格上本地验证者撤销属性基群签名的零知识证明

张彦华*① 胡予濮② 刘西蒙③ 张启坤① 贾惠文④

①(郑州轻工业大学计算机与通信工程学院 郑州 450002)

②(西安电子科技大学通信工程学院 西安 710071)

③(福州大学数学与计算机科学学院 福州 350108)

④(广州大学数学与信息科学学院 广州 510006)

摘 要：属性基群签名(ABGS)是一类特殊形式的群签名，其允许拥有某些特定属性的群成员匿名地代表整个群对消息进行签名；当有争议发生时，签名打开实体可以有效地追踪出真实签名者。针对格上第1个支持本地验证者撤销的属性基群签名群公钥尺寸过长，空间效率不高的问题，该文采用仅需固定矩阵个数的紧凑的身份编码技术对群成员身份信息进行编码，使得群公钥尺寸与群成员个数无关；进一步地，给出新的Stern类统计零知识证明协议，该协议可以有效地证明群成员的签名特权，而其撤销标签则通过单向和单射的带误差学习函数来进行承诺。

关键词：属性基群签名；格；本地验证者撤销；零知识证明；带误差学习

中图分类号：TN918, TP309 **文献标识码**：A **文章编号**：1009-5896(2020)02-0315-07

DOI: 10.11999/JEIT190587

Zero-knowledge Proofs for Attribute-Based Group Signatures with Verifier-local Revocation Over Lattices

ZHANG Yanhua① HU Yupu② LIU Ximeng③ ZHANG Qikun① JIA Huiwen④

①(*School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450002, *China*)

②(*School of Telecommunications Engineering, Xidian University, Xi'an* 710071, *China*)

③(*College of Mathematics and Computer Science, Fuzhou University, Fuzhou* 350108, *China*)

④(*School of Mathematics and Information Science, Guangzhou University, Guangzhou* 510006, *China*)

Abstract: Attribute-Based Group Signature(ABGS) is a new variant of group signature, and it allows group members with certain specific attributes to sign messages on behalf of the whole group anonymously; Once any dispute arises, an opening authority can effectively reveal and track the real identity information of the singer. For the problem that the first lattice-based attribute-based group signature scheme with verifier-local revocation has a long bit-size of group public-key, and thus a low space efficiency, a compact identity-encoding technique which only needs a fixed number of matrices is adopted to encode the identity information of group members, so that the bit-size of group public-key is independent of the number of group members. Moreover, a new Stern-like statistical zero-knowledge proofs protocol is proposed, which can effectively prove the member's signature privilege, and its revocation-token is bound to a one-way and injective learning with errors function.

Key words: Attribute-Based Group Signature (ABGS); Lattice; Verifier-local revocation; Zero-knowledge proofs; Learning With Errors (LWE)

1 引言

2007年，Khader[1]首次提出属性基群签名体制(Attribute-Based Group Signature, ABGS)。在此签名体制中，拥有不同属性信息的群成员可以代表整个群对消息进行匿名性地签名，当有争议产生时，签名打开实体可以有效地追踪出真实签名者。ABGS是一类特殊形式的群签名，其群成员并非拥有对等的签名特权，当且仅当其属性满足签名策略时才能代表整个群进行签名，且验证者可以有效地由签名判定出签名者的角色信息(并非具体身份信

收稿日期：2019-08-05；改回日期：2019-10-31；网络出版：2019-11-25

*通信作者： 张彦华 yhzhang@zzuli.edu.cn

基金项目：国家自然科学基金(61672412, 61772477)

Foundation Items: The National Natural Science Foundation of China (61672412, 61772477)

息)。相较于传统的群签名[2]，环签名[3]和属性基签名[4]，ABGS中的签名者需要高效且匿名地证明其拥有某些特定的属性或签名特权，且生成的签名能够获得追踪性。ABGS能够很好地应用于需要提供匿名性认证和访问控制的环境中。

2017年，基于Merkle类的访问树，Kuchta等人[5]首次给出了基于格的属性基群签名方案，即第1个抗量子攻击的属性基群签名。文献[5]方案的安全性可归约至格上平均情况下的小整数解(Short Integer Solution, SIS)问题和带误差学习(Learning With Errors, LWE)问题。然而，文献[5]方案仅支持候选成员动态地加入群，而不能安全有效地撤销和删除某些恶意操作的群成员。为了弥补该缺陷，2018年，基于本地验证者撤销(Verifier-Local Revocation, VLR)技术，Zhang等人[6]首次给出了格上本地验证者撤销的属性基群签名方案，即第1个抗量子攻击的可动态撤销群成员的属性基群签名。该方案支持门限结构的签名策略，且其安全性可归约至格上最坏情况下的渐进最短向量组问题(Shortest Independent Vectors Problem, SIVP)。然而，文献[6]方案的群公钥和群成员签名私钥的生成采用改进版Boyen签名方案[7]的密钥生成算法，因而获得较长的群公钥尺寸，确切地讲，群公钥含有的矩阵个数与群成员个数相关，即$\mathcal{O}(\log_2 N)$，其中N表示群成员个数。对于某些含有群成员个数较大的群，文献[6]方案的群公钥尺寸过长，空间运行效率不高的问题就显得尤为突出。

本文利用Nguyen等人[8]给出的高效且紧凑的身份编码技术对群成员的身份信息进行编码，且在编码操作中仅需要固定的矩阵个数，确切地讲，仅需3个公共矩阵，从而使得群公钥尺寸与群成员个数无关，即$\mathcal{O}(1)$；特别地，创造性地构造出一个新的Stern类统计零知识证明协议，该协议可以有效地证明签名者的签名特权，而其撤销标签则通过一个单向和单射的带误差学习函数来进行承诺。

2 预备知识

格上困难性问题是密码学方案构造的安全性保障，下面简单介绍SIS、非齐次的小整数解(Inhomogeneous SIS, ISIS)和带误差学习(LWE)问题的定义及困难性。

定义1 无穷范数下的小整数解问题$\mathrm{SIS}^{\infty}_{n,m,q,\beta}$：给定素数$q\geq 2$，随机矩阵$\boldsymbol{A}\in Z_q^{n\times m}$和实数$\beta>0$，求非零小尺寸整数向量$\boldsymbol{e}\in Z^m$，满足$\boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{0} \bmod q$，$||\boldsymbol{e}||_\infty\leq\beta$。

定义2 无穷范数下的非齐次小整数解问题$\mathrm{ISIS}^{\infty}_{n,m,q,\beta}$：给定素数$q\geq 2$，随机矩阵$\boldsymbol{A}\in Z_q^{n\times m}$，向量$\boldsymbol{u}\in Z_q^n$和实数$\beta>0$，求小尺寸整数向量$\boldsymbol{e}\in Z^m$，满足$\boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{u} \bmod q$，$||\boldsymbol{e}||_\infty\leq\beta$。

