot g_1+e_{11},b_1\cdot g_1+e_{12}+\lfloor q/4\rfloor)\cdot rdec(p)) \\ c_1=(c_{21},c_{22})=(a\cdot g_2+e_{21},b_2\cdot g_2+e_{22}+\lfloor q/4\rfloor)\cdot rdec(p)) \end{cases} \tag{5}$$

$$\bar{c}=(\bar{c_1},\bar{c_2})=(\bar{a}\cdot\bar{g}+e_3,\bar{b}\cdot\bar{g}+e_4+\lfloor q/4\rfloor\cdot\delta) \tag{6}$$

$$A_z\cdot v_z=u_0 \tag{7}$$

利用 IZK 协议将方程(3)~方程(7)变换成 $A\cdot x=u\ mod\ q$ 的形式,并定义了集合 $VALID$ 和 Γ_ϕ 置换,满足方程(1)和方程(2).

令 $v=(s\parallel z)\in\mathcal{R}^{(\bar{m}+k)}$,其中:$s\in\mathcal{R}^{\bar{m}},z\in\mathcal{R}^k$,方程可转化为:

$$A\cdot s+A_{[0]}\cdot z+\sum_{i=j}^{d}A_{[i]}\cdot h_{[i]}\cdot z=F\cdot y+u$$

其中:

$$\{h_{[i]}=\sum_{j=c_i-1}^{c_i-1}h_j\cdot X^j\}_{i=1}^{d};y=rdec(F_0\cdot r+F_1\cdot rdec(p))$$

分解统一:方程(3)可以被转换为 $A_1\cdot x_1=u_1\ mod\ q$,A_1,u_1 公开,向量 x_1 的系数属于集合 $\{-1,0,1\}$.

令:

$$s^*=\tau(rdec_\beta(s))\in\{-1,0,1\}^{n\bar{m}\delta\beta}$$

$$z^*=\tau(rdec_\beta(z))\in\{-1,0,1\}^{nk\delta\beta}$$

$$r^*=\tau(rdec_\beta(r))\in\{-1,0,1\}^{n\delta\beta\bar{m}}$$

方程(1)可以转换为:

$$\lfloor rot(A_{[0]}\cdot H_{k,\beta})\rfloor\cdot z^*+\sum_{i=1}^{d}\sum_{j=c_i-1}^{c_i-1}\lfloor rot(A_{[i]}\cdot X^j)\cdot H_{k,\beta})\rfloor\cdot h_j\cdot z^*+[rot(A)\cdot H_{\bar{m},\beta})]\cdot s^*-[rot(F)\cdot\tau(y)]=\tau(u)mod\ q$$

和:

$$[rot(F_0)\cdot H_{\bar{m},\beta}]\cdot r^*+[rot(F_1)]\cdot\tau(rdec(p))-[H]\cdot\tau(y)=0\ mod\ q$$

通过应用基本代数,可以将公开矩阵串联起来,并相应地重新排列秘密向量,得到一个统一的方程,其形式为:

$$A_1 \cdot x_1 = u_1 \bmod q$$

其中 $u_1 = (\tau(u) \| 0) \in \mathbb{Z}_q^{2n}$,$A_1$ 是由推导式串联得到的公共矩阵,且 $x_1 = (x_{11} \| x_{12})$.

$$x_{11} = (z^* \| h_0 \cdot z^* \| \cdots \| h_{c_d-1} \cdot z^* \in \{-1,0,1\}^{(c_d+1)nk\delta_\beta}$$

$$x_{12} = (s^* \| r^* \| \tau(rdec(p)) \| \tau(y)) \in \{-1,0,1\}^{(\bar{m}\delta_\beta+\ell)2n}$$

扩展:秘密向量 $x_1 = (x_{11} \| x_{12})$ 扩展如下:

$$x_{11} \mapsto x'_{11} = mix(h, z^*) \in \{-1,0,1\}^{L_1}$$

$$x_{12} \mapsto x'_{12} = enc(x_{12}) \in \{-1,0,1\}^{L_2}$$

向量 $x'_1 = (x'_{11} \| x'_{12}) \in \{-1,0,1\}^{L_1+L_2}$,其中:

$$L_1 = (c_d+1)3nk\delta_\beta; L_2 = (\bar{m}\delta_\beta + \ell)6n$$

与此同时,将必要的零列附加到矩阵 A_1 上,得到一个新的矩阵 $A'_1 \in \mathbb{Z}_q^{2n\times(L_1+L_2)}$,使得 $A'_1 \cdot x'_1 = A_1 \cdot x_1$.

分解统一:对于 $j \in \{1,2\}$,计算下列式子:

$$g_j^* = \tau(rdec_B(g_j)) \in \{-1,0,1\}^{n\delta_B}$$

$$e_{j1}^* = \tau(rdec_B(e_{j1})) \in \{-1,0,1\}^{nl\delta_B}$$

$$e_{j2}^* = \tau(rdec_B(e_{j2})) \in \{-1,0,1\}^{nl\delta_B}$$

计算:

$$\bar{g}^* = \tau(rdec_B(\bar{g})) \in \{-1,0,1\}^{n\delta_B}$$

$$e_3^* = \tau(rdec_B(e_3)) \in \{-1,0,1\}^{nl\delta_B}$$

$$e_4^* = \tau(rdec_B(e_4)) \in \{-1,0,1\}^{nl\delta_B}$$

$$x^* = \tau(x) \in \{-1,0,1\}^{nm}$$

重新整理条件:

$$A_z = [A | A_1^{z[1]} | \cdots | A_{d_z}^{z[d_z]}] \in \mathcal{R}_q^{1\times((d_z+1)m+k)}$$

