格上无匿名性撤销的隐藏的属性签名

张彦华[1)] 胡予濮[2)] 陈江山[3)]

[1)](郑州轻工业学院计算机与通信工程学院 郑州 450002)

[2)](西安电子科技大学综合业务网理论与关键技术国家重点实验室 西安 710071)

[3)](闽南师范大学数学与统计学院 福建 漳州 363000)

摘 要 隐藏的属性签名的签名者可利用其属性的任意子集签署消息,同时验证者可以有效地由消息的合法签名判定该消息的确是由拥有某些属性的签名者签署,而无法确定签名者的具体身份.隐藏的属性签名能够保证签名者即使被撤销,其匿名性仍然存在,即验证者无法确定哪些消息是由该签名者签署;而且不拥有某些属性的签名者无法伪造一个由该属性签署的合法签名.基于格上小整数解困难问题,文中利用 Boyen 给出的格基剪接技术,构造出第 1 个随机预言机模型下抵抗选择属性和适应性选择消息攻击的存在性不可伪造的格上无匿名性撤销的隐藏的属性签名方案;进一步地,利用格混合和陷门消失的完全安全的短签名方案,可将上述方案扩展到标准模型.

关键词 属性签名;隐藏;匿名性;格;小整数解;标准模型

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2018.00481

Hidden Attribute-Based Signatures without Anonymity Revocation from Lattices

ZHANG Yan-Hua[1)] HU Yu-Pu[2)] CHEN Jiang-Shan[3)]

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

[2)](*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071)

[3)](*School of Mathematical and Statistics, Minnan Normal University, Zhangzhou, Fujian* 363000)

Abstract As a new type of cryptographic primitive, attribute-based signature (ABS) can achieve the fine-grained access control over the identifying information. In an ABS system, the signer receives from the trusted authority a secret key depending on the set of attributes that he or she possesses. A valid signature can convince the verifier that it was produced by some signer with a set of attributes satisfying the given signing policy while it will reveal nothing else. Compared with the traditional identity-based signature (IBS) system, ABS has stronger anonymity, namely, given a valid signature, the verifier cannot get the knowledge of the identity of the real signer. Moreover, the signers in the ABS system cannot forge a valid signature with attributes that they do not own. Compared with the traditional anonymous signature system, such as group signatures and ring signatures, ABS is able to provide more abundant signing strategies. Hidden attribute-based signature (HABS) is a new signature notion inspired by the recent developments in the ABS system. The signer of HABS is able to sign messages with any subset of his or her attributes, and given the valid messages-signatures, the verifier can effectively decide that these messages are indeed signed by the signers who own the attributes, while the verifier cannot determine the specific identity of the underling signers. Furthermore, HABS can ensure that the anonymity still exists even the signer has been revoked, namely, the verifier still cannot determine which messages

收稿日期:2016-09-08;在线出版日期:2017-06-14.本课题得到国家自然科学基金(61472309)和国家留学基金资助.**张彦华**,男,1989 年生,博士,讲师,主要研究方向为格公钥密码方案的设计与分析.E-mail:yhzhangxidian@163.com.**胡予濮**,男,1955 年生,博士,教授,主要研究领域为格公钥密码学、多线性映射.**陈江山**,男,1981 年生,博士研究生,主要研究方向为多线性映射、不可区分混淆.

have been signed by the revoked signer and the signer cannot forge valid signatures with certain attributes which he or she has not been issued. HABS can be regarded as a special ring signature, when some signer of HABS signs messages with certain subset of his or her attributes, the users who own the same subset of attributes could be combined into a ring automatically, while the signer will not know which users are included in this ring, what is more, the signature size has nothing to do with the number of the ring users. As one of the most efficient candidates of post-quantum cryptography, lattice-based cryptography not only allows to construct powerful primitives which have no feasible instantiations in traditional number-theoretic cryptography, but it can also provide several advantages over the later, such as the conjectured resistance against quantum computers, the worst-case hardness assumptions and the faster arithmetic operations. During the last decade, lattice-based cryptography has received a permanent interest and to design some efficient and powerful lattice-based cryptographic constructions has become more challenging. Based on the small integer solution (SIS) problem and the basis-splicing technique due to Boyen, in this paper, we construct the first HABS scheme without anonymity revocation from lattices in the random oracle model and this construction has proven to be existentially unforgeable against selective-attribute and adaptive chosen message attacks (EUF-sA-aCMA). Further, using the fully secure short signature with lattice mixing and vanishing trapdoors, the above construction can be extended to be in the standard model. Compared with other lattice-based cryptographic constructions, the proposed two constructions have the shorter key size and signature size, in particular, the second one also obtains a stronger secure.