引理1[9,10] 设整数$m=\mathrm{poly}(n)$，实数$\beta=\mathrm{poly}(n)$，素数$q\geq\beta\cdot\tilde{\mathcal{O}}(\sqrt{n})$，平均情况下的$\mathrm{SIS}^{\infty}_{n,m,q,\beta}$和$\mathrm{ISIS}^{\infty}_{n,m,q,\beta}$问题的困难性至少等价于最坏情况下的$\mathrm{SIVP}_\gamma$问题，其中渐进因子$\gamma=\beta\cdot\tilde{\mathcal{O}}(\sqrt{nm})$。特别地，令$\beta=1$，$q=\tilde{\mathcal{O}}(n)$，$m=2n\lceil\log_2 q\rceil$，则$\mathrm{SIS}^{\infty}_{n,m,q,\beta}$和$\mathrm{ISIS}^{\infty}_{n,m,q,\beta}$问题的困难性等价于$\mathrm{SIVP}_{\tilde{\mathcal{O}}(n)}$问题的困难性。

定义3 带误差学习问题$\mathrm{LWE}_{n,q,\chi}$：给定$\boldsymbol{s}\in Z_q^n$，整数环Z上的误差分布χ，$\mathcal{A}_{\boldsymbol{s},\chi}$表示分布$(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e})$，其中随机矩阵$\boldsymbol{A}\in Z_q^{n\times m}$，误差向量$\boldsymbol{e}\leftarrow_R\chi^m$，区分伪随机分布$\mathcal{A}_{\boldsymbol{s},\chi}$与$Z_q^{n\times m}\times Z_q^m$上的真随机分布$\mathcal{U}$。

引理2[9-11] 设整数$m=\mathrm{poly}(n)$，实数$\beta\geq\sqrt{n}\cdot\omega(\log_2 n)$，$q$是一个素数幂(即$q=p^e$，素数$p\geq 2$)，$\chi$是一个上界为$\beta$的误差分布(如$\chi=\mathcal{D}_{Z^m,s}$)，则平均情况下的判定性$\mathrm{LWE}_{n,q,\chi}$问题的困难性至少等价于最坏情况下的$\mathrm{SIVP}_{\tilde{\mathcal{O}}(nq/\beta)}$问题的困难性。

3 身份编码技术

2015年，Nguyen等人[8]给出了一个紧凑的身份编码技术对群成员的身份信息进行编码，现对其进行简单介绍。该技术使群公钥仅包含3个公共矩阵(确切地讲，原群签名方案另需1个公共矩阵用于签名追踪)，即$\mathrm{Gpk}=(\boldsymbol{A}_0,\boldsymbol{A}_1,\boldsymbol{A}_2)$，其中$\boldsymbol{A}_0$，$\boldsymbol{A}_1$和$\boldsymbol{A}_2\in Z_q^{n\times m}$。对于任意群成员$i\in\{1,2,\cdots,N\}$，定义式(1)的矩阵

$$\boldsymbol{A}_i'=[\boldsymbol{A}_0\,|\,\boldsymbol{A}_1+i\boldsymbol{A}_2]\in Z_q^{n\times 2m} \tag{1}$$

群成员i的签名私钥为$q-$ary格$\Lambda_q^{\perp}(\boldsymbol{A}_i')$的一个短的陷门基矩阵，该身份编码技术可获得2个显著优势：

(1) 群公钥仅需3个公共矩阵，从而使得群公钥尺寸与群成员个数无关；

(2) 群成员关系简单，有利于构造有效的统计零知识证明协议。

本文的属性全集$\mathbf{Att}=\{\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_{n'}\}$，其中$\boldsymbol{u}_i\in Z_q^n$，$i\in\{1,2,\cdots,n'\}$。门限签名策略$\mathcal{T}=(t,\boldsymbol{S})$，其中$\boldsymbol{S}\subseteq\mathbf{Att}$，$t\leq|\boldsymbol{S}|$，$\boldsymbol{u}_j\in\boldsymbol{S}$，$j\in\{j_1,j_2,\cdots,j_p\}\subseteq\{1,2,\cdots,n'\}$。本文提出了一个改进的身份编码技术，即群成员$i$的签名私钥不是格$\Lambda_q^{\perp}(\boldsymbol{A}_i')$的陷门基矩阵，而是一系列短的$2m$维向量$\boldsymbol{e}_j^i=(\boldsymbol{e}_{j,1}^i,\boldsymbol{e}_{j,2}^i)\in Z^{2m}$，并且满足$\boldsymbol{A}_i'\cdot\boldsymbol{e}_j^i=\boldsymbol{u}_j^i \bmod q$，$||\boldsymbol{e}_j^i||_\infty\leq\beta$，其中$\boldsymbol{u}_j^i\in Z_q^n$为群成员$i$所拥有的属性信息，即$\boldsymbol{u}_j^i\in\boldsymbol{S}_i\subseteq\mathbf{Att}$；对应于群成员$i$未分配的属性信息$\boldsymbol{u}_j^i\in\mathbf{Att}\backslash\boldsymbol{S}_i$，其私钥为$\boldsymbol{e}_j^i=(\boldsymbol{e}_{j,1}^i,\boldsymbol{e}_{j,2}^i)$，其中$\boldsymbol{e}_{j,1}^i\leftarrow_R\mathcal{D}_{Z^m,s}$，$\boldsymbol{e}_{j,2}^i\in Z_q^m$，并且满足$\boldsymbol{A}_i'\cdot\boldsymbol{e}_j^i=\boldsymbol{u}_j^i \bmod q$，$||\boldsymbol{e}_{j,2}^i||_\infty>\beta$($\boldsymbol{e}_{j,2}^i$可通

过高等代数中高斯消去算法求得)。群成员i的撤销标签由$\boldsymbol{A}_0$和其签名私钥的第1部分构成，即$\mathbf{Grt}_{\boldsymbol{i}}=\{\mathbf{grt}_1^i,\ \mathbf{grt}_2^i,\ \cdots,\mathbf{grt}_n'^i\}$，其中$\mathbf{grt}_j^i=\boldsymbol{A}_0\ \cdot\ \boldsymbol{e}_{j,1}^i \bmod q$，$j\in\{1,2,\cdots,n'\}$。

在上述新的构造中，主要挑战是如何构造安全有效的Stern类统计零知识证明协议来证明式(2)、式(3)

$$\boldsymbol{A}_i'\cdot\boldsymbol{e}_j^i=\boldsymbol{u}_j^i \bmod q,\quad \boldsymbol{u}_j^i\in\boldsymbol{S},\quad j\in\{j_1,j_2,\cdots,j_p\} \tag{2}$$

$$\mathbf{grt}_j^i=\boldsymbol{A}_0\cdot\boldsymbol{e}_{j,1}^i \bmod q,\quad j\in\{j_1,j_2,\cdots,j_p\} \tag{3}$$

对应式(3)，本文采用Ling等人[12]给出的创造性证明方法，即随机谕言机输出矩阵$\boldsymbol{B}\in Z_q^{n\times m}$，选取误差向量$\boldsymbol{e}_j\leftarrow_R\chi^m, j\in\{j_1,j_2,\cdots,j_p\}$，令

$$\boldsymbol{b}_j=\left(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{A}_0\right)\cdot\boldsymbol{e}_{j,1}^i+\boldsymbol{e}_j=\boldsymbol{B}^{\mathrm{T}}\cdot\mathbf{grt}_j^i+\boldsymbol{e}_j \bmod q,\quad j\in\{j_1,j_2,\cdots,j_p\} \tag{4}$$