$$v_z = (v_0 \| v_1 \| \cdots \| v_{d_z}) \in \mathcal{R}^{(d_z+1)m+k}$$

令 $f = (d_z+1)m + k$,计算:

$$v_z^* = \tau(rdec_B(v_2)) \in \{-1,0,1\}^{n\delta_B f}$$

方程(4)可以写为:

$$[rot(\mathbf{B})] \cdot x^* - [H] \cdot \tau(rdec(p)) = 0^n \bmod q$$

令 $a = (a_1, \cdots, a_l)^{\mathrm{T}}$,$\{b = (b_{j1}, \cdots, b_{jl})^{\mathrm{T}}\}_{j=1,2}$,方程(5)可以转化为:

$$\begin{bmatrix} rot(a_1)\cdot H_B \\ \vdots \\ rot(a_l)\cdot H_B \end{bmatrix} \cdot g_j^* + [H_{l,B}] \cdot e_{j1}^* = \tau(c_{j1}) \bmod q$$

$$\begin{bmatrix} rot(b_{j1})\cdot H_B \\ \vdots \\ rot(b_{jl})\cdot H_B \end{bmatrix} \cdot g_j^* + [H_{l,B}] \cdot e_{j2}^* + \lfloor \frac{q}{4} \rfloor \cdot \tau(rdec(p)) = \tau(c_{j2}) \bmod q$$

令 $\bar{a} = (\bar{a}_1, \cdots, \bar{a}_l)^T$,$\bar{b} = (\bar{b}_1, \cdots, b_l)^T$,方程(6)转化为:

$$\begin{bmatrix} rot(\bar{a}_1)\cdot H_B \\ \vdots \\ rot(\bar{a}_l)\cdot H_B \end{bmatrix} \cdot \bar{g}_j^* + [H_{l,B}] \cdot e_3^* = \tau(\bar{c}_1) \bmod q$$

$$\begin{bmatrix} rot(\bar{b}_1)\cdot H_B \\ \vdots \\ rot(\bar{b}_1)\cdot H_B \end{bmatrix} \cdot \bar{g}^* + [H_{l,B}] \cdot e_4^* + \lfloor \frac{q}{4} \rfloor \cdot \tau(\delta) = \tau(\bar{c}_2) \bmod q$$

方程(7)可以转化为:

$$[rot(A_z) \cdot H_{f,B}] \cdot v_z^* = \tau(u_0) \bmod q$$

通过应用基本代数,可以串联公共矩阵,并相应地重新排列秘密向量来处理方程,从而得到一个方程形式为:

$$A_2 \cdot x_2 = u_2 \bmod q$$

其中 $u_2 = (0^n \| \tau(c_{j1}) \| \tau(c_{j2}) \| \tau(\bar{c_1}) \| \tau(\bar{c_2})) \in \mathbb{Z}_q^{(\Delta l+1)n}$,$A_2$ 是由推导式串联得到的公共矩阵.

$$x_2 = (x^* \| -\tau(rdec(p)) \| g_1^* \| e_{11}^* \| e_{12}^* \| g_2^* \| e_{21}^* \| e_{22}^* \| \bar{g}^* \| e_3^* \| e_4^* \| \lfloor \frac{q}{4} \rfloor \cdot \tau(rdec(p)) \| \lfloor \frac{q}{4} \rfloor \cdot \tau(\sigma) \| v_z^*) \in \{-1,0,1\}^{(m+3\ell+3\delta_B+6l\delta_B+f\delta_B)n}$$

扩展:秘密向量 x_2 扩展如下:

$$x_2 \mapsto x'_2 = enc(x_2) \in \{-1,0,1\}^{L_3}$$

其中 $L_3 = (M + 3\ell + 3\delta_B + 6l\delta_B + f\delta_B)3n$

与此同时,将必要的零列附加到矩阵 A_2 上,得到一个新的矩阵 $A'_2 \in \mathbb{Z}_q^{2n\times L_3}$,使得 $A'_2 \cdot x'_2 = A_2 \cdot x_2$.

所需的最终方程是 $A \cdot x = u \bmod q$:

$$A = \begin{bmatrix} A'_1 & \\ & A'_2 \end{bmatrix}, x = \begin{bmatrix} x'_1 \\ x'_2 \end{bmatrix}, u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$$

得到 $x = (x'_1 \| x'_2) = (x'_{11} \| x'_{12} \| x'_2) \in \{-1,0,1\}^L$,且 $L = L_1 + L_2 + L_3$.

定义一个集合 *VALID* 为所有向量 $u = (u'_1 \| u'_2) = (u'_{11} \| u'_{12} \| u'_2) \in \{-1,0,1\}^L$,满足条件:

$\exists h \in \{0,1\}^{c_d}$ 和 $z^* \in \{-1,0,1\}^{nk\delta_\beta}$ 使得:

$$u'_{11} = mix(h, z^*) \in \{-1,0,1\}^{L_1}$$

$\exists x_{12} \in \{-1,0,1\}^{(\bar{m}\delta_\beta+\ell)2n}$ 使得:

$$u'_{12} = enc(x_{12}) \in \{-1,0,1\}^{L_2}$$

$\exists x_2 \in \{-1,0,1\}^{(m+3\ell+3\delta_B+6l\delta_B+f\delta_B)n}$ 使得:

$$u'_2 = enc(x_2) \in \{-1,0,1\}^{L_3}$$

可以明显看出 $x \in VALID$.

