



## 格上高效的完全动态群签名方案

叶 青, 赵楠楠, 赵宗渠, 秦攀科, 闫玺玺, 汤永利

(河南理工大学 计算机科学与技术学院, 河南 焦作 454000)

**摘 要:** 为降低完全动态群签名加入和撤销机制的复杂性, 将动态群签名思想引入 NGUYEN 等人提出的格上群签名方案, 提出一种改进的完全动态群签名方案。在改进方案中, 用户产生自己的签名密钥而不是由群管理员产生, 当用户加入群时, 群管理员验证用户身份并为其颁发证书, 用户成为群成员后用自己的签名密钥和证书进行签名。若群成员有不合法行为或想退群, 则群管理员和群成员均可执行群成员的撤销操作, 使群成员退出该群。由于方案中群成员的签名密钥由自己生成, 因此能够抵抗群管理员的陷害攻击。在随机预言模型下, 基于错误学习问题和非齐次小整数解问题证明改进方案的安全性。分析结果表明, 该方案能够减少加入和撤销机制的计算代价, 且密钥长度和签名长度与群成员数量无关, 适用于大群组的签名系统。

**关键词:** 动态群签名; 格; 陷害攻击; 错误学习问题; 非齐次小整数解问题

开放科学(资源服务)标志码(OSID):



中文引用格式: 叶青, 赵楠楠, 赵宗渠, 等. 格上高效的完全动态群签名方案[J]. 计算机工程, 2021, 47(2): 160-167, 175.

英文引用格式: YE Qing, ZHAO Nannan, ZHAO Zongqu, et al. Efficient fully dynamic group signature scheme from lattice[J]. Computer Engineering, 2021, 47(2): 160-167, 175.

## Efficient Fully Dynamic Group Signature Scheme from Lattice

YE Qing, ZHAO Nannan, ZHAO Zongqu, QIN Panke, YAN Xixi, TANG Yongli

(College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan 454000, China)

**[Abstract]** In order to reduce the complexity of the joining and revoking mechanism of fully dynamic group signature, this paper introduces the concept of dynamic group signature into NGUYEN's group signature scheme from lattice, and on this basis proposes an improved fully dynamic group signature scheme. In this scheme, the signing key is generated by the user rather than the group manager. When the user joins a group, the group manager verifies the user's identity and issues a certificate for the user. After becoming a group member, the group member signs with his/her own signing key and the issued certificate. If a group member has illegal behavior or wants to withdraw from the group, both the group manager and the group member can perform the revocation operation on the group member to make the group member leave the group. In this scheme, since the signing key of a group member is generated by himself/herself, it can resist the trap attack from the group manager. Under the random oracle model, the security of the proposed scheme is verified based on the Learning with Error (LWE) problem and the Inhomogeneous Small Integer Solution (ISIS) problem. Analysis results show that the proposed scheme can reduce the computational cost of joining and revocation mechanism, and the length of a key and that of a signature do not depend on the number of group members, which makes the scheme suitable for the signature systems of large groups.

**[Key words]** dynamic group signature; lattice; trap attack; Learning with Error (LWE) problem; Inhomogeneous Small Integer Solution (ISIS) problem

DOI: 10.19678/j.issn.1000-3428.0057111

**基金项目:** 国家自然科学基金(61802117); 河南省高校科技创新团队支持计划(20IRTSTHN013); 河南省重点研发与推广专项(182102310923, 192102210280); 河南省高等学校重点科研项目(18A413001, 19A520025); 河南理工大学自然科学基金(T2018-1); 河南理工大学青年骨干教师资助计划(2018XQG-10)。

**作者简介:** 叶 青(1981—), 女, 讲师、博士, 主研方向为密码学、数字签名; 赵楠楠, 硕士研究生; 赵宗渠(通信作者), 秦攀科, 讲师、博士; 闫玺玺, 副教授、博士; 汤永利, 教授、博士后。

**收稿日期:** 2020-01-03 **修回日期:** 2020-02-06 **E-mail:** zhaozong-qu@hpu.edu.cn

## 0 概述

1991年,CHAUM等人首次提出群签名的概念<sup>[1]</sup>,其具有匿名性和追踪性。群签名允许群中合法成员代表群对消息进行签名,任意验证者均可利用群公钥来验证该签名的合法性,但无法确定签名者的真实身份,即匿名性;当发生争议时,群管理员可以通过追踪密钥打开签名找到真实的签名者,即追踪性。群签名的匿名性和追踪性使其被广泛应用于多种场景,如电子投票、电子商务系统和可信计算等。文献[2]指出,基于经典数论难题的传统密码方案<sup>[3-5]</sup>在多项式时间内会被量子计算机破解,基于格的新型密码体制将成为后量子密码时代的研究热点。

2010年,GORDON等人在Asiacrypt2010会议上提出格上群签名方案<sup>[6]</sup>,但该方案的密钥长度和签名长度都与群成员数量呈线性关系。2013年,LANGUILLAUMIE等人在Asiacrypt2013会议上提出一种密钥长度、签名长度与群成员数量呈对数关系的群签名方案<sup>[7]</sup>,虽然缩短了密钥长度和签名长度,但由于两者均依赖于群成员数量,因此该方案并不适用于大群组的群签名系统。2015年,NGUYEN等人提出一种简单高效的群签名方案<sup>[8]</sup>,该方案的密钥长度和签名长度与群成员数量无关,适用于大群组的群签名系统,但由于群成员私钥由群管理员产生,因此不能抵抗群管理员对群成员的陷害攻击。考虑到用户加入群的动作在任意时间都有可能发生,并且当发现某些群成员有行为不端的现象时,群管理员应有权撤销不法成员的签名权力,因此,群签名系统应包含支持群成员动态加入、撤销的加入机制和撤销机制<sup>[9-10]</sup>。然而,以上群签名方案都不支持群成员的加入和撤销。

2016年,LIBERT等人构造了一个包含加入机制的群签名方案<sup>[11]</sup>,但仍缺少群成员的动态撤销机制。2017年,LING等人基于Merkle哈希树构造了一个格基完全动态(同时包含加入和撤销机制)的群签名方案<sup>[12]</sup>,但该方案撤销成员时需要更新哈希树,计算较复杂且耗时较长,并且签名长度仍与群成员数量相关。2018年,LING等人又提出了格上本地撤销群签名方案<sup>[13]</sup>,但该方案不支持群成员的动态加入。2019年,李雪莲等人提出一种适合大群组的格基完全动态签名方案<sup>[14]</sup>,但由于在加入过程中使用变色龙哈希函数和随机采样技术,并且撤销过程中增加了与撤销图灵机的交互代价,因此该方案的开销较大。

为加快群成员的加入和撤销速度,降低完全动态群签名方案加入和撤销机制的复杂性,本文在文献[8]群签名方案的基础上,结合文献[11,14]提出的动态群签名思想,基于错误学习(Learning with Error, LWE)问题和非齐次小整数解(Inhomogeneous Small Integer Solution, ISIS)问题构造一个高效的格上完全动态群签名方案,对其进行安全性证明,并与现有的格上群签名方案进行效率对比。