Keywords attribute-based signature; hidden; anonymity; lattice; the small integer solution; standard model

1 引 言

属性签名[1]作为一种新型的密码学原语,它可以有效地实现细粒度的访问控制机制.在属性签名体制中,签名者利用属性权威中心生成的对应于签名者属性的私钥对消息和签名策略进行签名,验证者通过验证可确认该消息是否由属性满足签名策略的签名者产生.相比于传统的身份基签名[2],属性签名具有更强的匿名性,即验证者通过签名仅能够得知签名者的属性满足签名策略,而无法得知签名者的具体身份信息.同时,属性签名还具有不可伪造性和抗合谋性,即不拥有某些属性的签名者无法伪造一个由该属性签署的合法签名.相比于传统的匿名性签名(如群签名[3]、环签名[4]等),属性签名还能够提供丰富的签名策略.

2010 年,Li 和 Kim[5]首次提出了隐藏的属性签名(Hidden Attribute-Based Signature,HABS)的概念.隐藏的属性签名的签名者可利用其属性的任意子集签署消息,同时验证者可以有效地由消息的合法签名判定该消息的确是由拥有某些属性的签名者签署,而无法确定签名者的具体身份信息.在身份基环签名体制中,签名者和验证者都明确知道构成环的成员身份信息,签名者可以有效地代表其他环成员生成签名,而验证者无法由签名确定具体签名者身份.隐藏的属性签名可以看作是特殊的环签名,签名者利用其属性子集签署消息时,具有相同子集的用户自动构成环,而签名者并不知道哪些成员包含在环内,且生成的签名长度与环成员个数无关.例如:张三拥有属性("张三","学校","理学院","教授").张三要向校长匿名举报某位教师在先进个人评选活动中存在申报材料伪造的行为,张三可以利用属性"学校""理学院"对举报信进行签名,校长可以验证该签名的合法性,如果签名是合法的,校长能够由签名获知该举报信的确来自该学校理学院的工作人员,而无法确定其具体身份.隐藏的属性签名也能够保证签名者即使被撤销,其匿名性仍然存在,即无匿名性撤销,公开签名者属性和私钥,验证者仍无法确定哪些消息是由该签名者签署;而且不拥有某些属性的签名者无法伪造一个由该属性签署的合法

签名，即使通过联合也无法伪造出单个签名者无法伪造的合法签名，即抵抗合谋攻击.

近年来，基于格构造新型密码系统因具有较高的渐进效率、运算简单和抗量子攻击等特点，成为后量子时代密码领域的研究热点，并取得了一系列研究成果[6-12]. 2014 年，Miao 等人[13]构造出支持 And 门签名策略的属性签名方案. 2015 年，Wang 等人[14]构造出支持门限签名策略的属性签名方案. 随后，Wang 等人[15]构造出一个效率更高的支持门限签名策略的属性签名方案.

本文利用 Boyen[16]给出的格基剪接技术，基于格上小整数解(Small Integer Solution，SIS)困难问题，构造出第 1 个随机预言机模型下抵抗选择属性和适应性选择消息攻击的存在性不可伪造的格上无匿名性撤销的 HABS 方案；进一步地，利用格混合和陷门消失的完全安全的短签名方案，将上述方案扩展到标准模型.

本文第 2 节介绍格的基础知识，重要算法和困难问题；第 3 节描述 HABS 的定义以及安全性模型；第 4 节给出随机预言机模型下格上无匿名性撤销的 HABS 方案的具体构造及其安全性证明；第 5 节给出标准模型下格上无匿名性撤销的 HABS 方案的具体构造及其安全性证明；最后一节总结全文.