定义一个集合:

$$\mathcal{S} = \{0,1\}^{c_d} \times \{-1,0,1\}^{nk\delta_\beta} \times \{-1,0,1\}^{(\bar{m}\delta_\beta+\ell)2n} \times \{-1,0,1\}^{(m+3\ell+3\delta_B+6l\delta_B+f\delta_B)n}$$

$\phi = (b, e, f_1, f_2) \in \mathcal{S}$ 中每个元素与排列 Γ_ϕ 关联结果如下:

$$\Gamma_\phi(u) = (\Psi_{b,e}(u'_{11}) \| \pi_{f1}(u'_{12}) \| \pi_{f2}(u'_2))$$

可以观察到,x, $\mathcal{S}$ 和 Γ_ϕ 满足方程,关系式 R' 转化为 $R_{abstract}$ 形式. 因此,可以用 Libert 等人描述的 IZK 协议根据 $R_{abstract}$ 获得 R'.

3　安全性分析

Ling[5] 等人在其论文中证明了 Ducas-Micciancio 数字签名方案的变体 VoDM 方案的安全性与原始的 Ducas-Micciancio 数字签名方案相同. 本方案采用 VoDM 数字签名方案生成数字签名. 基于 VoDM 数字签名方案的不可伪造性和 RSIS、RLWE 假设的难度,证明了该方案的安全性.

3.1　正确性

群签名方案的正确性依赖于以下事实:1)生成 $\prod_{QS}$ 的底层系统是完整的;2)底层加密方案,即 LPR 加密方案是正确的.

具体来说,一个诚实用户代表群组对消息进行签名的时候,能够证明拥有有效元组 ζ,即 $\prod_{QS}$ 被 *Verify* 算法接受的概率为 1,就能证明 $\prod_{QS}$ 的论证系统的完整性. 而验证 *Open* 算法的正确性:

$$c_{11} - c_{12} \cdot s_1 = b_1 \cdot g_1 + e_{12} + \lfloor q/4 \rfloor \cdot rdec(p) - (a \cdot g_1 + e_{11}) \cdot s_1 =$$

$$(a\cdot s_1+e_1)\cdot g_1+e_{12}+\lfloor q/4\rfloor\cdot rdec(p)-(a\cdot g_1+e_{11})\cdot s_1=$$
$$e_1\cdot g_1+e_{12}-e_{11}\cdot s_1+\lfloor q/4\rfloor\cdot redc(p)$$

其中 $\|e_1\|_\infty\leqslant B$, $\|s_1\|_\infty\leqslant B$, $\|g_1\|_\infty\leqslant B$, $\|e_{11}\|_\infty\leqslant B$, $\|e_{12}\|_\infty\leqslant B$, 由于 $B=\tilde{O}(n^{5/4})$, $q=\tilde{O}(n^4)$, 因此:

$$\|e_1\cdot g_1+e_{12}-e_{11}\cdot s_1\|_\infty\leqslant 2B^2+B=$$
$$\tilde{O}(n^{2.5})\leqslant\lceil q/4\rceil=\tilde{O}(n^4)$$

Open 算法按照描述的过程恢复 $rdec(p)$ 的概率为 1, 因此输出实际的签名者身份 p. 因此, *Open* 算法的能够正确识别签名的签名者.

3.2 完全匿名性

定理 1. 基于 RLWE 假设的难度和协议 $\prod_{gs}$ 的零知识特性, 以及底层 PKE 方案满足 IND-CPA 安全和密钥隐私性, DFSGS 方案可以抵抗完全匿名攻击.

证明: 分别定义 $\mathcal{C}$ 和 $\mathcal{A}$ 为挑战者和敌手角色. 本方案定义了一系列游戏来证明针对完全匿名的安全性. 在 Game i 中, 设 W_i 表示敌手的输出.

Game 0. 这正是实验 $Exp_{\mathcal{A}}^{anon-b}(\lambda,T)$. 挑战者 $\mathcal{C}$ 根据方案获取群公钥、成员证书、现有群用户的私钥和追踪密钥并发送给敌手 $\mathcal{A}$. $\mathcal{C}$ 初始化撤销列表 $RL=\emptyset$ 和诚实用户列表 H_u. 在查询阶段, $\mathcal{A}$ 可以查询任意用户的任意签名. 在挑战阶段 $\mathcal{A}$ 发送消息 M^*, 同时发送两个用户 p_0 和 p_1, 满足 $p_0,p_1\in H_u$ 和吊销令牌 $grt_{p1}\notin RL$. $\mathcal{C}$ 返回一个挑战签名 $\sum^*=(\bar{c}^*,c_1^*,c_2^*,\Pi_{gs}^*)\leftarrow Sign(gpk,gsk_{p_b},M)$. 最后 $\mathcal{A}$ 返回 $b^*=1$ 作为对 p_b 的猜测, 则 $Pr[W_0=1]=Pr[Exp_{\mathcal{A}}^{anon-b}(\lambda,T)=1]$.

Game 1. 这里改变了挑战签名 $\sum^*$ 中的 $\bar{c}^*$ 所加密的明文. 即用一个随机的 p^* 代替 p_b, 由于底层的 PKE 方案满足 IND-CPA 的安全性, 这里改变了 $\mathcal{A}$ 的成功概率, 但这种改变很小, 可以忽略不计. 因此:

$$Pr[W_1=1]-Pr[W_0=1]=negl(\lambda)$$

Game 2. 在这里改变了密文 $\bar{c}^*$ 的加密密钥. 即用一个随机的 $(\bar{a}^*,\bar{b}^*)$ 来计算 $\bar{c}^*$, 其中:

$\bar{b}^*=\bar{a}^*\cdot\bar{s}^*+\bar{e}^*$. PKE 方案的关键隐私性使 Game1 和 Game 2 在统计上不可区分. 因此:

$$Pr[W_2=1]-Pr[W_1=1]=negl(\lambda)$$

Game 3. 在这里 $\mathcal{C}$ 不会抹去第 2 个解密密钥 (s_2,e_2), 而是保留加密方案的两个解密密钥. 除此以外. Game2 与 Game3 在统计上不可区分. 所以在 $\mathcal{A}$ 的角度和 Game2 是一样的. 因此 $Pr[W_3=1]\approx Pr[W_2=1]$.