## 1 预备知识

### 1.1 符号定义

本文方案中的符号定义如表1所示。

表1 符号定义

Table 1 Symbols definition

符号	定义	符号	定义
$\mathbb{Z}$	整数集合	$\lfloor \cdot \rfloor$	下取整
$\mathbb{R}^+$	正实数集合	$\lceil \cdot \rceil$	上取整
$[N]$	整数集合 $\{1, 2, \dots, N\}$	$\text{negl}(n)$	关于 $n$ 的可忽略函数
$\mathbf{x}$	列向量	$\text{poly}(n)$	关于 $n$ 的多项式函数
$\tilde{\mathbf{x}}_i$	$\mathbf{x}_i$ 的正交向量	$\ \cdot\ $	欧几里得范数
$\mathbf{X}$	矩阵	$\ \cdot\ _\infty$	无穷范数
$\mathbf{x} \sim D$	变量 $\mathbf{x}$ 服从 $D$ 分布	$\mathbf{X} \parallel \mathbf{Y}$	矩阵 $\mathbf{X}$ 和 $\mathbf{Y}$ 的级联
$\leftarrow_{\mathbb{R}} D$	从 $D$ 分布中随机选取元素		

### 1.2 格

定义1(格) 设 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m$ 是 $n$ 维欧式空间 $\mathbb{R}^n$ 上 $m$ 个线性无关的向量,则格 $L$ 被定义为 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m$ 上所有整系数线性组合所构成的集合,表示为 $L = \{a_1 \mathbf{b}_1 + a_2 \mathbf{b}_2 + \dots + a_m \mathbf{b}_m \mid (a_1, a_2, \dots, a_m) \in \mathbb{Z}_q^n\}$ ,而 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m$ 称为格 $L$ 的一组基。

定义2( $q$ 元格) 设 $q, m, n \in \mathbb{Z}, \mathbf{A} \in \mathbb{Z}_q^{n \times m}$ ,向量 $\mathbf{u} \in \mathbb{Z}_q^n, q$ 元格表示为:

$$\mathbf{A}_q^\perp(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}_q^m : \mathbf{A}\mathbf{e} = \mathbf{0} \pmod{q}\}$$

$$\mathbf{A}_q^u(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}_q^m : \mathbf{A}\mathbf{e} = \mathbf{u} \pmod{q}\}$$

$$\mathbf{A}_q^\perp(\mathbf{A}^\top) = \{\mathbf{y} \in \mathbb{Z}_q^m : \mathbf{y} = \mathbf{A}^\top \mathbf{e} \pmod{q}, \forall \mathbf{e} \in \mathbb{Z}_q^n\}$$

定义3(离散高斯分布) 给定实向量 $\mathbf{c} \in \mathbb{R}^m$ ,任意实数 $s > 0$ ,则格 $L$ 上以 $\mathbf{c}$ 为中心、以 $s$ 为参数的离散高斯分布密度函数表示为:

$$\forall \mathbf{x} \in L, \rho_{s, \mathbf{c}} = \exp\left(-\pi \left(\frac{\|\mathbf{x} - \mathbf{c}\|}{s}\right)^2\right)$$

当 $s = 1, \mathbf{c} = \mathbf{0}$ 时,格 $L$ 上任意一点 $\mathbf{x}$ 的离散高斯分布表示为:

$$D_{L, s, \mathbf{c}}(\mathbf{x}) = \frac{\rho_{s, \mathbf{c}}(\mathbf{x})}{\sum_{\mathbf{y} \in L} \rho_{s, \mathbf{c}}(\mathbf{y})}$$

### 1.3 格上困难问题

**定义 4 (SIS 问题)** 给定模数  $q \in \mathbb{Z}$ 、实数  $\beta$  和矩阵  $A \in \mathbb{Z}_q^{n \times m}$ , 找到一个非零向量  $e \in \mathbb{Z}^m$  且  $\|e\| \leq \beta$ , 满足  $Ae = 0 \pmod{q}$ 。

**定义 5 (ISIS 问题)** 给定模数  $q \in \mathbb{Z}$ 、实数  $\beta$ 、 $u \in \mathbb{Z}_q^n$  和矩阵  $A \in \mathbb{Z}_q^{n \times m}$ , 找到一个非零向量  $e \in \mathbb{Z}^m$  且  $\|e\| \leq \beta$ , 满足  $Ae = u \pmod{q}$ 。

**定义 6 (LWE 问题)** 给定模数  $q \in \mathbb{Z}$ 、 $\alpha \in \mathbb{R}^+$ 、向量  $u \in \mathbb{Z}_q^n$  和矩阵  $A \in \mathbb{Z}_q^{n \times m}$ ,  $\chi_\alpha$  表示  $\mathbb{Z}_q$  上的离散高斯分布。随机选择  $e \leftarrow_{\mathcal{R}} \chi_\alpha^m$ ,  $e \in \mathbb{Z}_q^m$ , 则:

1) LWE 搜索问题为: 求出向量  $t \in \mathbb{Z}_q^m$ , 使得等式  $u = At + e$  成立。

2) LWE 判定问题为: 判断向量  $u \in \mathbb{Z}_q^n$  是由  $u \leftarrow_{\mathcal{R}} \mathbb{Z}_q^n$  还是由  $u = At + e$  计算得到。

### 1.4 抽样函数

**引理 1<sup>[15]</sup>** 给定正数  $n, q = \text{poly}(n), m > 5n \ln q$ , 则存在一个多项式时间算法  $\text{TrapGen}(1^n, 1^m, q)$ , 产生一个矩阵  $A \in \mathbb{Z}_q^{n \times m}$  和一个陷门基  $T_A \subset A_q^\perp(A)$ , 矩阵  $A$  的分布统计接近于  $\mathbb{Z}_q^{n \times m}$  上的均匀分布, 并且  $\|T_A\| \leq O(\sqrt{n \ln q}) = O(\sqrt{m})$  以极大概率成立。

**引理 2<sup>[7]</sup>** 给定  $n \in \mathbb{Z}, q \geq 2, m \geq \lceil 6n \ln q + n \rceil$ , 矩阵  $C \in \mathbb{Z}_q^{n \times n}, A \in \mathbb{Z}_q^{n \times m}$ , 则存在一个多项式时间算法  $\text{SuperSamp}(1^n, 1^m, q, A, C)$ , 产生格基  $T_B \subset A_q^\perp(B)$  和矩阵  $B \in \mathbb{Z}_q^{n \times m}$  满足  $AB^T = C$ , 并且同时满足  $\|T_B\| \leq m^{1.5} \cdot \omega(\sqrt{\ln m}), \|T_B\| \leq m \cdot \omega(\sqrt{\ln m})$ 。

**引理 3<sup>[16]</sup>** 给定矩阵  $A \in \mathbb{Z}_q^{n \times m_1}, T_A \subset A_q^\perp(A), B \in \mathbb{Z}_q^{n \times m_2}$  以及一个实数  $s \geq \|T_A\| \cdot \omega(\sqrt{\ln m})$ , 令  $A' = (A \| B) \in \mathbb{Z}_q^{n \times (m_1 + m_2)}$ , 存在一个概率多项式算法  $\text{ExtRandBasis}(A', T_A, s)$  输出一个格基  $T_{A'} \subset A_q^\perp(A')$ , 且同时满足  $\|T_{A'}\| \leq s(m_1 + m_2), \|T_{A'}\| \leq s\sqrt{(m_1 + m_2)}$ 。

**引理 4<sup>[17]</sup>** 给定矩阵  $A \in \mathbb{Z}_q^{n \times m}, T_A \subset A_q^\perp(A)$ 、实数  $s \geq \|T_A\| \cdot \omega(\sqrt{\ln m})$  和向量  $u \in \mathbb{Z}_q^n$ , 则存在一个多项式时间算法  $\text{SamplePre}(A, T_A, s, u)$  输出一个向量  $e \sim D_{\mathbb{Z}^m, s}, e \in \mathbb{Z}^m$ , 满足  $Ae = u \pmod{q}$ 。