进而群成员i的撤销标签$\mathbf{grt}_j^i$可通过一个单向和单射的带误差学习函数来进行承诺。

对应式(2)，为保护群成员i的匿名性，矩阵$\boldsymbol{A}_i'$不能公开，而这将导致无法构造安全的Stern类统计零知识证明协议。为解决该问题，本文给出一个创造性的构造方法，将$\boldsymbol{A}_i'$变换为一个与身份索引i无关的矩阵$\boldsymbol{A}''$。在本文中，考虑群尺寸即最大群成员个数$N=2^l=\mathrm{poly}(n)$。为方便表述，首先定义符号：

(1) $\boldsymbol{g}_l=\left(1,2,2^2,\cdots,2^{l-1}\right)$是一个2的幂次向量；

(2) $\mathbf{bin}(i)\in\{0,1\}^l$表示群成员身份索引$i$的二进制。显然地，$i=\boldsymbol{g}_l^{\mathrm{T}}\cdot\mathbf{bin}(i)$；

(3) $\boldsymbol{e}\otimes\boldsymbol{e}'=\left(e_1\boldsymbol{e}',e_2\boldsymbol{e}',\cdots,e_l\boldsymbol{e}'\right)\in Z_q^{ml}$，其中$\boldsymbol{e}=(e_1,e_2,\cdots,e_l)\in Z_q^l,\boldsymbol{e}'\in Z_q^m$；

(4) $\boldsymbol{e}\otimes\boldsymbol{A}=[e_1\boldsymbol{A}\,|e_2\boldsymbol{A}\,|\cdots|e_l\boldsymbol{A}]\in Z_q^{n\times ml}$，其中$\boldsymbol{e}=(e_1,e_2,\cdots,e_l)\in Z_q^l,\ \boldsymbol{A}\in Z_q^{n\times m}$。

关键转换步骤为：

(1) $\boldsymbol{A}_i'$转换为$\boldsymbol{A}''=\left[\boldsymbol{A}_0\,|\boldsymbol{A}_1\,|\boldsymbol{A}_2\,|2\boldsymbol{A}_2\,|\cdots|2^{l-1}\boldsymbol{A}_2\right]=[\boldsymbol{A}_0\,|\boldsymbol{A}_1\,|\boldsymbol{g}_l\otimes\boldsymbol{A}_2]\in Z_q^{n\times(l+2)m}$；

(2) 签名私钥$\boldsymbol{e}_j^i=\left(\boldsymbol{e}_{j,1}^i,\boldsymbol{e}_{j,2}^i\right)\in Z^{2m}$转换为$\boldsymbol{e}'^i_j=\left(\boldsymbol{e}_{j,1}^i,\boldsymbol{e}_{j,2}^i,\mathbf{bin}(i)\otimes\boldsymbol{e}_{j,2}^i\right)\in Z^{(l+2)m}, j\in\{j_1,j_2,\cdots,j_p\}$。

由此转换易知，式(2)变换为新形式

$$\boldsymbol{A}_i'\cdot\boldsymbol{e}_j^i=\boldsymbol{A}''\cdot\boldsymbol{e}'^i_j=\boldsymbol{u}_j^i \bmod q,\quad \boldsymbol{u}_j^i\in\boldsymbol{S},\quad j\in\{j_1,j_2,\cdots,j_p\} \tag{5}$$

将上述一系列创造性的转换技巧和Ling等人[13]提出的扩展Stern类零知识证明系统相结合，第4节将给出一个安全有效的本地验证者撤销属性基群签名的Stern类统计零知识证明协议来证明式(4)和式(5)。

4　一个安全有效的Stern类统计零知识证明协议

本节介绍一个安全有效的Stern类统计零知识证明协议，通过该协议，证明者$\mathcal{P}$能够使得任意验证者$\mathcal{V}$相信$\mathcal{P}$是一个签署了消息的合法群成员，即相信$\mathcal{P}$的属性信息满足给定的门限签名策略$\mathcal{T}$且$\mathcal{P}$未被撤销，$\mathcal{P}$的撤销标签正确地嵌入到一个带误差学习函数中。

4.1　特定集合和置换

给定$\mathbf{id}\in\{d_1,d_2,\cdots,d_l\}\in\{0,1\}^l$，定义如下4个向量集合，1个置换集合和1个截断函数：

(1) $\boldsymbol{B}_{2l}$：由满足$\boldsymbol{e}\in\{0,\ 1\}^{2l}$且汉明重量$\mathrm{HW}(\boldsymbol{e})=l$的所有向量$\boldsymbol{e}$构成的集合；

(2) $\boldsymbol{B}_{3m}$：由满足$\boldsymbol{e}\in\{-1,0,1\}^{3m}$且含有相同个数的$-1$, 0和1的所有向量$\boldsymbol{e}$构成的集合；

(3) $\mathbf{Sec}_\beta(\mathbf{id})$：由满足$\boldsymbol{e}\in(\boldsymbol{e}_1,\ \boldsymbol{e}_2,\ d_1\boldsymbol{e}_2,\ d_2\boldsymbol{e}_2,\ \cdots,d_l\boldsymbol{e}_2)\in Z_q^{(l+2)m}$且$||\boldsymbol{e}||_\infty\le\beta$的所有向量$\boldsymbol{e}$构成的集合；

(4) $\mathbf{SecExt}(\mathbf{id}^*)$：由满足$\boldsymbol{e}\in(\boldsymbol{e}_1,\ \boldsymbol{e}_2,\ d_1\boldsymbol{e}_2,\ \cdots,\ d_l\boldsymbol{e}_2,d_{l+1}\boldsymbol{e}_2,\cdots,d_{2l}\boldsymbol{e}_2)\in\{-1,0,1\}^{(2l+2)3m}$的所有向量$\boldsymbol{e}$构成的集合，其中$\mathbf{id}^*\in\boldsymbol{B}_{2l}$是$\mathbf{id}$的扩展，且$\boldsymbol{e}_1,\boldsymbol{e}_2\in\boldsymbol{B}_{3m}$；

(5) $\mathcal{S}_k$: k个元素的所有置换构成的集合；

(6) $\mathrm{Parse}(\boldsymbol{e},k_1,k_2)$：输出向量$(e_{k_1},e_{k_1+1},\cdots,e_{k_2})\in R^{k_2-k_1+1}$，其中$\boldsymbol{e}=(e_1,e_2,\cdots,e_n)\in R^n$，$1\le k_1\le k_2\le n$。

给定$\boldsymbol{e}_j\in(\boldsymbol{e}_{j,-1},\boldsymbol{e}_{j,0},\boldsymbol{e}_{j,1},\boldsymbol{e}_{j,2},\cdots,\boldsymbol{e}_{j,2l})\in Z_q^{(2l+2)3m}$，$j\in\{1,2,\cdots,p\}$，置换$\rho$，$\varphi\in\mathcal{S}_{3m}$，$\tau\in\mathcal{S}_{2l}$和$\phi\in\mathcal{S}_p$，定义变换为

$$\mathcal{F}_{\rho,\varphi,\tau,\phi}(\boldsymbol{e}_j)=\left(\rho\left(\boldsymbol{e}_{\phi(j),-1}\right),\varphi\left(\boldsymbol{e}_{\phi(j),0}\right),\varphi\left(\boldsymbol{e}_{\phi(j),\tau(1)}\right),\varphi\left(\boldsymbol{e}_{\phi(j),\tau(2)}\right),\cdots,\varphi\left(\boldsymbol{e}_{\phi(j),\tau(2l)}\right)\right) \tag{6}$$