Game 4. 除了在开放预言查询中使用 s_2 去解密密文 c_2, 和 Game3 基本一致. 在事件 F_1 发生之前, $\mathcal{A}$ 的视角保持不变. 事件 F_1 为 $\mathcal{A}$ 向开放预言机查询有效签名 $\sum=(\bar{c},c_1,c_2,\Pi_{gs})$. 由于 F_1 破坏了 NIZK 参数系统 Π_{gs} 的稳健性, 因此:

$$|Pr[W_4=1]-Pr[W_3=1]|\leqslant Pr[F_1]\leqslant Adv_{\Pi gs}^{sound}=negl(\lambda)$$

Game 5. 调用模拟器生成协议代替见证生成协议, 通过编程随机预言机中的 $\mathcal{H}_{FS}$ 来生成开放预言查询的模拟证明 Π_{gs}, 用模拟证据代替合法证据. 基于统计零知识性质, Game 4 和 Game 5 在统计上是不可区分的, 因此 $Pr[W_5=1]\approx Pr[W_4=1]$.

Game 6. 在 Game5 中, c_1 和 c_2 加密同一条消息, 即 $rdec(p_o)$. 而在 Game 6 中, c_1 为 $rdec(p_1)$ 的加密, c_2 为 $rdec(p_0)$ 的加密. 公钥 (a,b_1) 加密方案的语义安全性确保了:

$$|Pr[W_6=1]-Pr[W_5=l]|=negl(\lambda)$$

Game 7. 在这里切换回在开放预言查询中使用 s_1 并重新抹去 (s_2,e_2). 在事件 F_2 发生之前, $\mathcal{A}$ 的视角和 Game 6 相同. 事件 F_2 为 $\mathcal{A}$ 向开放预言查询有效签名 $\sum=(\bar{c},c_1,c_2,\Pi_{gs})$, 由于事件 F_2 违反了 NIZK 协议的模拟合理性, 因此:

$$|Pr[W_7=1]-Pr[W_6=1]|\leqslant Pr[F_2]\leqslant Adv_{\Pi gs}^{sim}=negl(\lambda)$$

Game 8. 这里除了 c_2 为 $rdec(p_1)$ 的加密外, 和 Game 7 没有区别. 根据公钥 (a,b_2) 加密方案的语义安全性, $\mathcal{A}$ 不受该改变的影响. 因此:

$$|Pr[W_8=1]-Pr[W_7=l]|=negl(\lambda)$$

Game 9. 在这里切换到生成真实的 NIZK 协议而不是使用模拟器. 基于统计零知识属性, $\mathcal{A}$ 的视角和 Game 8 不可区分, 因此:

$$Pr[W_9=1]\approx Pr[W_8=1]$$

因此得到:

$$Pr[Exp_{\mathcal{A}}^{anon-1}](\lambda,T)=1]-$$
$$Pr[Exp_{\mathcal{A}}^{anon-0}](\lambda,T)=1]|=negl(\lambda)$$

3.3 前向可追溯性

定理 2. 基于 RSIS 假设的难度, DFSGS 方案具有前向安全可追溯性.

证明: 假设攻击者 $\mathcal{A}$ 可以用不可忽略的概率破坏方案的前向安全可追溯性, 那么构造了一个算法 $\mathcal{B}$ 也可以用不可忽略的概率解决 RSIS 问题.

给定一个矩阵 $\bar{A}\in\mathcal{R}^{l\times m'}$, 要求 $\mathcal{B}$ 找到一个非零向量 $\bar{v}\in\mathcal{R}_q^{m'}$ 满足 $\bar{A}\cdot\bar{v}=u_0$, 且 $\|\bar{v}\|_\infty\leqslant\beta$. 模拟攻击者 $\mathcal{A}$ 攻击前向安全可追溯性的视角, $\mathcal{B}$ 构建了一个算法, 该算法输出一个有效向量 $\bar{v}$ 满足 $\bar{A}\cdot\bar{v}=u_0$ 和 $\|\bar{v}\|_\infty\leqslant\beta$.

Setup. 定义矩阵 $\bar{A}=[\bar{A}_0|\bar{A}_1|\cdots|\bar{A}_d]$, 其中 $\bar{A}_0\in\mathcal{R}_q^{l\times m}$, $\bar{A}_j\in\mathcal{R}_q^{l\times\bar{m}}, j\in\{1,2,\cdots,d\}$. 设 $t=0, B_u=\emptyset$, 采样 $\bar{z}=(z_0\|z_1\|\cdots\|z_d)\in\mathcal{R}^{m'}$, 且 $\|\bar{z}\|_\infty\leqslant\beta$, 计算 $u_0=\bar{A}\cdot\bar{z}$. 设 p^* 为目标用户, $t^*\in[0,T-1]$ 为目标伪造时间, $z^*=bin(t^*)$. 定义 A_0 为 $\bar{A}_0, A_b^{z^*[b]}$ 为 $\bar{A}_b$, 其中 $b\in[d]$. 最后将组公钥和跟踪密钥发送给对手 $\mathcal{A}$.

Join. 对于不是用户 p^* 的用户, 随机选择 $x\in\mathcal{R}^m$, 计算出 $p=\mathbf{B}\cdot x\in\mathcal{R}_q$. 并发送给 $\mathcal{B}$. $\mathcal{B}$ 计算出 $A_h=[A_0|A_1^{z[1]}|\cdots|A_d^{z[d]}]$, 并将成员证书 $cert=(h,r,v)$ 发送给用户.