2　预备知识

2.1　格

定义 1.　设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 是 $\mathbb{R}^n$ 上 m 个线性无关的向量，格 Λ 定义为所有这些向量的整系数线性组合构成的集合，即 $\Lambda=\mathcal{L}(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_m)=\left\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i \mid x_i\in\mathbb{Z}\right\}$，其中向量组 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 构成格 Λ 的一组基 $\boldsymbol{B}$.

定义 2.　设 q 是素数，$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{u}\in\mathbb{Z}_q^n$，则

$$\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{x}=\boldsymbol{0} \bmod q\},$$

$$\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{x}=\boldsymbol{u} \bmod q\}.$$

定义 3.　对任意 $s>0$，定义以向量 $\boldsymbol{c}$ 为中心，s 为参数的格 Λ 上的离散高斯分布为

$$D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)}=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\sum_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})},$$

其中 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/s^2)$. 本文中 $\|\cdot\|$ 表示欧几里得范数，即二范数.

2.2　相关算法

引理 1[6].　设 n 是正整数，$q\geq 2$，$m\geq 2n\log_2 q$，对于除了至多 $2q^{-n}$ 的部分之外所有的 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 以及任意 $s\geq\omega(\sqrt{\log_2 n})$，向量 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{e} \bmod q$ 的分布统计接近 $\mathbb{Z}_q^n$ 上的均匀分布，其中 $\boldsymbol{e}\in D_{\mathbb{Z}^m,s}$.

引理 2[7].　设 n 是正整数，$q\geq 2$，$m>5n\log_2 q$，则存在概率多项式时间(Probabilistic Polynomial Time，PPT)算法 $TrapGen(q,n)$，输出 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}\in\mathbb{Z}_q^{m\times m}$，其中 $\boldsymbol{A}$ 在 $\mathbb{Z}_q^{n\times m}$ 上是统计均匀的，$\boldsymbol{T}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基，且满足 $\|\boldsymbol{T}\|\leq O(n\log_2 q)$，$\|\widetilde{\boldsymbol{T}}\|\leq O(\sqrt{n\log_2 q})$.

引理 3[6].　设 n 是正整数，素数 $q\geq 2$，$m>n$，矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$. $\boldsymbol{T}\in\mathbb{Z}_q^{m\times m}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基，高斯参数 $s\geq\|\widetilde{\boldsymbol{T}}\|\cdot\omega(\sqrt{\log_2 m})$. 对于 $\boldsymbol{c}\in\mathbb{R}^m$，$\boldsymbol{u}\in\mathbb{Z}_q^n$，有

(1) $\Pr[\|\boldsymbol{x}-\boldsymbol{c}\|>s\sqrt{m} \mid \boldsymbol{x}\in D_{\Lambda_q^{\perp}(\boldsymbol{A}),s,\boldsymbol{c}}]\leq negl(n)$.

(2) 存在 PPT 算法 $SampDom(n)$ 输出一个统计接近 $D_{\mathbb{Z}_q^m,s}$ 的向量 $\boldsymbol{x}\in\mathbb{Z}_q^m$.

(3) 存在 PPT 算法 $SampPre(\boldsymbol{A},\boldsymbol{T},\boldsymbol{u},s)$ 输出一个统计接近 $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}),s}$ 的向量 $\boldsymbol{x}\in\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})$.

引理 4[8].　设 n 是正整数，矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 的列向量的子集合构成 $\mathbb{Z}_q^n$，则存在确定性多项式时间的算法 $ExtBasis(\boldsymbol{T},\boldsymbol{F}=[\boldsymbol{A}\|\boldsymbol{A}'])$，输出格 $\Lambda_q^{\perp}(\boldsymbol{F})$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{F}}\in\mathbb{Z}_q^{(m+m')\times(m+m')}$，且 $\|\widetilde{\boldsymbol{T}}\|=\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}}\|$，其中 $\boldsymbol{A}'\in\mathbb{Z}_q^{n\times m'}$，$\boldsymbol{T}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基. 特别地，将 $\boldsymbol{F}$ 的列向量重新排列，上述结论仍然成立.