### 1.5 非交互零知识证明

2013 年, LAGUILLAUMIE 等人给出一个关于 ISIS 问题的零知识证明<sup>[7]</sup>:

$$R_{\text{ISIS}} = \left\{ (A, y, \beta; x) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n \times \mathbb{R} \times \mathbb{Z}_q^m : \right. \\ \left. Ax = y, \|x\| < \beta \right\}$$

2015 年, NGUYEN 等人给出一个关于 Split-SIS 问题上的零知识证明<sup>[8]</sup>:

$$R_{\text{Split-SIS}} = \left\{ (A, y, \beta, N; x_1, h) \in \mathbb{Z}_q^{n \times 2m} \times (\mathbb{Z}_q^n \times \mathbb{Z}^m) \times \right. \\ \left. \mathbb{R} \times \mathbb{Z} \times \mathbb{Z}_q^m \times \mathbb{Z} : A_1 x_1 + h A_2 y_2 = y_1, \right. \\ \left. y = (y_1, y_2), \|x_1\| < \beta \sqrt{m}, h \in [N] \right\}$$

由 ISIS 和 LWE 的对偶性可得关于 LWE 的零知识证明<sup>[18]</sup>:

$$R_{\text{LWE}} = \left\{ (A, b, \alpha; t) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n \times \mathbb{R} \times \mathbb{Z}_q^n : \right. \\ \left. \|b - A^T t\| < \alpha q \sqrt{m} \right\}$$

同时, 也可构造一个  $\gamma = \max(\alpha q \sqrt{m}, \beta)$  的 eLWE 关系的零知识证明<sup>[18]</sup>:

$$R_{\text{eLWE}} = \left\{ (A, b, \gamma; t, e, x) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n \times \mathbb{R} \times \mathbb{Z}_q^n \times \mathbb{Z}^{2m} : \right. \\ \left. b = At + pe + x, \|x\| < \gamma, \|e\| < \gamma \right\}$$

以上零知识证明都可经过 Fiat-Shamir 变换转换为非交互零知识证明 (Non-Interactive Zero-Knowledge Proofs, NIZKP)。

## 2 格上高效的动态群签名方案

### 2.1 动态群签名定义和安全模型

#### 2.1.1 群签名定义

一个动态群签名算法<sup>[8, 13-14, 19-20]</sup> 由以下多项式时间算法组成:

1)  $\text{GSetup}(1^n, 1^N) \rightarrow pp$ : 输入群签名系统的安全参数  $n$  和群成员数量  $N$ , 算法产生公共参数  $pp$ 。

2) 密钥生成算法:

(1)  $\text{GKgen}_{\text{Gm}}(pp) \rightarrow ((gmsk, gmpk), (gtpk, gtsk))$ : 该算法由群管理员执行, 输入公共参数  $pp$ , 生成群管理员的主密钥对  $(gmsk, gmpk)$  和追踪密钥对  $(gtpk, gtsk)$ 。

(2)  $\text{GKgen}_{\text{User}}(pp) \rightarrow (usk_i, upk_i)$ : 该算法由群成员执行, 输入公共参数  $pp$ , 生成群成员的密钥对  $(usk_i, upk_i)$ 。

3)  $\text{GUJoin}(pp, gpk, gmsk) \rightarrow (cert_i, reg_i)$ : 该算法是由群管理员和用户执行的交互式算法, 输入公共参数  $pp$ 、群管理员的主私钥  $gmpk$  和群公钥  $gpk$ ,  $gpk = (gmpk, gtpk, upk_i)$ 。若算法执行成功, 则群管理员颁发成员证书  $cert_i$  和计算用户的撤销标记  $reg_i$ , 用户加入成功。

4)  $\text{GSig}(gpk, usk_i, cert_i, m) \rightarrow \Sigma$ : 该算法由群成员执行, 将  $(gpk, usk_i, cert_i, m)$  作为输入参数, 输出一个由用户  $usk_i$  在消息  $m$  上的签名。

5)  $\text{GRevoke} \rightarrow 0/1$ : 该算法由群管理员或用户执行, 主要是群管理员将撤销标记加入到撤销列表  $RL$  中, 并更新和发布撤销列表, 若算法输出为 1 则撤销成功, 否则输出为 0。



6)  $GVerify(gpk, m, \Sigma, RL) \rightarrow 0/1$ : 该算法为确定性算法, 并由验证者执行, 将  $(gpk, m, \Sigma, RL)$  作为输入参数来判断该签名的签名者是否已被撤销, 若未被撤销, 则判定该签名是否是消息  $m$  上的合法签名, 若是, 则输出为 1, 否则输出为 0。

7)  $GOpen(gpk, gtsk, m, \Sigma) \rightarrow Id_i$ : 该算法为确定性算法, 由群管理员执行, 输入参数  $(gpk, gtsk, m, \Sigma)$ , 返回对消息  $m$  做签名的用户者身份  $Id_i$ 。

### 2.1.2 群签名安全模型

一个群签名方案必须满足正确性、匿名性和追踪性这 3 个安全特性<sup>[6-8, 13-14]</sup>, 其中, 正确性是群签名中最基本的要求, 匿名性和追踪性是对群签名的安全性要求。

1) 在正确性方面, 要求方案满足签名验证正确性和签名打开正确性<sup>[6-8, 13-14]</sup>, 其中: 签名验证正确性是指按算法步骤产生的签名一定能通过验证算法的验证; 签名打开正确性是指按算法步骤产生的签名一定能被群管理员打开。

2) 匿名性是指任何获得签名的人都不能通过签名判断出真正的签名者身份(除群管理员外)。匿名性又分为弱匿名性(CPA-匿名)和完全匿名性(CCA-匿名)<sup>[6-8]</sup>。在 CCA-匿名的游戏中, 敌手能够进行签名打开查询, 而在 CPA-匿名的游戏中, 敌手不能进行签名打开查询。显然, CCA-匿名游戏中的敌手比 CPA-匿名游戏中的敌手具有更强的攻击能力, 因此, 满足 CCA-匿名的群签名方案比满足 CPA-匿名的群签名方案更安全。本文的群签名方案是满足 CCA-匿名的。

3) 追踪性是指群成员产生的合法签名能够被群管理员打开, 而伪造的签名, 即使是由合谋的群成员共同伪造的签名, 也不能够被群管理员打开。追踪性又分为 CPA-追踪和 CCA-追踪, 两者的区别在于游戏中敌手是否能够进行腐败查询。本文方案的追踪性是满足 CCA-追踪的。

正确性具体的形式化定义如下:

**定义 7(正确性)** 对于任意  $n, N$ , 所有由  $GKgen_{Gm}(\cdot)$ 、 $GKgen_{User}(\cdot)$ 、 $GUJoin(\cdot)$  产生的  $(gpk, cert_i, gmsk, gtsk, usk_i)$ 、消息  $m, i \in [N]$ , 若  $GSig(gpk, usk_i, cert_i, m) \rightarrow \Sigma$ , 则  $GVerify(gpk, m, \Sigma) = 1 \Leftrightarrow reg_i \in RL$  且  $GOpen(gpk, gtsk, m, \Sigma) = Id_i$ 。

关于匿名性, 下面给出一个敌手  $A$  和挑战者  $B$  之间的游戏:

1) 参数建立。输入任意正整数  $n, N$ , 挑战者  $B$  执行算法  $GSetup(\cdot)$ 、 $GKgen_{Gm}(\cdot)$ 、 $GKgen_{User}(\cdot)$ 、 $GUJoin(\cdot)$  产生  $(gpk, cert_i, gmsk, gtsk, usk_i)$ , 并将群公钥  $gpk$  发送给敌手  $A$ 。

2) 查询。敌手  $A$  可以做签名、撤销、腐败和签名打开查询, 查询过程如下:

(1) 签名查询: 敌手  $A$  输入用户身份  $Id_i$ 、任意消息  $m$ , 签名预言机用  $(cert_i, usk_i)$  产生用户  $Id_i$  的签名, 并将签名返回给敌手  $A$ 。

(2) 腐败查询: 敌手  $A$  输入用户身份  $Id_i$ , 腐败预言机返回用户  $Id_i$  的私钥给敌手  $A$ , 挑战者  $B$  将腐败的用户加入到腐败集合  $U_a$ 。

(3) 撤销查询: 敌手  $A$  可以查询任意用户的撤销标记, 挑战者  $B$  将被查询过的标记加入到集合  $U$ 。

(4) 签名打开查询: 敌手  $A$  输入  $(m, \Sigma)$ , 签名打开预言机返回用户身份  $Id_i$ 。

3) 挑战。敌手  $A$  选择未被查询的消息  $m$ , 并同时选择 2 个用户  $d_0, d_1 \notin U_a \cup U_c$ , 其中, 用户的私钥和证书分别为  $(usk_0^*, cert_0^*)$  和  $(usk_1^*, cert_1^*)$ , 将这些信息发送给挑战者  $B$ 。挑战者  $B$  选择  $b \leftarrow_R \{0, 1\}$ , 用  $(usk_b^*, cert_b^*)$  计算挑战签名  $\Sigma^*$ , 将其发送给敌手  $A$ 。

4) 受限查询。敌手仍可做一些查询, 但不能对用户  $d_0, d_1$  做腐败、撤销和签名打开查询。

5) 输出。敌手  $A$  输出  $b^*$ 。若  $b^* = b$ , 称敌手获胜。

敌手  $A$  在上述游戏中获胜的优势定义为:

$$Adv_A^{anony} = |\Pr[b^* = b] - 1/2|。$$

**定义 8(匿名性)** 对于任意概率多项式时间的敌手  $A$ , 若  $Adv_A^{anony} \leq \text{negl}(n)$ , 则称群签名方案具有 CCA-匿名性。

关于追踪性, 下面给出一个敌手  $A$  与挑战者  $B$  之间的游戏。在游戏中, 敌手  $A$  的目标是伪造一个签名, 管理员利用签名打开算法不能打开伪造的签名。敌手  $A$  能够腐化群管理员, 在查询阶段也能腐化用户, 并可利用加入算法产生一些虚拟成员。游戏过程如下:

1) 参数建立。挑战者  $B$  执行算法  $GSetup(\cdot)$ 、 $GKgen_{Gm}(\cdot)$ 、 $GKgen_{User}(\cdot)$ , 产生  $(gpk, cert_i, gmsk, gtsk, usk_i)$ , 将群公钥发送给敌手  $A$ , 并设置  $U_a = \emptyset$ 。

2) 查询。敌手  $A$  可以做签名和腐败用户的查询, 查询过程如下:

(1) 签名查询: 敌手  $A$  输入任意消息  $m$  和用户身份  $Id_i$ , 签名预言机可以返回对应的签名  $\Sigma$ , 并将查询过的签名加入到集合  $U_{sig}$  ( $U_{sig}$  是由用户身份  $Id_i$ 、消息  $m$  和对应消息签名  $\Sigma$  组成的集合)。

(2) 腐败查询: 敌手  $A$  询问任意用户的私钥时, 挑战者  $B$  将询问过的用户加入到集合  $U_a$ , 并返回对应用户的私钥。

3) 伪造。敌手  $A$  利用其所拥有的信息产生一个消息签名对  $(m^*, \Sigma^*)$  和撤销列表  $RL^*$ , 如果  $GVerify(gpk, m^*, \Sigma^*, RL^*) \rightarrow 1$ , 对于  $Id_i \notin U_a, (Id_i, m^*,$

$\Sigma^* \notin U_{\text{sig}}$ , 签名打开失败同时  $\text{GOpen}(\text{gpk}, \text{gtsk}, m^*, \Sigma^*) = Id_i$  且  $Id_i \in U_a/\text{RL}$ , 则称敌手  $\mathcal{A}$  获胜。

敌手  $\mathcal{A}$  在上述游戏中获胜的优势可定义为  $\text{Adv}_{\mathcal{A}}^{\text{trace}}$ 。

**定义 9 (追踪性)** 若对于任意概率多项式时间的敌手  $\mathcal{A}$ ,  $\text{Adv}_{\mathcal{A}}^{\text{trace}} \leq \text{negl}(n)$ , 则称群签名方案具有 CCA-追踪性。

## 2.2 本文方案

本文将文献[11, 14]提出的动态群签名思想引入到文献[8]的群签名方案中, 提出一个具有加入和撤销机制的格上完全动态群签名方案。该方案包含 2 个密钥生成阶段: 第 1 个阶段是群管理员的密钥生成阶段, 其中使用文献[8]的 GPV 陷门生成算法和正交抽样算法产生群管理员的主密钥和追踪密钥; 第 2 个阶段是群成员的密钥生成阶段, 其中使用文献[11]的离散高斯采样算法, 采取满足一定条件的短向量作为群成员的签名私钥。在加入阶段, 使用 GPV 的格基扩展技术和原像采样算法生成群成员证书; 在签名阶段, 采用和文献[6-8, 14]类似的对偶 LWE 算法; 撤销阶段分为用户主动撤销和群管理员撤销群成员, 两者共同之处是都将撤销标记加入到撤销列表中。

对于方案参数, 本文仍按照文献[8]进行选择:  $n$  为安全参数;  $\delta$  为实数;  $N$  为群成员数;  $m = 6n^{1+\delta}$ ,  $q = m^{2.5} \cdot \max\left(m^6 \cdot \omega\left((\text{lb } m)^{2.5}\right), 4N\right)$  且满足  $n^{1+\delta} > \lceil (n+1) \text{lb } q + n \rceil$ ,  $\beta = m^{1.5} \cdot \omega\left((\text{lb } m)^{1.5}\right)$ ;  $s = m \cdot \omega(\text{lb } m)$ ,  $p = m^{2.5} \beta = m^4 \cdot \omega\left((\text{lb } m)^{1.5}\right)$ ,  $\alpha = 2\sqrt{m}/q$ ,  $\eta = \max(\beta, \alpha q)\sqrt{m} = m^2 \cdot \omega\left((\text{lb } m)^{1.5}\right)$ 。

### 1) 系统建立

$\text{GSetup}(1^n, 1^N) \rightarrow pp$ :  $n$  为系统安全参数,  $N$  为群成员个数, 该算法产生的随机预言机为  $H: \{0, 1\}^* \rightarrow \{0, 1\}^t$ , 其中,  $t = \omega(\text{lb } n)$ ,  $A_0, A_1 \leftarrow_{\mathbb{R}} \mathbb{Z}_q^{n \times m}$ , 则参数  $pp = \{n, N, m, q, s, p, \alpha, \beta, \eta, A_0, A_1\}$ 。

### 2) 密钥生成算法

(1)  $\text{GKGen}_{\text{Gm}}(pp) \rightarrow ((\text{gmsk}, \text{gmpk}), (\text{gtpk}, \text{gtsk}))$ : 群管理员首先计算  $(A, T_A) \leftarrow \text{TrapGen}(1^n, 1^m, q)$ , 其中,  $A \in \mathbb{Z}_q^{n \times m}$ ,  $T_A$  为格  $A_q^\perp(A)$  的一个短基, 然后计算  $(B, T_B) \leftarrow \text{SuperSamp}(1^n, 1^m, q, A, 0)$ , 其中,  $B \in \mathbb{Z}_q^{n \times m}$ ,  $T_B$  为格  $A_q^\perp(B)$  的一个短基, 则群管理员的主私钥  $\text{gmsk} = T_A$ , 主公钥  $\text{gmpk} = A$ , 追踪私钥  $\text{gtsk} = T_B$ , 追踪公钥  $\text{gtpk} = B$ 。