Queries. 当 $\mathcal{A}$ 查询随机预言机时, $\mathcal{B}$ 响应一个随机字符串, 并记录查询的信息. 在时间段 t, $\mathcal{B}$ 与 $\mathcal{A}$ 交互, 并且回复如下:

· 密钥查询: 当被查询的用户身份 $p=p^*$ 时, 若 $p^*\in B_u$ 或 $t\leqslant t^*$, 则 $\mathcal{B}$ 响应终止. 否则对于 $z\in Nodes(t\rightarrow T-1)$, $\mathcal{B}$ 通过 $SampleD(DelBasis(R,A_z),u_0,s_{d_1})$ 生成 usk_0, 发送 $gsk_t=(usk,\bar{a},\bar{b},x,cert)$ 给 $\mathcal{A}$, 并将 p^* 添加到 $\boldsymbol{B}_u$ 中. 当用户身份 $p\neq p^*$ 时, 若 $p\in\boldsymbol{B}_u$, 则 $\mathcal{B}$ 响应终止. 否则 $\mathcal{B}$ 用同样的方法计算 usk_t. 最后, $\mathcal{B}$ 将 gsk_t, 发送给 $\mathcal{A}$, 并将其添加到 $\boldsymbol{B}_u$ 中.

· 签名查询: $\mathcal{A}$ 从随机预言机中查询消息 $\boldsymbol{M}$ 的签名, 若当 $p\in\boldsymbol{B}_u$ 且在时刻 t, 则 $\mathcal{B}$ 终止响应. 否则, 若 $p=p^*$, $\mathcal{B}$ 在预言机中利用模拟零知识证明生成消息 $\boldsymbol{M}$ 的签名, 并将签名返回给 $\mathcal{A}$. 若 $p\neq p^*$, $\mathcal{B}$ 用算法 G_{sign} 回复 $\mathcal{A}$.

Forgery. $\mathcal{A}$在目标时间段 t'伪造消息 $\boldsymbol{M}^*$ 的签名 $\sum^*$,满足 $Verify=1$,并且在 $\boldsymbol{M}^*$ 处进行签名查询,没有产生 $\prod$的结果.若 $t'\neq t^*$,则$\mathcal{B}$终止响应.假设$\mathcal{A}$以 ε 的优势成功伪造了签名 $\sum^*=(\{CMT_i^*\}_{i=1}^k, CH, \{RSP_i^*\}_{i=1}^k, \bar{c}, c_1, c_2)$,$p'$可以由 Open 算法得出.若 $p'=p^*$,$\mathcal{B}$可以用下面的方法使用伪造来处理 RSIS 问题:对于$(M^*, \{CMT_i^*\}_{i=1}^k, \xi^*)$,$\mathcal{A}$需要查询预言机$\mathcal{H}_{\mathrm{FS}}$.由于挑战空间和二次约束,猜出挑战值的概率可以忽略不计.设 $Q_{\mathcal{H}FS}$是对预言机$\mathcal{H}_{FS}$查询的上限,q_h 是第 h 个预言机查询,设 h 表示目标分叉点.用相同的输入重复$\mathcal{A}$的操作多次.在这些查询中,前 $h-1$ 个查询保持输入和预言机$\mathcal{H}_{FS}$不变,返回一样的查询值$(r_1, r_2, \cdots, r_{h-1})$.从第 h 次查询开始,它在$\{1,2,3\}$中均匀选择并用新的$(r_h, \cdots, Q_{\mathcal{H}FS})$进行回复.通过概率大于$\frac{1}{2}$的分叉引理,$\mathcal{B}$得到了涉及元组$(M^*, \{CMT_i^*\}_{i=1}^k, \xi^*)$的 3 个分叉分支,并令分支的结果为:

$$r_h^{(1)}=(ch_1^{(1)}, \cdots, ch_k^{(1)})$$
$$r_h^{(2)}=(ch_1^{(2)}, \cdots, ch_k^{(2)})$$
$$r_h^{(3)}=(ch_1^{(3)}, \cdots, ch_k^{(3)})$$

其响应分别为(RSP_1, RSP_2, RSP_3),因此:

$$P_r[\{\exists l\in(1,\cdots,\kappa): (ch_i^{(1)}, ch_i^{(2)}, ch_i^{(3)})=\{1,2,3\}\}]=1-(\frac{7}{9})^{\kappa}$$

从对应的响应(RSP_1, RSP_2, RSP_3)中,$\mathcal{B}$可以提取出见证元组 $\zeta^*=(t, r, v, x, p, \bar{g}, e_3, e_4, g_1, g_2, e_{1,1}, e_{2,1}, e_{1,2}, e_{2,2}, v_z)$满足 $\bar{c}, c_1, c_2$ 分别为 δ 和 p 的正确加密以及:

$$\begin{cases} A_h\cdot v=F\cdot rdec(F_0\cdot r+F_1\cdot p)+u \\ A_z\cdot v_z=u_0 \end{cases}$$

当正确猜测 p^* 和 t^* 时,它意味着 $p=p^*$ 和 $z=z^*$.在这种情况下,有 $A_z\cdot v_z=\bar{A}\cdot\bar{z}=u_0$.因为$\mathcal{A}$在 t^* 之前从来没有查询过用户秘密密钥,所以 $\bar{z}$ 对于$\mathcal{A}$来说是未知的.而且,从$\mathcal{A}$的角度来看,$\bar{z}$ 来自分布 $D_{z_m, s_{d+1}}$.这时就有很大的概率 $v_z\neq\bar{z}$.设 $\bar{v}=v_z-\bar{z}$ 且 $\|\bar{v}\|_\infty\leqslant\beta$,则 $\bar{v}$ 是 $\bar{A}\cdot\bar{v}=0$ 的非零解,由于 RSIS 假设的难度,$\mathcal{A}$成功伪造签名的优势可以忽略不计,因此该方案是前向安全可追溯的.