引理 5[8].　设 n 是正整数，素数 $q>2$，高斯参数 $s\geq\|\widetilde{\boldsymbol{T}}\|\cdot\omega(\log_2 n)$，存在PPT算法 $RandBasis(\boldsymbol{T},s)$，输出格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一个基矩阵 $\boldsymbol{T}'\in\mathbb{Z}_q^{m\times m}$，$\|\widetilde{\boldsymbol{T}'}\|\leq s\sqrt{m}$. 其中 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{T}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基. 特别地，对于格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的任意两个基矩阵 $\boldsymbol{T},\boldsymbol{T}'\in\mathbb{Z}_q^{m\times m}$，高斯参数 $s\geq\max\{\|\widetilde{\boldsymbol{T}}\|,\|\widetilde{\boldsymbol{T}'}\|\}\cdot\omega(\log_2 n)$，则 $RandBasis(\boldsymbol{T},s)$ 与 $RandBasis(\boldsymbol{T}',s)$ 统计不可区分.

引理 6[9].　设素数 $q>2$，$m>n$，则存在 PPT 算法 $SampRight(\boldsymbol{A},\boldsymbol{B},\boldsymbol{R},\boldsymbol{T},\boldsymbol{u},s)$，输出格 $\Lambda_q^{\perp}(\boldsymbol{F})$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{F}}\in\mathbb{Z}_q^{2m\times 2m}$，向量 $\boldsymbol{e}\in\mathbb{Z}^{2m}$，且 $\boldsymbol{e}$ 的分布与 $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{F}),s}$ 统计不可区分. 其中 $\boldsymbol{A},\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{R}\in\{1,-1\}^{m\times m}$，$\boldsymbol{T}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的陷门基，$\boldsymbol{u}\in\mathbb{Z}_q^n$，$s>\|\widetilde{\boldsymbol{T}}\|\sqrt{m}\cdot\omega(\log_2 m)$，矩阵 $\boldsymbol{F}=[\boldsymbol{A}\|\boldsymbol{A}\boldsymbol{R}+\boldsymbol{B}]$. 特别地，$\boldsymbol{e}\in\Lambda_q^{\boldsymbol{u}}(\boldsymbol{F})$.

引理 7[12].　设 $D=(l!)^2$，任取 $k\leq l$ 个数

$a_1,\cdots,a_k$. 令拉格朗日插值系数 $L_i=\prod_{i\neq j}\frac{a_j}{a_j-a_i}$, $1\leq i,j\leq k$, 则 DL_i 是整数, 且 $|DL_i|\leq D^2$.

2.3 格上困难问题

定义 4. 小整数解问题(Small Integer Solution, SIS). 设 n 是正整数, q 为素数, 给定矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和实数 $\beta=poly(n)$, 找到非零向量 $\boldsymbol{e}$ 使得 $\boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q$ 且 $\|\boldsymbol{e}\|\leq\beta$.

引理 8[6]. 设 n 是正整数, $\beta=poly(n)$, 对于素数 $q\geq\beta\cdot\omega(\sqrt{n\log_2 n})$, 平均情况下的 SIS 问题的困难性与最差情况下的近似最短独立向量问题(Shortest Independent Vector Problem, SIVP)的困难性是相同的, 其近似因子 $\gamma=\beta\cdot\tilde{O}(\sqrt{n})$.

3 隐藏的属性签名

3.1 定 义

隐藏的属性签名[5]由如下 4 个 PPT 算法构成.

系统建立(Setup): 给定安全参数 n, 输出公开参数 PP(包含属性全集 U)和权威中心的主私钥 MSK.

密钥生成(KeyGen): 给定公开参数 PP, 主私钥 MSK 和用户属性集 $w\subset U$, 输出私钥 SK_w.

签名(Sign): 给定公开参数 PP, 消息 M, 签名者属性子集 $w'\subseteq w$ 和私钥 SK_w, 输出签名 σ.

验证(Verify): 给定公开参数 PP, 签名 σ, 消息 M 和签名者属性子集 w', 输出接受或拒绝.

HABS 的正确性需满足由 Sign 算法生成的合法签名 σ 必能通过 Verify 算法的验证的条件.

3.2 安全模型

隐藏的属性签名应满足如下 2 个安全需要: 不可伪造性和匿名性. 可通过挑战者与攻击者的交互游戏来定义其安全性.