(2)  $\text{GKGen}_{\text{User}}(pp) \rightarrow (usk, upk)$ : 用户在格上利用离散高斯采样算法<sup>[17]</sup>, 采取一个短向量  $z_i \in \mathbb{Z}_q^n$ , 再随机选取矩阵  $F \leftarrow_{\mathbb{R}} \mathbb{Z}_q^{m \times n}$ , 并计算满足  $v_i = F \cdot z_i \in \mathbb{Z}_q^m$ ,

则用户的签名私钥为  $z_i$ , 用户公钥为  $v_i$ 。

由此可知群公钥  $\text{gpk} = (A, B, F, pp, v_i)$ 。

3)  $\text{GUJoin}(pp, \text{gpk}, \text{gmsk}) \rightarrow (\text{cert}_i, \text{reg}_i)$

用户先利用 PKI 中注册过的密钥  $(\text{pusk}[i], \text{pupk}[i])$  对  $v_i$  做普通的数字签名:  $\text{sig}_i = \text{Sig}_{\text{pusk}[i]}(v_i)$ , 再将  $(v_i, \text{sig}_i)$  发送给群管理员。群管理员验证  $v_i$  是否已被注册, 并且用  $\text{pupk}[i]$  验证该签名的合法性。若该签名合法或是已被注册过, 则终止加入过程; 否则群管理员做以下工作:

首先群管理员为用户选取新的身份, 令  $Id_i = i, i \in [N]$ , 计算  $A_{Id_i} = [A \| A_0 + Id_i A_1] \in \mathbb{Z}_q^{n \times 2m}$ ,  $T_{A_{Id_i}} \leftarrow \text{ExtRandBasis}(A_{Id_i}, T_A, s)$ , 其中,  $T_{A_{Id_i}} \in \mathbb{Z}_q^{m \times m}$  且满足  $\|\tilde{T}_{A_{Id_i}}\| \leq s\sqrt{2m}$ , 令  $u_i = Av_i \in \mathbb{Z}_q^n$ ; 然后计算  $(x_0, x_1) \leftarrow \text{SamplePre}(A_{Id_i}, T_{A_{Id_i}}, \beta, u_i)$  且  $x_0, x_1 \in D_{\mathbb{Z}_q^{n \times \beta}}$ ; 最后计算群成员的撤销标记  $\text{reg}_i = A_1 v_i \in \mathbb{Z}_q^n$ 。由以上步骤产生群成员证书  $\text{cert}_i = (Id_i, x_0, x_1)$ , 群管理员将  $(v_i, \text{cert}_i, \text{reg}_i, \text{sig}_i)$  存储在注册列表中, 并将证书通过安全信道发送给群成员。

4)  $\text{GSig}(\text{gpk}, usk, \text{cert}, m) \rightarrow \Sigma$

(1) 群成员选取  $s_0 \leftarrow_{\mathbb{R}} \mathbb{Z}_q^n$ ,  $e_0 \leftarrow_{\mathbb{R}} \chi_a^m$ , 计算  $c_0 = B^T s_0 + p e_0 + x_0$ , 并产生一个关于  $(s_0, e_0, x_0)$  的非交互零知识证明  $\pi_0$ , 使得  $(B, c_0, \eta; s_0, e_0, x_0) \in R_{\text{LWE}^0}$ 。

(2) 令  $\bar{\beta} = \lfloor \beta \rfloor$ ,  $l = \lceil \log_{\bar{\beta}} N \rceil$ , 定义  $u_i = Av_i \in \mathbb{Z}_q^n$ ,  $b = A_1 x_1 \in \mathbb{Z}_q^n$ ,  $D = (b, \bar{\beta} b, \bar{\beta}^2 b, \dots, \bar{\beta}^{l-1} b) \in \mathbb{Z}_q^{n \times l}$ ,  $Id_i$  的向量表示  $id_i = (id_0, id_1, \dots, id_{l-1}) \in \mathbb{Z}_{\bar{\beta}}^l$ , 并产生一个关于  $(x_0, e_0, Id_i)$  的非交互零知识证明  $\pi_1$ , 满足  $Ac_0 + A_0 x_1 - u_i = (pA) e_0 - D \cdot id_i$ ,  $Ac_0 = (pA) e_0 + Ax_0$ 。

(3) 群成员选取  $e_1 \leftarrow_{\mathbb{R}} \chi_a^m$ , 计算  $c_1 = B^T \text{reg}_i + e_1$ , 同时产生一个关于  $\text{reg}_i$  满足  $(A, c_1, a; \text{reg}_i) \in R_{\text{LWE}}$  的非交互零知识证明  $\pi_2$ 。

(4) 群成员产生一个关于  $z_i$  并满足  $(F, v_i, \beta; z_i) \in R_{\text{ISIS}}$  的非交互零知识证明  $\pi_3$ 。

(5) 输出签名  $\Sigma = (c_0, c_1, x_1, \pi_0, \pi_1, \pi_2, \pi_3)$ 。

5)  $\text{GRevoke} \rightarrow 0/1$

(1) 若是群管理员执行该算法, 则将撤销标记  $\text{reg}_i$  加入到撤销列表中, 即令  $\text{RL} = \text{RL} \cup \{\text{reg}_i\}$ , 然后发布撤销列表, 撤销成功并返回 1; 否则返回 0。

(2) 若是用户执行该算法, 则将  $(v_i, \text{cert}_i, \text{reg}_i, \text{sig}_i)$  发送给群管理员, 向群管理员提交撤销申请, 群管理员对用户进行身份验证, 若验证成功, 则将用户的撤销

标记  $\text{reg}_i$  加入到撤销列表中,  $\text{RL} = \text{RL} \cup \{\text{reg}_i\}$ , 然后发布撤销列表, 撤销成功返回 1, 否则, 返回 0。

6)  $\text{GVerify}(gpk, m, \Sigma, \text{RL}) \rightarrow 0/1$

验证者首先查看  $\text{RL}$ , 对任意的  $\text{reg}_j \in \text{RL}$ , 计算  $e'_1 = c_1 - B^T \text{reg}_j$ , 即  $e'_1 = B^T(\text{reg}_i - \text{reg}_j) + e$ , 若  $\text{reg}_i = \text{reg}_j$  且  $e'_1 \leq \alpha q \sqrt{m}$ , 则说明该验证者已被撤销, 验证者则拒绝接受签名; 反之, 分析签名, 验证  $\pi_0 \sim \pi_3$  有效且满足  $\|x_1\| \leq \beta \sqrt{m}$ ,  $A_1 x_1 \neq 0$ , 则验证成功, 若签名为合法签名, 输出 1; 反之, 输出 0。

7)  $\text{GOpen}(gpk, gtsk, m, \Sigma) \rightarrow Id_i$

群管理员使用追踪密钥  $T_B$  对密文  $c_0$  解密, 得到  $x_0$ , 计算  $y_0 = A_1 x_1$ ,  $y_1 = Ax_0 + A_0 x_1$ , 若  $y_0 \neq 0$ , 能够找到一个  $Id_i$  同时满足  $y_1 + Id_i y_0 = u_i$  则该算法输出  $Id_i$ ; 否则输出  $\perp$ 。