特别地，给定$\mathbf{id}\in\{0,1\}^l$，$\mathbf{id}^*\in\boldsymbol{B}_{2l}$是$\mathbf{id}$的扩展，则式(7)的关系易得到验证

$$\boldsymbol{e}_j\in\mathbf{SecExt}(\mathbf{id}^*)\Leftrightarrow\mathcal{F}_{\pi,\varphi,\tau,\phi}(\boldsymbol{e}_j)\in\mathbf{SecExt}(\tau(\mathbf{id}^*)),\quad j\in\{1,2,\cdots,p\} \tag{7}$$

4.2　特定算法

令$k=\lfloor\log_2\beta\rfloor+1$，定义整数序列：$\beta_1=\lceil\beta/2\rceil$，$\beta_2=\lceil(\beta-\beta_1)/2\rceil,\beta_3=\lceil(\beta-\beta_1-\beta_2)/2\rceil,\cdots,\beta_k=1$。

向量分解算法Dec：给定$\boldsymbol{e}\in(e_1,e_2,\cdots,e_m)\in Z^m$，$||\boldsymbol{e}||_\infty\le\beta$，该算法目的是用$k$个$\{-1,0,1\}^m$表示$\boldsymbol{e}$。运行步骤：

(1) 令$e_i=\sum_{j=1}^k\beta_j\cdot e_{i,j}$，$e_{i,j}\in\{-1,0,1\}$，$i\in\{1,2,\cdots,m\}$；

(2) 令$\hat{\boldsymbol{e}}_j=(e_{1,j},e_{2,j},\cdots,e_{m,j})$, $j\in\{1,2,\cdots,k\}$。由上易知，$\hat{\boldsymbol{e}}_j\in\{-1,0,1\}^m$，$\boldsymbol{e}_i=\sum_{j=1}^{k}\beta_j\cdot\hat{\boldsymbol{e}}_j$，$i\in\{1,2,\cdots,m\}$。

向量扩展算法Ext：给定$\hat{\boldsymbol{e}}_j\in\{-1,0,1\}^m$，该算法目的是将其扩展为$\boldsymbol{e}_j\in\boldsymbol{B}_{3m}$。运行步骤：

(1) 令$\hat{\boldsymbol{e}}_j$中分量元素-1, 0和1的个数分别为λ_{-1}, λ_0和λ_1；

(2) 选取$\boldsymbol{e}'_j\leftarrow_R\{-1,0,1\}^{2m}$，其中分量元素$-1$, 0和1的个数分别为$m-\lambda_{-1}$, $m-\lambda_0$和$m-\lambda_1$；

(3) 令$\boldsymbol{e}_j=(\hat{\boldsymbol{e}}_j,\boldsymbol{e}'_j)\in\{-1,0,1\}^{3m}$。由上易知，$\rho\leftarrow_R\mathcal{S}_{3m}$, $\boldsymbol{e}_j\in\boldsymbol{B}_{3m}\Leftrightarrow\pi(\boldsymbol{e}_j)\in\boldsymbol{B}_{3m}$。

矩阵扩展算法MExt：给定$\boldsymbol{A}'=[\boldsymbol{A}\,|\boldsymbol{A}_0\,|\boldsymbol{A}_1\,|\cdots|\boldsymbol{A}_l]\in Z_q^{n\times(l+2)m}$，该算法目的是将其扩展为$\boldsymbol{A}^*\in Z_q^{n\times(2l+2)3m}$。运行步骤：

(1) 向每个元矩阵增添零矩阵$\boldsymbol{0}^{n\times2m}$且另增添一个零矩阵$\boldsymbol{0}^{n\times3ml}$；

(2) 令$\boldsymbol{A}^*=\left[\boldsymbol{A}\,\middle|\boldsymbol{0}^{n\times2m}|\boldsymbol{A}_0\,\middle|\boldsymbol{0}^{n\times2m}|\boldsymbol{A}_1\,\middle|\boldsymbol{0}^{n\times2m}|\cdots|\boldsymbol{A}_l\,\middle|\boldsymbol{0}^{n\times2m}\,\middle|\boldsymbol{0}^{n\times3ml}\right]\in Z_q^{n\times(2l+2)3m}$。

4.3 协议设计

本文考虑的群尺寸即最大群成员个数$N=2^l=\text{poly}(n)$，群成员$i\in\{1,2,\cdots,N-1\}$的身份信息(非属性信息)由其索引的二进制表示，即$\mathbf{id}_i=(d_1,d_2,\cdots,d_l)=\mathbf{bin}(i)\in\{0,1\}^l$。

令安全参数为n，该协议中其他重要参数的设置为：

(1) 群尺寸即最大群成员个数$N=2^l=\text{poly}(n)$；

(2) 素数模$q=\omega\left(n^2\log_2 n\right)>N$，属性全集尺寸$n'=\text{poly}(n)$，门限签名策略中属性个数$p\le n'$；

(3) 维数$m=2n\lceil\log_2 q\rceil$，高斯参数$s=\omega\left(\sqrt{n\log_2 q\log_2 n}\right)$；

(4) 整数上界$\beta=\lceil s\cdot\log_2 m\rceil$满足$(4\beta+1)^2\le q$。

首先对证明者$\mathcal{P}$(其属性集$\boldsymbol{S}_i\subseteq\mathbf{Att}$)与验证者$\mathcal{V}$之间的Stern类统计零知识证明协议进行整体概括：

(1) $\mathcal{P}$与$\mathcal{V}$之间的公共信息包括：矩阵$\boldsymbol{A}''=[\boldsymbol{A}_0\,|\boldsymbol{A}_1\,|\boldsymbol{g}_l\otimes\boldsymbol{A}_2]\in Z_q^{n\times(l+2)m}$，门限签名策略$\mathcal{T}=(t,\boldsymbol{S})$，其中$\boldsymbol{S}=\{\boldsymbol{u}_{j_1},\boldsymbol{u}_{j_2},\cdots,\boldsymbol{u}_{j_p}\}\subseteq\mathbf{Att}$, $t\le|\boldsymbol{S}|=p$，随机谕言机的输出$\boldsymbol{B}\in Z_q^{n\times m}$，向量$\boldsymbol{b}_j\in Z_q^m$, $j\in\{j_1,j_2,\cdots,j_p\}$, $\boldsymbol{S}_0\subseteq(\boldsymbol{S}\cap\boldsymbol{S}_i)$, $|\boldsymbol{S}_0|=t$。为方便分析，令$\boldsymbol{S}_0=\{\boldsymbol{u}_{j_1},\boldsymbol{u}_{j_2},\cdots,\boldsymbol{u}_{j_t}\}$；