定义 5. 不可伪造性. 若不存在多项式有界的敌手 $\mathcal{A}$ 能以不可忽略的优势赢得如下游戏, 则称一个 HABS 方案是抵抗选择属性和适应性选择消息攻击存在性不可伪造的.

预先固定一个常数 $0<d<|U|$.

初始化. $\mathcal{A}$ 选取签名策略 $w^*\subset U$, $|w^*|\leq d$, 并发送给 $\mathcal{C}$.

系统建立. $\mathcal{C}$ 输入安全参数 n, 运行 Setup 算法生成公开参数 PP 和权威中心主私钥 MSK, 并将 PP 发送给 $\mathcal{A}$.

询问阶段. $\mathcal{A}$ 进行如下多项式有界次适应性询问.

私钥询问: $\mathcal{C}$ 运行 KeyGen 算法可获得对应于签名策略 $w(w^*\not\subset w)$ 的私钥 SK_w, 并返回给 $\mathcal{A}$.

签名询问: $\mathcal{C}$ 运行 Sign 算法可获得任意消息 M 和签名策略 $w'\subset U$, $|w'|\leq d$ 的签名 σ, 并返回给 $\mathcal{A}$.

如果方案是随机预言机模型下可证明安全的, 敌手可以对任意消息 M 进行另外一个询问, 即

Hash 询问: $\mathcal{C}$ 选取一个随机值, 并返回给 $\mathcal{A}$.

伪造. $\mathcal{A}$ 输出 M^*, 签名策略 w^* 及伪造签名 σ^*.

敌手 $\mathcal{A}$ 赢得上述游戏当且仅当:

(1) σ^* 是消息 M^* 的一个合法签名.

(2) (M^*,w^*) 不是签名询问阶段的输入.

定义 6. 匿名性. 若不存在敌手 $\mathcal{A}$ 能以不可忽略的优势赢得如下游戏, 则称一个 HABS 方案是匿名的.

系统建立. $\mathcal{C}$ 输入安全参数 n, 运行 Setup 算法生成公开参数 PP 和权威中心主私钥 MSK, 并将 PP 和 MSK 发送给 $\mathcal{A}$.

$\mathcal{A}$ 利用主私钥 MSK 可以生成对应于任意属性集的私钥和对任意消息进行签名.

挑战阶段. $\mathcal{A}$ 选取挑战消息 M^*, 不同属性集 $w_0,w_1\subset U$, $w'=w_0\cap w_1$, 签名策略 $w^*\subset w'$, $|w^*|\leq d$, $\mathcal{C}$ 利用 MSK 生成对应于 w_0,w_1 的私钥 SK_{w_0},SK_{w_1}. $\mathcal{C}$ 随机选取 $b\in\{0,1\}$, 利用 SK_{w_b}, 运行 Sign 算法获得对消息 M^* 和签名策略 w^* 的签名 σ^*, 并返回给 $\mathcal{A}$.

猜测. $\mathcal{A}$ 输出一个比特 b' 作为对 b 的猜测.

敌手 $\mathcal{A}$ 赢得上述游戏当且仅当 $b'=b$.

4 随机预言机模型下 HABS 方案

在方案中假设属性全集 U 共有 l 个属性分量, 即 $U=\{1,2,\cdots,l\}$. 预先固定一个满足实际应用的常数 $d<l$, 签名者可以灵活利用其属性集的 $1,2,\cdots,d$ 个属性分量对消息进行签名.

4.1 方案构造

Setup: 输入安全参数 n, 属性全集 $U=\{1,\cdots,l\}$.

(1) 令默认属性集 $U'=\{l+1,l+2,\cdots,l+d\}$.

(2) 令 $i\in U\cup U'$, 运行算法 $TrapGen(q,n)$ 生成矩阵 $\boldsymbol{A}_i\in\mathbb{Z}_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{A}_i)$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{A}_i}\in\mathbb{Z}_q^{m\times m}$.

(3) 选取抗碰撞 Hash 函数 $H:\{0,1\}^{*}\rightarrow\mathbb{Z}_q^{dn}$.