3.4　不可帧性

定理 3. 基于 RSIS 假设的难度,DFSGS 方案具有抗可帧性的安全性.

证明:与前面的证明类似,假设有一个对手$\mathcal{A}$以不可忽略的概率对方案进行帧攻击.然后,构造了一个算法$\mathcal{B}$,以不可忽略的概率求解 RSIS 实例矩阵 $B\in\mathcal{R}_q^{1\times m}$.

KeyGen. 运行上节 2.3 中给出的密钥生成算法.把 gpk, ok, ik 发送给$\mathcal{B}$.

Queries. 当$\mathcal{A}$查询随机预言机时,$\mathcal{B}$响应一个随机字符串,并记录查询的信息.$\mathcal{B}$与$\mathcal{A}$交互,并且回复如下:

· Get_{ik}. $\mathcal{A}$使用预言机获取 ik.

· Q_{user}. 获取 ik 后,$\mathcal{A}$作为 GM,作为 GM 与一个诚实用户 U_p 参与 $join$ 协议.对于每个查询,$\mathcal{B}$代表诚实用户 U_p 参与 $join$ 协议,新加入的用户的身份 p 保存在 H_u 集合中.

· $Gsign$. $p\notin C_u$,则终止查询.否则使用 gsk_p 在消息 M 生成签名 $\sum$,并将$(t, M, \sum)$保存在 $Sigs$ 中,t 是签名的生成时间.

· Get_{reg}. 输入环多项式 p,通过在 reg 中搜索 p 得到(p, grt_p).

· Get_{gsk}. 输入环多项式 p,返回 gsk_p,并将 p 添加到 C_u 集合中.

Forgery. $\mathcal{A}$生成一个伪造,包含消息签名对$(M^*, \sum^*)$,签名者 p^* 和吊销列表 RL^*,使得:

$$Verify(gpk, M^*, \sum^*, t^*, RL^*)=1$$
$$Open(gpk, ok, M^*, \sum^*)=p^*$$

即使用户 p^* 没有签名,$\mathcal{A}$也必须指控 p^*.如果 $p^*\in C_u$ 则终止,否则$\mathcal{A}$必须以高概率输入$(M^*, \{CMT_i^*\}_{i=1}^\kappa, \xi^*)$来查询随机预言机$\mathcal{H}_{FS}$.否则:

$$Pr[(M^*, \{CMT_i^*\}_{i=1}^\kappa, \xi^*)]\leqslant\frac{1}{3^\kappa}$$

以上概率可以忽略不计,因此在 $\varepsilon-\frac{1}{3^\kappa}$的概率下,$\mathcal{A}$一定查询过随机预言机$\mathcal{H}_{FS}$.设 $Q_{\mathcal{H}\mathrm{FS}}$是对预言机$\mathcal{H}_{FS}$查询的上限,$q_h$ 是第 h 个预言机查询,设 h 表示目标分叉点.用相同的输入重复$\mathcal{A}$的操作多次.在这些查询中,前 $h-1$ 个查询保持输入和预言机$\mathcal{H}_{FS}$不变,返回一样的查询值$(r_1, r_2, \cdots, r_{h-1})$.从第 h 次查询开始,它在$\{1,2,3\}$中均匀选择并用新的$(r_h, \cdots, r_{Q_{\mathcal{H}FS}})$进行回复.通过概率大于$\frac{1}{2}$的分叉引理,$\mathcal{B}$得到了涉及元组$(M^*, \{CMT_i^*\}_{i=1}^\kappa, \zeta^*)$的 3 个分叉分支,并令分支的结果为:

$$r_h^{(1)}=(ch_1^{(1)}, \cdots, ch_\kappa^{(1)})$$
$$r_h^{(2)}=(ch_1^{(2)}, \cdots, ch_\kappa^{(2)})$$
$$r_h^{(3)}=(ch_1^{(3)}, \cdots, ch_\kappa^{(3)})$$

并且他们的响应分别为(RSP_1, RSP_2, RSP_3),因此:

$$P_r[\{\exists l\in(1,\cdots,\kappa): (ch_i^{(1)}, ch_i^{(2)}, ch_i^{(3)})=\{1,2,3\}\}]=1-(\frac{7}{9})^{\kappa}$$

从对应的响应(RSP_1, RSP_2, RSP_3)中,$\mathcal{B}$可以提取出见证元组 $\zeta^*=(t, r, v, x, p, \bar{g}, e_3, e_4, g_1, g_2, e_{1,1}, e_{2,1}, e_{1,2}, e_{2,2}, v_z)$满足 $\bar{c}, c_1, c_2$ 为 p 的正确加密以及 $\mathbf{B}\cdot x=p$.

由于加密方案的正确性,c_1 将被解密为 p^*.

因为$\mathcal{A}$赢得了不可帧性博弈,所以 $p^*\neq\perp$是一个诚实的组成员,并且 gsk_{p^*}不会被$\mathcal{B}$通过 Get_{gsk}查询到.因此有 $\mathbf{B}\cdot x=p=p^*=\mathbf{B}\cdot x^*$.

根据文献[5]中的引理 2,具有至少$\frac{1}{2}$的概率 $x^*\neq x$.在这种情况下,得到一个非零向量 $y=x^*-x$ 使得 $\mathbf{B}\cdot y=0$ 且 $\|y\|_\infty=1$.因此,$\mathcal{B}$以不可忽略的概率$\frac{1}{2}\cdot(\varepsilon-\frac{1}{3^\kappa})(1-(\frac{7}{9})^\kappa)\cdot\frac{1}{2}$解出 $RSIS$ 问题的实例.