### 3 安全性分析

#### 3.1 正确性证明

对本文方案的验证正确性和打开正确性进行证明。

##### 3.1.1 验证正确性证明

对每个  $\text{reg}_j \in \text{RL}$ , 计算  $e'_1 = c_1 - B^T \text{reg}_j = B^T(\text{reg}_i - \text{reg}_j) + e_1$ ,  $e'_1 \leq \alpha q \sqrt{m}$ , 若存在用户  $i$  使得  $\text{reg}_i = \text{reg}_j$  且  $e'_1 \leq \alpha q \sqrt{m}$ , 则说明验证不通过, 拒绝接受签名; 反之, 接受签名。又由于  $x_1 \sim D_{\mathbb{Z}^m, \beta}$ , 则由文献[8]的引理 3 可知,  $\|x_1\| \leq \beta \sqrt{m} \Pr(A_1 x_1 = 0) \leq O(q^{-n})$ , 又由文献[8]可知  $(\pi_0, \pi_1, \pi_2, \pi_3)$  具有完备性, 所以, 签名能通过  $\text{GVerify}$  算法的检验, 该签名为合法签名。

##### 3.1.2 打开正确性证明

因为  $c_0 = B^T s_0 + p e_0 + x_0$ , 群管理员使用  $T_B \in \mathbb{Z}_q^{m \times m}$  对  $c_0$  解密, 即有  $T_B^T c_0 = T_B^T (p e_0 + x_0) \bmod q$ 。由文献[8]的引理 1 和引理 2 可知  $\|p e_0 + x_0\| \leq 3m^6 \cdot \omega((\ln m)^3)$ , 又由本文引理 2 可知  $\|T_B\| \leq m^{1.5} \cdot \omega(\sqrt{\ln m})$ , 易得  $\|T_B^T (p e_0 + x_0)\| \leq 3m^8 \cdot \omega((\ln m)^{3.5}) \ll q$ , 因此, 当  $\|T_B^T (p e_0 + x_0)\| < q/2$  时, 等式  $T_B^T c_0 = T_B^T (p e_0 + x_0) \bmod q$  成立, 又因为  $T_B \in \mathbb{Z}_q^{m \times m}$  为满秩矩阵, 所以可利用高斯消元法得到  $x' = p e_0 + x_0$ 。此外, 由  $\beta = m^{1.5} \omega((\ln m)^{1.5})$ ,  $p = m^{2.5} \beta$  的选择, 存在  $\|x_0\| \leq \|x'\| < p/2$ , 通过计算  $x' = p e_0 + x_0$  可求解出  $x_0$ 。因此, 可利用追踪密钥  $T_B$  解密  $c_0$  得到  $x_0$ , 进而计算得到  $Id_i$ , 即找到签名者。

#### 3.2 安全性证明

本文方案满足 CCA-匿名性和 CCA-追踪性, 并且能够抵抗陷害攻击。下文将对其匿名性、追踪性、安全性和抗陷害攻击性进行证明。

##### 3.2.1 匿名性证明

**定理 1** 在随机预言机模型下, 本文方案在 LWE 假设下是 CCA-匿名的。

证明: 通过一系列的游戏  $G_0 \sim G_5$  证明。

$G_0$  游戏过程如下:

1) 挑战者  $\mathcal{B}$  按照本文方案获得群公钥  $gpk = (A, B, F, pp, v_i)$ 、成员证书  $\text{cert}_i = (Id_i, x_0, x_1)$ 、群成员的私钥  $\text{usk}_i = z_i, i \in [N]$  和追踪私钥  $gtsk = T_B$ , 并将群公钥、成员证书和群成员私钥发送给敌手。

2)  $\mathcal{B}$  初始化撤销链表  $\text{RL} = \emptyset$ 、腐败用户集合  $U_a = \emptyset$  和撤销查询集合  $U_c = \emptyset$ 。

3) 敌手  $\mathcal{A}$  在查询阶段可以对任意用户的任意消息  $m$  的签名进行查询, 对对应消息上的签名进行打开查询, 还可以更新  $U_a$  和  $U_c$ 。

4) 敌手  $\mathcal{A}$  输出选择的消息  $m^*$  和身份标识  $Id_0$ ,  $Id_1 \in [N]$ , 满足  $Id_0, Id_1 \notin U_a \cup U_c$  且  $\text{reg}_{d_0}, \text{reg}_{d_1} \notin \text{RL}$ 。

5) 挑战者选择  $b \leftarrow_{\mathcal{R}} \{0, 1\}$ , 以  $Id_b$  的身份按照本文方案计算  $\Sigma^* = (c_0^*, c_1^*, \pi_0^*, \pi_1^*, \pi_2^*, \pi_3^*)$ , 然后将该签名发送给敌手  $\mathcal{A}$ 。此后, 敌手  $\mathcal{A}$  还可以做关于  $Id_i \neq Id_b$  签名、私钥、打开和撤销标记查询。

$G_1$  游戏过程与  $G_0$  类似, 除了  $G_1$  中是利用 NIZKP 模拟器生成  $\pi_0^*, \pi_1^*, \pi_2^*, \pi_3^*$  ( $G_0$  利用随机预言机), 则由 NIZKP 的性质可得,  $G_0$  和  $G_1$  是计算上不可区分的。

$G_2$  游戏过程与  $G_1$  类似, 除了  $x_1^* \leftarrow_{\mathcal{R}} D_{\mathbb{Z}^m, \beta}$ , 利用  $T_A$  计算  $x_0^*$ , 满足等式  $\overline{A}_{i_b}(x_0^*; x_1^*) = u_{i_b}$ , 又由  $\text{SamplePre}(\cdot)$  函数的性质<sup>[12-13]</sup>可知,  $G_2$  与  $G_1$  中选择的  $x_1^*$  是统计接近的。

$G_3$  游戏过程与  $G_2$  类似, 除了  $g_i \leftarrow_{\mathcal{R}} \mathbb{Z}_q^n$ , 计算  $c_1^* = B^T g_i + e_1$ , 输出签名  $\Sigma^* = (c_0^*, c_1^*, \pi_0^*, \pi_1^*, \pi_2^*, \pi_3^*)$ , 根据 LWE 的假设,  $G_2$  和  $G_3$  是统计不可区分的。

$G_4$  游戏过程与  $G_3$  类似, 除了  $d_0 \leftarrow_{\mathcal{R}} \mathbb{Z}_q^m$ , 计算  $c_0^* = d_0 + x_0^*$ , 由文献[8]可得,  $G_3$  和  $G_4$  不能通过计算区分, 则 LWE 判定问题难以求解, 因此,  $G_3$  和  $G_4$  是统计不可区分的。

$G_5$  游戏过程与  $G_4$  类似, 除了  $c_0^* \leftarrow_{\mathcal{R}} \mathbb{Z}_q^m, c_1^* \leftarrow_{\mathcal{R}} \mathbb{Z}_q^m$ , 在  $G_4$  中, 签名与身份的选取无关,  $b' = b$  的概率接近 1/2, 因此, 敌手  $\mathcal{A}$  获胜的优势可忽略。

综上所述, 在随机预言机模型下, 本文方案在 LWE 假设下是 CCA-匿名的。

##### 3.2.2 追踪性证明

**定理 2** 在随机预言机模型下, 本文方案在 ISIS 假设下是 CCA-追踪的。

证明: 假设敌手  $\mathcal{A}$  多项式时间内攻破本文方案的追踪性, 则可构造一格算法  $\mathcal{C}$  解决 ISIS 问题, 即给定矩阵  $A \in \mathbb{Z}_q^{n \times m}, u \in \mathbb{Z}_q^n$ , 寻找一个  $x \in \mathbb{Z}_q^m$ , 满足  $\|x\| \leq$



$\text{poly}(m)$ ,  $Ax = u \bmod q$ 。C下一步工作为:

1) GSetup( $1^n, 1^N$ )。首先计算 $(A, T_A) \leftarrow \text{TrapGen}(1^n, 1^m, q)$ ,  $(B, T_B) \leftarrow \text{SuperSamp}(1^n, 1^m, q, A, 0)$ , 然后选择 $F \leftarrow_{\mathbb{R}} \mathbb{Z}_q^{m \times n}$ , 高斯采样 $z_i \in \mathbb{Z}_q^n$ , 计算 $v_i = F \cdot z_i \in \mathbb{Z}_q^m$ , 并设置 $\text{RL} = \emptyset$ , 腐败用户集合 $U_a = \emptyset$ , 最后将 $\text{gpk} = (A, B, F, pp, v_i)$ , 追踪密钥 $\text{gtsk} = T_B$ 发送给敌手 $\mathcal{A}$ 。

2) GUJoin( $pp, \text{gmpk}, \text{gtpk}$ )。对 $i \in [N]$ , 当 $i \neq i^*$ 时, 首先对 $v_{i^*} \in \mathbb{Z}_q^m$ 做签名 $\text{sig}_{i^*} = \text{Sig}_{\text{pusk}[i]}(v_{i^*})$ , 并将 $(v_{i^*}, \text{sig}_{i^*})$ 发送到C, C随机选择 $R \leftarrow_{\mathbb{R}} \{-1, 1\}^{m \times m}$ , 从 $\text{Id}_i^* \leftarrow \{-4m^{2.5}N + 1, -4m^{2.5}N + 2, \dots, 4m^{2.5}N - 1\}$ 选择新身份, 计算 $(A_1, T_{A_1}) \leftarrow \text{TrapGen}(1^n, 1^m, q)$ ,  $A_0 = AR - \text{Id}_i^* A_1$ ; 然后计算 $A_{\text{Id}_i^*} = [A \| A_0 + \text{Id}_i^* A_1] \in \mathbb{Z}_q^{n \times 2m}$ ,  $T_{A_{\text{Id}_i^*}} \leftarrow \text{ExtRandBasis}(A_{\text{Id}_i^*}, T_A, s)$ , 其中 $T_{A_{\text{Id}_i^*}} \in \mathbb{Z}_q^{m \times m}$ 且满足 $\|\tilde{T}_{A_{\text{Id}_i^*}}\| \leq s\sqrt{2m}$ ; 再令 $u_{i^*} = Av_{i^*} \in \mathbb{Z}_q^n$ , 计算 $(x_0^*, x_1^*) \leftarrow \text{SamplePre}(A_{\text{Id}_i^*}, T_{A_{\text{Id}_i^*}}, \beta, u_{i^*})$ 且 $x_0^*, x_1^* \in D_{\mathbb{Z}^{2m}, \beta}$ , 并计算撤销标记 $\text{reg}_{i^*} = A_1 v_{i^*}$ ; 最后向用户 $i$ 发送成员证书 $\text{cert}_{i^*} = (\text{Id}_{i^*}, x_0^*, x_1^*)$ 。

3) 查询。敌手 $\mathcal{A}$ 先对用户进行腐败, 再做签名查询, 过程如下:

(1) 腐败。向预言机询问任意用户 $i \in [N]$ 的私钥, 将 $i$ 加入到集合 $U_a = \emptyset$ 中, 并返回 $z_i$ 。

(2) 签名询问。敌手 $\mathcal{A}$ 向预言机询问用户关于消息 $m$ 的签名, 并将签名发送给C。若 $\text{Id}_i = i$ ,  $i \notin [N]$ , 则C拒绝接受签名; 若 $\text{Id}_i = \text{Id}_{i^*}$ , C对消息 $m$ 进行签名并利用NIZKP模拟器产生 $\pi_0^* \sim \pi_3^*$ , 否则, 将在私钥询问阶段中用回答的签名私钥作为 $\text{Id}_i$ 对消息 $m$ 签名。

4) 伪造。设成功伪造有效签名 $\Sigma = (c_0, c_1, x_1, \pi_0, \pi_1, \pi_2, \pi_3)$ 的概率为 $\varepsilon$ , 利用随机预言机对 $z_i$ 和 $e_0, x_0, \text{Id}_i \leq 4\eta m^2$ 进行零知识提取, 并由文献[21]可得, 对于其提取成功的概率为 $\varepsilon(\varepsilon/q_h - 2^{-t})$ , 其中 $q_h$ 是敌手 $\mathcal{A}$ 访问hash函数的最大次数, 利用 $T_B$ 对密文 $c_0$ 解密, 得到 $e'_0, x'_0$ 。若 $(e'_0, x'_0) \neq (e_0, x_0)$ , 则有 $Ac_0 =$

$pAe_0 + Ax_0 = pAe'_0 + Ax'_0$ , 因此 $x = p(e_0 - e'_0) + (x_0 - x'_0)$ 是SIS问题的一个解, 且 $\|x\| \leq 8(p+1)\eta m^2 = m^8 \omega((\text{lb } m)^3)$ ;

若 $(e'_0, x'_0) = (e_0, x_0)$ 且 $u_i = Av_i \in \mathbb{Z}_q^n$ , 则有 $Ax_0 + A_0 x_1 + \text{Id}_i A_1 x_1 = u_i$ , 其中 $\text{Id}_i = \sum_{i=0}^{l-1} \text{Id}_i \beta^i$ ,  $\|\text{Id}_i\| < 4m^{2.5}N < q$ 。

又因为 $A_1 x_1 \neq 0$ ,  $q$ 是素数, 所以能够求解出 $\text{Id}_i$ 。若 $\text{Id}_i \neq \text{Id}_{i^*}$ , 则终止; 否则输出 $x = x_0 + Rx_1$ 为所给的ISIS问题的解。因为 $\text{Id}_i \leftarrow \{-4m^{2.5}N + 1, -4m^{2.5}N + 2, \dots, 4m^{2.5}N - 1\}$ , 所以 $\text{Id}_i = \text{Id}_{i^*}$ 的概率至少为 $1/8m^{2.5}N$ 。因为 $\text{Id}_i = \text{Id}_{i^*}$ 时 $Ax_0 + A_0 x_1 + \text{Id}_i A_1 x_1 = A(x_0 + Rx_1) = u_i$ , 所以ISIS的解 $\|x\| \leq \eta m^{2.5} \omega(\sqrt{\text{lb } m}) = m^{4.5} \omega((\text{lb } m)^2)$ 。

由以上所证得, C解决ISIS问题的概率至少为 $\varepsilon(\varepsilon/q_h - 2^{-t})/8m^{2.5}N$ , 若 $\varepsilon$ 是不可忽略的, 则 $\varepsilon(\varepsilon/q_h - 2^{-t})/8m^{2.5}N$ 也是不可忽略的。

综上所述, 在随机预言机模型下, 本文方案在ISIS假设下是CCA-追踪的。

### 3.2.3 抗陷害攻击

在本文方案中, 用户 $i$ 的私钥是其通过高斯采样算法采取的短向量 $z_i \in \mathbb{Z}_q^n$ , 进而选取 $F \leftarrow_{\mathbb{R}} \mathbb{Z}_q^{m \times n}$ 并计算用户 $i$ 的公钥 $v_i = F \cdot z_i \in \mathbb{Z}_q^m$ 。若群管理员或其他合谋群成员想伪造 $i$ 的签名, 就必须产生一个非交互零知识 $\pi_3$ , 又由于零知识证明 $\pi_3$ 具有可靠性, 不知道 $z_i$ 的群管理员或其他群成员无法产生一个能通过验证的 $\pi_3$ , 因此本文方案能够抵抗陷害攻击。