(2) $\mathcal{P}$拥有的证据信息包括：

(a) $\boldsymbol{e'}^i_j=\left(\boldsymbol{e}^i_{j,1},\boldsymbol{e}^i_{j,2},\mathbf{bin}(i)\otimes\boldsymbol{e}^i_{j,2}\right)\in\mathbf{Sec}_\beta(\mathbf{id}_i)$, $\boldsymbol{u}_j\in\boldsymbol{S}_0$, $j\in\{j_1,j_2,\cdots,j_t\}$；

(b) $\boldsymbol{e'}^i_j=\left(\boldsymbol{e}^i_{j,1},\boldsymbol{e}^i_{j,2},\mathbf{bin}(i)\otimes\boldsymbol{e}^i_{j,2}\right)\notin\mathbf{Sec}_\beta(\mathbf{id}_i)$, $\boldsymbol{u}_j\in\boldsymbol{S}\backslash\boldsymbol{S}_0$, $j\in\{j_{t+1},j_{t+2},\cdots,j_p\}$；

(c) $\boldsymbol{e}_j\in\chi^m$, $j\in\{j_1,j_2,\cdots,j_p\}$。

(3) $\mathcal{P}$的目标是使$\mathcal{V}$相信如下关系：

(a) $\boldsymbol{A''}\cdot\boldsymbol{e'}^i_j=\boldsymbol{u}_j\bmod q$, $\boldsymbol{e'}^i_j\in\mathbf{Sec}_\beta(\mathbf{id}_i)$, $j\in\{j_1,j_2,\cdots,j_t\}$；

(b) $\boldsymbol{A''}\cdot\boldsymbol{e'}^i_j=\boldsymbol{u}_j\bmod q$, $\boldsymbol{e'}^i_j\notin\mathbf{Sec}_\beta(\mathbf{id}_i)$, $j\in\{j_{t+1},j_{t+2},\cdots,j_p\}$；

(c) $\boldsymbol{b}_j=\left(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{A}_0\right)\cdot\boldsymbol{e}^i_{j,1}+\boldsymbol{e}_j=\boldsymbol{B}^{\mathrm{T}}\cdot\mathbf{grt}^i_j+\boldsymbol{e}_j\bmod q$, $0<||\boldsymbol{e}^i_{j,1}||_\infty,||\boldsymbol{e}_j||_\infty\le\beta$, $j\in\{j_1,j_2,\cdots,j_p\}$。

首先给出群成员关系的证明思路，即$\mathcal{P}$的目标(a)和(b)。$\mathcal{P}$运行步骤：

(1) 令$\boldsymbol{A''}=[\boldsymbol{A}_0\,|\boldsymbol{A}_1\,|\boldsymbol{g}_l\otimes\boldsymbol{A}_2]=[\boldsymbol{A}_0\,|\boldsymbol{A}_1\,|\boldsymbol{A}_2\,|2\boldsymbol{A}_2\,|\cdots|2^{l-1}\boldsymbol{A}_2]\in Z_q^{n\times(l+2)m}$，运行算法MExt将其扩展为

$$\boldsymbol{A}^*=\left[\boldsymbol{A}\,\middle|\boldsymbol{0}^{n\times2m}|\boldsymbol{A}_0\,\middle|\boldsymbol{0}^{n\times2m}|\boldsymbol{A}_1\,\middle|\boldsymbol{0}^{n\times2m}|\cdots|\boldsymbol{A}_l\,\middle|\boldsymbol{0}^{n\times2m}\,\middle|\boldsymbol{0}^{n\times3ml}\right]\in Z_q^{n\times(2l+2)3m}\tag{8}$$

(2) 令$\mathbf{id}_i=\mathbf{bin}(i)=(d_1,d_2,\cdots,d_l)\in\{0,1\}^l$，将其扩展为$\mathbf{id}^*=(d_1,d_2,\cdots,d_l,d_{l+1},\cdots,d_{2l})\in\boldsymbol{B}_{2l}$；

(3) 令$\boldsymbol{e'}^i_j=\left(\boldsymbol{e}^i_{j,1},\boldsymbol{e}^i_{j,2},\mathbf{bin}(i)\otimes\boldsymbol{e}^i_{j,2}\right)=\left(\boldsymbol{e}^i_{j,1},\boldsymbol{e}^i_{j,2},d_1\boldsymbol{e}^i_{j,2},d_2\boldsymbol{e}^i_{j,2},\cdots,d_l\boldsymbol{e}^i_{j,2}\right)$, $j\in\{j_1,j_2,\cdots,j_t\}$，运行算法Dec和Ext将$\boldsymbol{e}^i_{j,1}$和$\boldsymbol{e}^i_{j,2}$分别变换为$k$个向量$\boldsymbol{e}^i_{j,1,1},\boldsymbol{e}^i_{j,1,2},\cdots,\boldsymbol{e}^i_{j,1,k}\in\boldsymbol{B}_{3m}$和$k$个向量$\boldsymbol{e}^i_{j,2,1},\boldsymbol{e}^i_{j,2,2},\cdots,\boldsymbol{e}^i_{j,2,k}\in\boldsymbol{B}_{3m}$。接下来，令$\boldsymbol{e'}^i_{j,h}=\left(\boldsymbol{e}^i_{j,1,h},\boldsymbol{e}^i_{j,2,h},d_1\boldsymbol{e}^i_{j,2,h},d_2\boldsymbol{e}^i_{j,2,h},\cdots,d_{2l}\boldsymbol{e}^i_{j,2,h}\right)$, $h\in\{1,2,\cdots,k\}$；

(4) 令$\boldsymbol{e'}^i_j=\left(\boldsymbol{e}^i_{j,1},\boldsymbol{e}^i_{j,2},\mathbf{bin}(i)\otimes\boldsymbol{e}^i_{j,2}\right)=\left(\boldsymbol{e}^i_{j,1},\boldsymbol{e}^i_{j,2},d_i^1\boldsymbol{e}^i_{j,2},d_i^2\boldsymbol{e}^i_{j,2},\cdots,d_i^l\boldsymbol{e}^i_{j,2}\right)$, $j\in\{j_{t+1},j_{t+2},\cdots,j_p\}$，运行算法Dec和Ext将$\boldsymbol{e}^i_{j,1}$变换为$k$个向量$\boldsymbol{e}^i_{j,1,1},\boldsymbol{e}^i_{j,1,2},\cdots,\boldsymbol{e}^i_{j,1,k}\in\boldsymbol{B}_{3m}$，将$\boldsymbol{e}^i_{j,2}$分解和扩展为$\boldsymbol{e}^i_{j,2,1},\boldsymbol{e}^i_{j,2,2},\cdots,\boldsymbol{e}^i_{j,2,k}\in Z_q^{3m}$。接下来，令$\boldsymbol{e'}^i_{j,h}=\left(\boldsymbol{e}^i_{j,1,h},\boldsymbol{e}^i_{j,2,h},d_1\boldsymbol{e}^i_{j,2,h},d_2\boldsymbol{e}^i_{j,2,h},\cdots,d_{2l}\boldsymbol{e}^i_{j,2,h}\right)$, $h\in\{1,2,\cdots,k\}$。