4　效率分析

这里选择了一些与本工作相似的先进方案进行比较,分别从群组公钥 Gpk 的长度、群组用户密钥 Gsk 的长度、签名 Signature 的长度、前向安全性、匿名性和动态性等方面比较了上述的方案.其中 λ 为安全参数,N 为群组用户数量,T 为时

间段的最大数量. SA 表示无私匿名;AFA 表示几乎完全匿名;FA 表示完全匿名;S 表示静态;PD 表示部分动态;FD 表示完全动态.

4.1 功能性分析

本方案将 Ducas-Micciancio 方案和 VLR 机制相结合,利用 Ducas-Micciancio 方案对用户身份签名并颁发证书以实现成员的加入,通过 VLR 机制的撤销令牌实现成员的撤销. 使得方案具备完全动态性,能够灵活加入和撤销成员,显著提升了方案的实用性和效率. 同时,本方案利用 PKE 为用户生成额外密钥对,将加密密钥作为签名密钥的一部分,并把解密密钥作为用户的吊销令牌. 有效防止了非法用户通过签名密钥构建用户的吊销令牌,进而保护了用户的身份隐私安全,实现了方案的完全匿名性. 此外,本方案还将盆景树技术引入理想格结构,显著提升了性能,并实现了前向安全性,即使当前密钥泄露,攻击者也无法伪造过去的签名. 盆景树的高效密钥更新机制和理想格的数学特性相结合,增强了方案的安全性,优化了计算开销.

表 4 方案的功能性对比

Table 4 Functional comparison of schemes

方案	前向安全	匿名性	动态性	量子安全
Ling[5]	No	FA	PD	Yes
Ling[21]	Yes	FA	S	Yes
Perera[22]	No	AFA	FD	Yes
Liao[23]	Yes	FA	FD	Yes
Gao[24]	No	AFA	FD	Yes
Ours	Yes	FA	FD	Yes

在本节中,通过对本方案和其他方案的功能性进行对比,如表 4 所示,可以看出所有方案均满足量子安全性. 此外,文献[5,22,24]缺乏前向安全性,方案[22,24]不具备完全匿名性,方案[5,21]未能实现完全动态性. 相比之下,本方案和文献[23]同时具备前向安全性、完全匿名性和完全动态性,展现了更全面的功能性优势.

4.2 计算开销分析

根据功能性分析的结果,得出本方案和文献[23]在功能性表现更为完善的结论. 在此基础上,本节进一步对两者的计算开销进行了详细对比,如表 5 所示. 对比结果表明,本方案在计算效率上具有明显优势:本方案在群公钥、用户私钥和签名大小方面均优于文献[23],具备更小的计算和存储开销. 因此本方案在计算效率和性能上展现出更显著的优越性.

表 5 方案的计算开销对比

Table 5 Comparison of computational cost of schemes

方案	Gpk	Gsk	Signature
Liao[23]	$\tilde{O}(\lambda^2 logT+\lambda logN)$	$\tilde{O}(\lambda log^3 T)$	$\tilde{O}(\lambda^2(logN+logT))$
Ours	$\tilde{O}(\lambda(logT))$	$\tilde{O}(\lambda log^2 T)$	$\tilde{O}(\lambda(logT))$

本方案之所以拥有更高的计算效率,主要归因于两个方面:一方面是因为本方案引入了理想格结构,在标准格中,一个 $n\times n$ 的矩阵需要存储 n^2 个元素,而理想格仅需要几个生成元就可以进行表示,凭借理想格独特的结构特性,能够有效地减小计算开销[25]. 另一方面,本方案对盆景树技术进行改进,利用理想格上的 $TrapGen_{R_q}$ 算法、$SampleD_{R_q}$ 算法和 $DelBasis_{R_q}$ 算法来减小盆景树技术的计算开销,同时,利用 Ducas – Micciancio 方案对用户身份签名并颁发证书,将用户身份和盆景树技术分离,从而使得密钥和签名大小和群组用户的数量无关,在实际应用中更加高效,能够更好地满足实际应用场景的需求.

为了使对比结果更加清晰且易于理解,本节对两种方案进行了仿真实验. 在实验中,用户数量 N 设置为 1024,时间周期 T 设置为 100,安全参数 λ 从 10 到 160 依次取值,共进行 16 次测试. 得到了两种方案在公钥长度、私钥长度和签名长度的对比结果,其中,图 2 展示了公钥长度对比结果,图 3 展示了私钥长度对比结果,图 4 展示了签名长度对比结果.

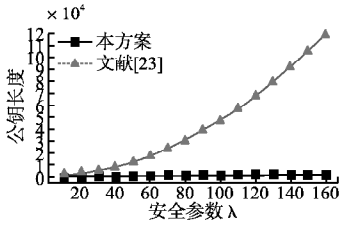

图 2 公钥长度对比图

Fig. 2 Public key length comparison diagram

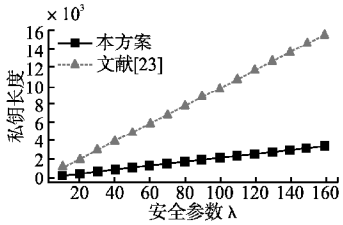

图 3 私钥长度对比图

Fig. 3 Private key length comparison chart

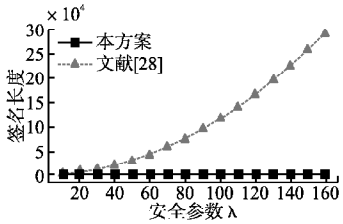

图 4 签名长度对比图

Fig. 4 Signature length comparison chart

可以看出,随着安全参数 λ 的逐步增加,本方案的公钥长度和签名长度增长非常平缓,几乎呈现为一条水平的直线. 相比之下,文献[23]在公钥长度和签名长度上则表现出显著的指数增长趋势. 而在私钥长度方面,两个方案随着安全参数 λ 的逐步增加,都呈线性增长趋势,但文献[23]的增长斜率明显更大,其私钥长度的增长速度远高于本方案. 对比结果表明,本方案在提升安全性的同时,能够更加高效地控制密钥和签名的大小,从而展现出更优的可扩展性和实用性.