## 4 效率分析

选取以下4个方案: 文献[8]格上高效的群签名方案, 文献[11]格上具有高效协议和动态群签名的签名方案, 文献[13]格上具有本地撤销机制的群签名方案, 文献[14]适合大群组的格基动态群签名方案, 从公私钥大小、签名大小、加入代价、撤销代价以及是否为完全动态群签名等方面与本文方案进行比较, 如表2所示。其中 $n$ 为安全参数,  $N$ 为群成员个数,  $q \in \mathbb{Z}$ 为模数,  $m = 6n^{1+\delta}$ ,  $t = \omega(\text{lb } n)$ 为零知识证明中证明者和验证者间交互的次数,  $V$ 为一次签名运算时间,  $T_1$ 为一次随机采样算法时间,  $T_2$ 为一次乘运算时间,  $T_3$ 为一次特殊采样算法时间(耗时较少的运算如矩阵-矩阵加法、向量-向量加法, 运算时间忽略不计)。

表2 不同方案的性能对比

Table 2 Performance comparison of different schemes

方案	公钥大小	私钥大小	签名大小	加入代价	撤销代价	是否动态
文献[8]方案	$O(m \text{lb } q)$	$O(m \text{lb } q)$	$O(t \text{lb } q)$	—	—	静态
文献[11]方案	$O(m \text{lb } N \text{lb } q)$	$O(m)$	$O(\text{lb } q)$	$V + 2T_1 + 5nmT_2 + T_3$	—	部分动态
文献[13]方案	$O(m \text{lb } N \text{lb } q)$	$O(\text{lb } N \text{lb } q)$	$O(t \text{lb } N \text{lb } q \text{lb } \beta)$	—	$mnT_2$	部分动态
文献[14]方案	$O(m \text{lb } q)$	$O(m)$	$O(\text{lb } q)$	$V + 2T_1 + 6nmT_2 + 3T_3$	$2mnT_2$	全动态
本文方案	$O(m \text{lb } q)$	$O(m)$	$O(t \text{lb } q)$	$V + 2nmT_2 + 2T_3$	$mnT_2$	全动态

由表2可知:文献[8]方案中公私钥大小均为 $O(m\ln b\ q)$ ,签名大小为 $O(tm\ln b\ q)$  ( $t=\omega(\ln n)>1$ ),与群成员数量 $N$ 无关,但该方案不具有加入和撤销机制,属于静态群签名;文献[11]方案为具有加入机制的部分动态群签名方案,但公钥大小与成员数量相关,不适合大群组的群签名系统,加入过程与本文方案相比虽然减少了1次特殊采样运算,但增加了 $3nm$ 次数乘运算和2次随机采样运算;文献[13]方案为具有撤销机制的部分动态群签名方案,但公私钥大小、签名大小均与群成员数量 $N$ 有关,不适合大群组的群签名系统;文献[14]方案是同时具有加入和撤销机制的全动态群签名方案,其签名大小虽比本文方案的签名短,但在加入过程中与本文方案相比增加了 $4nm$ 次数乘运算时间、2次随机采样算法的时间以及1次特殊采样算法时间,在撤销过程中增加了 $1mn$ 次的数乘运算时间;本文方案是具有加入和撤销机制的完全动态群签名方案,其加入、撤销代价较小,并且签名尺寸为 $O(tm\ln b\ q)$ ,公钥尺寸为 $O(m\ln b\ q)$ ,签名私钥尺寸为 $O(m)$ ,均与群成员的数量 $N$ 无关,因此,本文方案也是适合大群组的群签名方案。

## 5 结束语

群签名的加入与撤销机制及其密钥与签名的长度,始终是密码学领域研究者所关注的重点问题。本文将动态群签名思想引入文献[8]群签名方案,提出一个具有加入和撤销机制的格上完全动态群签名方案。在安全性方面,随机预言机模型下该方案基于ISIS和LWE假设是可证明安全的,能够抵抗量子攻击,同时也能避免陷害攻击;在效率方面,该方案不仅能够实现加入和撤销功能,而且复杂度较低。此外,其签名和密钥长度均较短且与群成员的数量无关。本文方案中群成员的加入需要群管理员颁发数字证书,这会增加群成员的加入开销和数字证书的存储开销,下一步将对此进行改进,设计无证书的动态群签名方案。

## 参考文献

- [1] CHAUM D, HEYST E. Group signatures[C]//Proceedings of Workshop on the Theory and Application of Cryptographic Techniques. Berlin, Germany: Springer, 1991: 257-265.
- [2] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303-332.
- [3] CAMENISCH J, STADLER M. Efficient group signature schemes for large groups[C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany: Springer, 1997: 410-424.
- [4] ATENIESE G, CAMENISCH J, JOYE M, et al. A practical and provably secure coalition-resistant group signature scheme[C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany: Springer, 2000: 255-270.
- [5] BONEH D, BOYEN X, SHACHAM H. Short group signatures[C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany: Springer, 2004: 41-55.
- [6] GORDON S D, KATZ J, VAIKUNTANATHAN V. A group signature scheme from lattice assumptions[C]//Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2010: 395-412.
- [7] LAGUILLAUMIE F, LANGLOIS A, LIBERT B, et al. Lattice-based group signatures with logarithmic signature size[C]//Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2013: 41-61.
- [8] NGUYEN P Q, ZHANG J, ZHANG Z. Simpler efficient group signatures from lattices[C]//Proceedings of IACR International Workshop on Public Key Cryptography. Berlin, Germany: Springer, 2015: 401-426.
- [9] BRESSON E, STERN J. Efficient revocation in group signatures[C]//Proceedings of International Workshop on Public Key Cryptography. Berlin, Germany: Springer, 2001: 190-206.
- [10] ZHANG Yanhua, HU Yupu, GAO Wen, et al. Simpler efficient group signature scheme with verifier-local revocation from lattices[J]. KSII Transactions on Internet & Information Systems, 2016, 10(1): 414-430.
- [11] LIBERT B, LING S, MOUHARTEM F, et al. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions[C]//Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2016: 373-403.
- [12] LING S, NGUYEN K, WANG H, et al. Lattice-based group signatures: achieving full dynamicity with ease[C]//Proceedings of International Conference on Applied Cryptography and Network Security. Berlin, Germany: Springer, 2017: 293-312.
- [13] LING S, NGUYEN K, ROUX-LANGLOIS A, et al. A lattice-based group signature scheme with verifier-local revocation[J]. Theoretical Computer Science, 2018, 730: 1-20.
- [14] LI Xuelian, LÜ Xiaolin, GUO Lijuan, et al. A dynamic group signature scheme based on lattice for large group[J]. Journal of University of Electronic Science and Technology of China, 2019, 48(1): 80-87. (in Chinese)  
李雪莲, 吕晓琳, 郭利娟, 等. 适合大群组的格基动态群签名方案[J]. 电子科技大学学报, 2019, 48(1): 80-87.
- [15] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48(3): 535-553.
- [16] CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate a lattice basis[C]//Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2010: 523-552.



(上接第 167 页)

- [17] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]//Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York, USA: ACM Press, 2008: 197-206.
- [18] MICCIANCIO D, MOL P. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions [C]//Proceedings of Annual Cryptology Conference. Berlin, Germany: Springer, 2011: 465-484.
- [19] BELLARE M, MICCIANCIO D, WARINSCHI B. Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions [C]//Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2003: 614-629.
- [20] BOOTLE J, CERULLI A, CHAIDOS P, et al. Foundations of fully dynamic group signatures [C]//Proceedings of International Conference on Applied Cryptography and Network Security. Berlin, Germany: Springer, 2016: 117-136.
- [21] BELLARE M, NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma [C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2006: 390-399.

编辑 金胡考