综上分析，$\mathcal{P}$的目标(a)和(b)转化为证明如式(9)所示：

$$\left.\begin{aligned}&\boldsymbol{A}^*\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\boldsymbol{e'}^i_{j,h}\right)=\boldsymbol{u}_j\bmod q,\\&\boldsymbol{e'}^i_{j,h}\in\mathbf{SecExt}(\mathbf{id}^*);\ j\in\{j_1,j_2,\cdots,j_t\}\\&\boldsymbol{A}^*\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\boldsymbol{e'}^i_{j,h}\right)=\boldsymbol{u}_j\bmod q,\\&\boldsymbol{e'}^i_{j,h}\notin\mathbf{SecExt}(\mathbf{id}^*);\ j\in\{j_{t+1},j_{t+2},\cdots,j_p\}\end{aligned}\right\}\tag{9}$$

证明新关系式(9), $\mathcal{P}$运行步骤

(1) 随机选取$\boldsymbol{r}'_{j,1},\boldsymbol{r}'_{j,2},\cdots,\boldsymbol{r}'_{j,k}\leftarrow_R Z_q^{(2l+2)3m}$来隐藏$\boldsymbol{e'}^i_{j,1},\boldsymbol{e'}^i_{j,2},\cdots,\boldsymbol{e'}^i_{j,k}$, $j\in\{j_1,j_2,\cdots,j_p\}$。由上文易知

$$\boldsymbol{A}^{*}\cdot\left(\sum_{h=1}^{k}\beta_{h}\cdot\left(\boldsymbol{e'}_{j,h}^{i}+\boldsymbol{r}'_{j,h}\right)\right)-\boldsymbol{u}_{j}$$
$$=\boldsymbol{A}^{*}\cdot\left(\sum_{h=1}^{k}\beta_{h}\cdot\boldsymbol{r}'_{j,h}\right)\bmod q \tag{10}$$

(2) 随机选取$\rho_{j,1},\rho_{j,2},\cdots,\rho_{j,k}\leftarrow_{R}\mathcal{S}_{3m}$, $\varphi_{j,1},\varphi_{j,2},\cdots,\varphi_{j,k}\leftarrow_{R}\mathcal{S}_{3m}$, $\tau\leftarrow_{R}\mathcal{S}_{2l}$, $\phi\leftarrow_{R}\mathcal{S}_{p}$, $j\in\{j_1,j_2,\cdots,j_p\}$，则如下关系易得到验证：$\mathcal{F}_{\rho_{j,h},\varphi_{j,h},\tau,\phi}\left(\boldsymbol{e'}_{j,h}^{i}\right)\in\mathbf{SecExt}\left(\tau\left(\mathbf{id}^{*}\right)\right)$，其中$\mathbf{id}^{*}\in\boldsymbol{B}_{2l}$是$\mathbf{id}_i=\mathbf{bin}\left(i\right)$的扩展。

接下来给出群成员撤销的证明思路，即$\mathcal{P}$的目标(c)。$\mathcal{P}$运行步骤：

(1) 令$\boldsymbol{B'}=\boldsymbol{B}^{\mathrm{T}}\cdot\boldsymbol{A}_0\bmod q\in Z_q^{m\times m}$, $\boldsymbol{e'}_{j,h,0}^{i}=\mathrm{Parse}\left(\boldsymbol{e'}_{j,h}^{i},1,m\right)$, $j\in\{j_1,j_2,\cdots,j_p\}$, $h\in\{1,2,\cdots,k\}$;

(2) 令$\boldsymbol{e}_j=(e_{j,1},e_{j,2},\cdots,e_{j,m})\in Z^m$，运行算法Dec和Ext将其变换为$\boldsymbol{e}_{j,1},\boldsymbol{e}_{j,2},\cdots,\boldsymbol{e}_{j,k}\in\boldsymbol{B}_{3m}$;

(3) 令$\boldsymbol{B}^{*}=[\boldsymbol{B'}\,|\boldsymbol{I}^{*}]$，其中$\boldsymbol{I}^{*}=\left[\boldsymbol{I}_m\,\middle|\,\boldsymbol{0}^{n\times 2m}\right]$，$\boldsymbol{I}_m$为$m$维单位阵。

综上分析，$\mathcal{P}$的目标(c)转化为证明如下关系：

$$\begin{aligned}\boldsymbol{b}_j&=\boldsymbol{B'}\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\boldsymbol{e'}_{j,h,0}^{i}\right)+\boldsymbol{I}^{*}\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\boldsymbol{e}_{j,h}\right)\\&=\boldsymbol{B}^{*}\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\left(\boldsymbol{e'}_{j,h,0}^{i},\boldsymbol{e}_{j,h}\right)\right)\bmod q,\\&\quad\boldsymbol{e}_{j,h}\in\boldsymbol{B}_{3m},\ \ j\in\{j_1,j_2,\cdots,j_p\},\ \ h\in\{1,2,\cdots,k\}\end{aligned} \tag{11}$$

证明新关系式(11), $\mathcal{P}$运行步骤：

(1) 令$\boldsymbol{r}'_{j,h,0}=\mathrm{Parse}\left(\boldsymbol{r}'_{j,h},1,m\right)$, $j\in\{j_1,j_2,\cdots,j_p\}$, $h\in\{1,2,\cdots,k\}$;

(2) 随机选取$\boldsymbol{r}_{j,1},\boldsymbol{r}_{j,2},\cdots,\boldsymbol{r}_{j,k}\leftarrow_{R}Z_q^{3m}$来隐藏$\boldsymbol{e}_{j,1},\boldsymbol{e}_{j,2},\cdots,\boldsymbol{e}_{j,k}$, $j\in\{j_1,j_2,\cdots,j_p\}$。由上易知

$$\boldsymbol{B}^{*}\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\left(\boldsymbol{e'}_{j,h,0}^{i}+\boldsymbol{r}'_{j,h,0},\boldsymbol{e}_{j,h}+\boldsymbol{r}_{j,h}\right)\right)-\boldsymbol{b}_j$$
$$=\boldsymbol{B}^{*}\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\left(\boldsymbol{r}'_{j,h,0},\boldsymbol{r}_{j,h}\right)\right)\bmod q \tag{12}$$

(3) 随机选取$\sigma_{j,1},\sigma_{j,2},\cdots,\sigma_{j,k}\leftarrow_{R}\mathcal{S}_{3m}$, $j\in\{j_1,j_2,\cdots,j_p\}$，则如下关系易得到验证

$$\sigma_{j,h}\left(\boldsymbol{e}_{j,h}\right)\in\boldsymbol{B}_{3m},\ \ h\in\{1,2,\cdots,k\} \tag{13}$$

将上述一系列技术结合起来，本文获得一个安全有效的交互式Stern类统计零知识证明协议；进一步地，该交互式协议可重复执行$\omega\left(\log_2 n\right)$次使可靠性误差忽略不计，且可以采用随机谕言机模式下Fiat – Shamir启发式证明技巧将其转化为非交互式，现给出构造的零知识证明协议的详细过程。

采用Kawachi等人[14]构造的基于格的满足统计隐藏性和计算捆绑性的承诺方案COM作为部件之一，为方便分析，省略随机输入。令$s_1=\{j_1,j_2,\cdots,j_p\}$, $s_2=\{1,2,\cdots,k\}$，证明者$\mathcal{P}$与验证者$\mathcal{V}$的交互过程为：