综上所述,本方案不仅在功能性方面表现出色,而且在计算和存储开销方面也具有明显优势. 这些优势使得本方案在

实际研究中具有更强的竞争力,为相关领域的研究和应用提供了有力的支持.

5 结　论

本文构造了一个基于理想格的 DFSGS 方案,该方案在随机预言机模型下是安全的.在本方案中,理想格应用的有效减小了密钥和签名的大小.而通过添加额外密钥对来设置吊销令牌,解决了 VLR 撤销机制无法实现完全匿名性的问题.与现有方案相比,本方案允许成员随时加入和撤销,实现了前向安全性,并通过构造有效的零知识证明有效实现了完全匿名性.在接下来的工作中,将探索一种基于格的更有效的动态前向安全群签名方案,如减小吊销列表的大小以及没有零知识系统的 DFSGS 方案.

References:

[1] Chaum D, Van Heyst E. Group signatures[C]//Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, 1991: 257-265.

[2] Sahin Meryem Soysaldi, Akleylek Sedat. A survey of quantum secure group signature schemes: lattice-based approach[J]. Journal of Information Security and Applications, 2023, 73(3): 1.1-1.24, doi: 10.1016/j.jisa.2023.103432.

[3] Aggarwal D, Brennen G K, Lee T, et al. Quantum attacks on Bitcoin, and how to protect against them[J]. arxiv preprint arxiv: 1710.10377, 2017.

[4] Regev O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2009, 56(6): 1-40.

[5] Ling S, Nguyen K, Wang H, et al. Constant-size group signatures from lattices[C]//Public-Key Cryptography-PKC: 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, 2018: 58-88.

[6] Luo Q, Jiang C Y. A new constant-size group signature scheme from lattices[J]. IEEE Access, 2020, 8: 10198-10207, doi: 10.1109/ACCESS.2020.2964686.

[7] Canard S, Georgescu A, Kaim G, et al. Constant-size lattice-based group signature with forward security in the standard model[C]// Provable and Practical Security: 14th International Conference, 2020: 24-44.

[8] Ling S, Nguyen K, Wang H, et al. Lattice-based group signatures: achieving full dynamicity with ease[C]//Applied Cryptography and Network Security: 15th International Conference, 2017: 293-312.

[9] Perera M N S, Koshiba T. Achieving almost-full security for lattice-based fully dynamic group signatures with verifier-local revocation [C]//Information Security Practice and Experience: 14th International Conference, 2018: 229-247.

[10] Abhilash M H, Amberker B B. Dynamic group signature scheme using ideal lattices[J]. International Journal of Information and Computer Security, 2023, 22(1): 60-90.

[11] Lyubashevsky V, Micciancio D. Generalized compact knapsacks are collision resistant[C]//International Colloquium on Automata, Languages, and Programming, 2006: 144-155.

[12] Peikert C, Rosen A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices[C]//Theory of Cryptography: 3rd Theory of Cryptography Conference, 2006: 145-166.

[13] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM, 2013, 60(6): 1-35.

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

[15] Ling S, Nguyen K, Wang H. Group signatures from lattices: simpler, tighter, shorter, ring-based[C]//IACR International Workshop on Public Key Cryptography, 2015: 427-449.

[16] Ducas L, Micciancio D. Improved short lattice signatures in the standard model[C]//Advances in Cryptology-CRYPTO: 34th Annual Cryptology Conference, 2014: 335-352.

[17] Agrawal S, Boneh D, Boyen X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE[C]//Advances in Cryptology-CRYPTO: 30th Annual Cryptology Conference, 2010: 98-115.

[18] Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis[J]. Journal of Cryptology, 2012, 25: 601-639, doi: 10.1007/978-3-642-13190-5_27.

[19] Emura K, Hayashi T, Ishida A. Group signatures with time-bound keys revisited: a new model and an efficient construction[C]// Proceedings of the ACM on Asia Conference on Computer and Communications Security, 2017: 777-788.

[20] Libert B, Ling S, Mouhartem F, et al. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions[C]//International Conference on the Theory and Application of Cryptology and Information Security, 2016: 373-403.

[21] Ling S, Nguyen K, Wang H, et al. Forward-secure group signatures from lattices[C]//Post-Quantum Cryptography: 10th International Conference, 2019: 44-64.

[22] Perera M N S, Koshiba T. Almost fully secured lattice-based group signatures with verifier-local revocation[J]. Cryptography, 2020, 4(4): 33, doi: 10.3390/cryptography4040033.

[23] Liao Z, Huang Q, Chen X. A fully dynamic forward-secure group signature from lattice[J]. Cybersecurity, 2023, 6(1): 40-53.

[24] Gao S, Chen X, Li H, et al. Post-quantum secure group signature with verifier local revocation and backward unlinkability[J]. Computer Standards & Interfaces, 2024, 88: 103782, doi: 10.1016/j.csi.2023.103782.

[25] WANG Q N, WANG K, CHEN H Y, et al. Identity-based Interceptable Signature Scheme on Ideal Lattice[J]. Research on Information Security, 2025, 11(1): 57-65.

附中文参考文献:

[25] 王庆楠,王　克,陈辉焱,等.理想格上基于身份的可截取签名方案[J].信息安全研究,2025,11(1):57-65.