(1) **承诺过程** $\mathcal{P}$均匀选取如下随机量：$\boldsymbol{r}'_{j,h}\leftarrow_{R}Z_q^{(2l+2)3m}$, $\boldsymbol{r}_{j,h}\leftarrow_{R}Z_q^{(2l+2)3m}$, $\rho_{j,h}$, $\varphi_{j,h}$, $\sigma_{j,h}\leftarrow_{R}\mathcal{S}_{3m}$, $\tau\leftarrow_{R}\mathcal{S}_{2l}$, $\phi\leftarrow_{R}\mathcal{S}_{p}$, $j\in s_1$, $h\in s_2$。令$\boldsymbol{r}'_{j,h,0}=\mathrm{Parse}\left(\boldsymbol{r}'_{j,h},1,m\right)$，$\mathcal{P}$发送承诺$\mathrm{CMT}=(\boldsymbol{c}_1,\boldsymbol{c}_2,\boldsymbol{c}_3)$，

$$\left.\begin{aligned}\boldsymbol{c}_1&=\mathrm{COM}\left(\left\{\rho_{j,h},\varphi_{j,h},\sigma_{j,h}\right\}_{j\in s_1,h\in s_2},\tau,\phi,\right.\\&\qquad\left\{\boldsymbol{A}^{*}\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\boldsymbol{r}'_{j,h}\right),\right.\\&\qquad\left.\left.\boldsymbol{B}^{*}\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\left(\boldsymbol{r}'_{j,h,0},\boldsymbol{r}_{j,h}\right)\right)\right\}_{j\in s_1}\right)\\\boldsymbol{c}_2&=\mathrm{COM}\left(\left\{\mathcal{F}_{\rho_{j,h},\varphi_{j,h},\tau,\phi}\left(\boldsymbol{r}'_{j,h}\right),\right.\right.\\&\qquad\left.\left.\sigma_{j,h}\left(\boldsymbol{r}_{j,h}\right)\right\}_{j\in s_1,h\in s_2}\right)\\\boldsymbol{c}_3&=\mathrm{COM}\left(\left\{\mathcal{F}_{\rho_{j,h},\varphi_{j,h},\tau,\phi}\left(\boldsymbol{e'}_{j,h}^{i}+\boldsymbol{r}'_{j,h}\right),\right.\right.\\&\qquad\left.\left.\sigma_{j,h}\left(\boldsymbol{e}_{j,h}+\boldsymbol{r}_{j,h}\right)\right\}_{j\in s_1,h\in s_2}\right)\end{aligned}\right\} \tag{14}$$

(2) **挑战过程** $\mathcal{V}$均匀选取一个挑战$\mathrm{CH}\leftarrow_{R}\{1,2,3\}$，并将其发送给$\mathcal{P}$。

(3) **应答过程** 根据CH的不同取值，$\mathcal{P}$运行如下步骤进行应答：

(a) 若$\mathrm{CH}=1$，令$\boldsymbol{v}'_{j,h}=\mathcal{F}_{\pi_{j,h},\varphi_{j,h},\tau,\phi}\left(\boldsymbol{e'}_{j,h}^{i}\right)$, $\boldsymbol{w}'_{j,h}=\mathcal{F}_{\pi_{j,h},\varphi_{j,h},\tau,\phi}\left(\boldsymbol{r}'_{j,h}\right)$, $\boldsymbol{v}_{j,h}=\sigma_{j,h}\left(\boldsymbol{e}_{j,h}\right)$, $\boldsymbol{w}_{j,h}=\sigma_{j,h}\left(\boldsymbol{r}_{j,h}\right)$, $\boldsymbol{t}=\tau\left(\mathbf{id}^{*}\right)$, $j\in s_1$, $h\in s_2$，则应答为：$\mathrm{RSP}=\left(\left\{\boldsymbol{v}'_{j,h},\boldsymbol{w}'_{j,h},\boldsymbol{v}_{j,h},\boldsymbol{w}_{j,h}\right\}_{j\in s_1,h\in s_2},\boldsymbol{t}\right)$;

(b) 若$\mathrm{CH}=2$，令$\rho'_{j,h}=\rho_{j,h},$, $\varphi'_{j,h}=\varphi_{j,h}$, $\sigma'_{j,h}=\sigma_{j,h}$, $\boldsymbol{x}'_{j,h}=\boldsymbol{e'}_{j,h}^{i}+\boldsymbol{r}'_{j,h}$, $\boldsymbol{x}_{j,h}=\boldsymbol{e}_{j,h}+\boldsymbol{r}_{j,h}$, $\tau'=\tau$, $\phi'=\phi$, $j\in s_1$, $h\in s_2$，则应答为：$\mathrm{RSP}=\left(\left\{\rho'_{j,h},\varphi'_{j,h},\sigma'_{j,h},\boldsymbol{x}'_{j,h},\boldsymbol{x}_{j,h}\right\}_{j\in s_1,h\in s_2},\tau',\phi'\right)$;

(c) 若$\mathrm{CH}=3$，令$\rho''_{j,h}=\rho_{j,h}$, $\varphi''_{j,h}=\varphi_{j,h}$, $\tau''=\tau$, $\phi''=\phi$, $\sigma''_{j,h}=\sigma_{j,h}$, $\boldsymbol{h}'_{j,h}=\boldsymbol{r}'_{j,h}$, $\boldsymbol{h}_{j,h}=\boldsymbol{r}_{j,h}$, $j\in s_1$, $h\in s_2$，则应答为：$\mathrm{RSP}=\left(\left\{\rho''_{j,h},\varphi''_{j,h},\sigma''_{j,h},\boldsymbol{h}'_{j,h},\boldsymbol{h}_{j,h}\right\}_{j\in s_1,h\in s_2},\tau'',\phi''\right)$。

(4) **验证过程** 根据不同挑战CH下接收到的RSP, $\mathcal{V}$运行如下步骤进行验证，

(a) 若$\mathrm{CH}=1$，验证如下是否成立：$\boldsymbol{t}\in\boldsymbol{B}_{2l}$, $\boldsymbol{v}'_{j,h}$中有且仅有t个不同的下标j，即存在$s'_1\subseteq s_1$,

$|s_1'|=t$，使得$\boldsymbol{v}_{j,h}'\in\mathbf{SecExt}(\boldsymbol{t})$, $j\in s_1'$, $h\in s_2$; $\boldsymbol{v}_{j,h}\in\boldsymbol{B}_{3m}$, $j\in s_1$, $h\in s_2$，且

$$\left.\begin{aligned}\boldsymbol{c}_2&=\mathrm{COM}\left(\left\{\boldsymbol{w}_{j,h}',\boldsymbol{w}_{j,h}\right\}_{j\in s_1,h\in s_2}\right)\\ \boldsymbol{c}_3&=\mathrm{COM}\left(\left\{\boldsymbol{v}_{j,h}'+\boldsymbol{w}_{j,h}',\boldsymbol{v}_{j,h}+\boldsymbol{w}_{j,h}\right\}_{j\in s_1,h\in s_2}\right)\end{aligned}\right\}\tag{15}$$

（b）若$\mathrm{CH}=2$，令$\boldsymbol{x}_{j,h,0}'=\mathrm{Parse}\left(\boldsymbol{x}_{j,h}',1,m\right)$，验证式(16)是否成立

$$\left.\begin{aligned}\boldsymbol{c}_1=\mathrm{COM}\Bigg(&\left\{\rho_{j,h}',\varphi_{j,h}',\sigma_{j,h}'\right\}_{j\in s_1,h\in s_2},\tau',\phi',\\&\left\{\boldsymbol{A}^*\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\boldsymbol{x}_{j,h}'\right)-\boldsymbol{u}_j,\right.\\&\left.\boldsymbol{B}^*\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\left(\boldsymbol{x}_{j,h,0}',\boldsymbol{x}_{j,h}\right)\right)-\boldsymbol{b}_j\right\}_{j\in s_1}\Bigg)\\ \boldsymbol{c}_3=\mathrm{COM}\Big(&\left\{\mathcal{F}_{\rho_{j,h}',\varphi_{j,h}',\tau',\phi'}\left(\boldsymbol{x}_{j,h}'\right),\right.\\&\left.\sigma_{j,h}'\left(\boldsymbol{x}_{j,h}\right)\right\}_{j\in s_1,h\in s_2}\Big)\end{aligned}\right\}\tag{16}$$

（c）若$\mathrm{CH}=3$，令$\boldsymbol{h}_{j,h,0}'=\mathrm{Parse}\left(\boldsymbol{h}_{j,h}',1,m\right)$，验证式(17)是否成立

$$\left.\begin{aligned}\boldsymbol{c}_1=\mathrm{COM}\Bigg(&\left\{\rho_{j,h}'',\varphi_{j,h}'',\sigma_{j,h}''\right\}_{j\in s_1,h\in s_2},\tau'',\phi'',\\&\left\{\boldsymbol{A}^*\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\boldsymbol{h}_{j,h}'\right),\right.\\&\left.\boldsymbol{B}^*\cdot\left(\sum_{h=1}^{k}\beta_h\cdot\left(\boldsymbol{h}_{j,h,0}',\boldsymbol{h}_{j,h}\right)\right)\right\}_{j\in s_1}\Bigg)\\ \boldsymbol{c}_2=\mathrm{COM}\Big(&\left\{\mathcal{F}_{\rho_{j,h}'',\varphi_{j,h}'',\tau'',\phi''}\left(\boldsymbol{h}_{j,h}'\right),\right.\\&\left.\sigma_{j,h}''\left(\boldsymbol{h}_{j,h}\right)\right\}_{j\in s_1,h\in s_2}\Big)\end{aligned}\right\}\tag{17}$$

当且仅当不同取值CH下所有条件都成立，验证者$\mathcal{V}$输出1表示接受$\mathcal{P}$的零知识证明；否则，输出0拒绝该证明。

5 协议分析

定理1 若COM是一个满足统计隐藏性和计算捆绑性的承诺方案，则第4节构造的Stern类协议是一个安全有效的零知识证明协议，其满足完备性，知识论证性，可靠性误差为2/3，且交互信息尺寸为$l\cdot\tilde{\mathcal{O}}(n)$。

证明 证明采用Stern类统计零知识证明协议的一系列标准证明方法和技巧(可参考文献[12,14])；因篇幅所限，证明过程略。

6 结束语

本文利用仅需固定矩阵个数的格上高效且紧凑的身份编码技术对群成员的身份信息进行编码，使得群公钥尺寸与群成员个数无关，即$\mathcal{O}(1)$，弥补了格上第1个支持本地验证者撤销的属性基群签名群公钥尺寸过长，即$\mathcal{O}(\log_2 N)$，和空间效率不高的缺陷。进一步地，本文创造性地构造出一个新的Stern类统计零知识证明协议，该协议可以有效地证明签名者的签名特权，而其撤销标签则通过一个单向和单射的带误差学习函数来进行承诺。未来的工作是构造支持完全动态群的格上属性基群签名方案。

参 考 文 献

[1] KHADER D. Attribute based group signatures[EB/OL]. http://eprint.iacr.org/2007/159, 2007.

[2] CHAUM D and VAN HEYST E. Group signatures[C]. The Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, 1991: 257–265. doi: 10.1007/3-540-46416-6_22.

[3] RIVEST R L, SHAMIR A, and TAUMAN Y. How to leak a secret[C]. The 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 2001: 552–565. doi: 10.1007/3-540-45682-1_32.

[4] MAJI H, PRABHAKARAN M, and ROSULEK M. Attribute-based signatures[C]. The Cryptographers' Track at the RSA Conference on Topics in Cryptology, San Francisco, USA, 2011: 376–392. doi: 10.1007/978-3-642-19074-2_24.

[5] KUCHTA V, SAHU R A, SHARMA G, *et al*. On new zero-knowledge arguments for attribute-based group signatures from lattices[C]. The 20th International Conference on Information Security and Cryptology, Seoul, South Korea, 2017: 284–309. doi: 10.1007/978-3-319-78556-1_16.

[6] ZHANG Yanhua, GAN Yong, YIN Yifeng, *et al*. Attribute-based VLR group signature scheme from lattices[C]. The 18th International Conference on Algorithms and Architectures for Parallel Processing, Guangzhou, China, 2018: 600–610. doi: 10.1007/978-3-030-05063-4_46.

[7] MICCIANCIO D and PEIKERT C. Trapdoors for lattices: Simpler, tighter, faster, smaller[C]. The 31st International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 2012: 700–718. doi: 10.1007/978-3-642-29011-4_41.

[8] NGUYEN P Q, ZHANG Jiang, and ZHANG Zhenfeng. Simpler efficient group signatures from lattices[C]. The 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, USA, 2015: 401–426. doi: 10.1007/978-3-662-46447-2_18.

[9] GENTRY C, PEIKERT C, and VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]. The 40th Annual ACM Symposium on Theory of Computing, Victoria, Canada, 2008, 197–206. doi: 10.1145/1374376.1374407.

[10] MICCIANCIO D and PEIKERT C. Hardness of SIS and LWE with small parameters[C]. The 33rd Annual Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2013: 21–39. doi: 10.1007/978-3-642-40041-4_2.

[11] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]. The 37th Annual ACM Symposium on Theory of Computing, Baltimore, USA, 2005, 84–93. doi: 10.1145/1060590.1060603.

[12] LING San, 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. doi: 10.1016/j.tcs.2018.03.027.

[13] LING San, NGUYEN K, STEHLÉ D, *et al*. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications[C]. The 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, 2013: 107–124. doi: 10.1007/978-3-642-36362-7_8.

[14] KAWACHI A, TANAKA K, and XAGAWA K. Concurrently secure identification schemes based on the worst-case hardness of lattice problems[C]. The 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, 2008: 372–389. doi: 10.1007/978-3-540-89255-7_23.

张彦华：男，1989年生，讲师，研究方向为格公钥密码学、属性基密码学和后量子密码学等.

胡予濮：男，1955年生，教授，研究方向为多线性映射、后量子密码学等.

刘西蒙：男，1988年生，研究员，研究方向为私计算、密文数据挖掘等.

张启坤：男，1980年生，副教授，研究方向为群组密钥协商等.

贾惠文：男，1990年生，讲师，研究方向为多线性映射、格公钥密码学等.