(4) 输出公开参数 PP 和权威中心主私钥 MSK,

$$PP=(\{\boldsymbol{A}_i\}_{i\in U\cup U'},H,U,U'),$$

$$MSK=(\{\boldsymbol{T}_{\boldsymbol{A}_i}\}_{i\in U\cup U'}).$$

KeyGen:输入公开参数 PP,主私钥 MSK 和用户属性集 $w\subset U$,可简记 $w=\{1,2,\cdots,l_1\}$,$d\leq l_1\leq l$.

(1) 令 $\boldsymbol{C}\in\mathbb{Z}_q^{(l_1+d)n\times(l_1+d)m}$ 是由 $\{\boldsymbol{A}_i\in\mathbb{Z}_q^{n\times m}\}_{i\in w\cup U'}$ 构成的对角矩阵,即

$$\boldsymbol{C}=\begin{pmatrix}\boldsymbol{A}_1 & & & & \\ & \ddots & & & \\ & & \boldsymbol{A}_i & & \\ & & & \ddots & \\ & & & & \boldsymbol{A}_{l+d}\end{pmatrix}_{i\in w\cup U'}.$$

(2) 令 $\boldsymbol{T}_{\boldsymbol{C}}\in\mathbb{Z}_q^{(l_1+d)m\times(l_1+d)m}$ 是由 $\{\boldsymbol{T}_{\boldsymbol{A}_i}\in\mathbb{Z}_q^{m\times m}\}_{i\in w\cup U'}$ 构成的对角矩阵,即

$$\boldsymbol{T}_{\boldsymbol{C}}=\begin{pmatrix}\boldsymbol{T}_{\boldsymbol{A}_1} & & & & \\ & \ddots & & & \\ & & \boldsymbol{T}_{\boldsymbol{A}_i} & & \\ & & & \ddots & \\ & & & & \boldsymbol{T}_{\boldsymbol{A}_{l+d}}\end{pmatrix}_{i\in w\cup U'}.$$

易知 $\boldsymbol{T}_{\boldsymbol{C}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{C})$ 的陷门基,$\|\widetilde{\boldsymbol{T}}_{\boldsymbol{C}}\|\leq O(\sqrt{n\log_2 q})$.

(3) 随机选取 $\boldsymbol{B}_i\in\mathbb{Z}_q^{n\times m}$ 和最高次数不超过 $d-1$ 的多项式 $f_i(x)\in\mathbb{Z}_q[x]$,且 $f_i(0)=0 \bmod q$,$i\in w\cup U'$. $f_i(x)$ 在签名用户生成私钥和签名阶段生成签名私钥中扮演重要角色.

(4) 记 $l_2=l+d$,构造 $\boldsymbol{C}'\in\mathbb{Z}_q^{(l_1+d)n\times(l_1+d)m}$,

$$\boldsymbol{C}'=\begin{pmatrix}f_1(1)\boldsymbol{B}_1 & \cdots & f_i(1)\boldsymbol{B}_i & \cdots & f_{l_2}(1)\boldsymbol{B}_{l_2}\\ \vdots & & \vdots & & \vdots\\ f_1(i)\boldsymbol{B}_1 & \cdots & f_i(i)\boldsymbol{B}_i & \cdots & f_{l_2}(i)\boldsymbol{B}_{l_2}\\ \vdots & & \vdots & & \vdots\\ f_1(l_2)\boldsymbol{B}_1 & \cdots & f_i(l_2)\boldsymbol{B}_i & \cdots & f_{l_2}(l_2)\boldsymbol{B}_{l_2}\end{pmatrix}_{i\in w\cup U'}.$$

(5) 令 $\boldsymbol{F}=[\boldsymbol{C}\|\boldsymbol{C}']$,由引理 4 和引理 5 知,利用格 $\Lambda_q^{\perp}(\boldsymbol{C})$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{C}}$,可求得格 $\Lambda_q^{\perp}(\boldsymbol{F})$ 的陷门基矩阵 $\boldsymbol{T}_{\boldsymbol{F}}\in\mathbb{Z}_q^{(2l_1+2d)m\times(2l_1+2d)m}$,且 $\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}}\|=\|\widetilde{\boldsymbol{T}}_{\boldsymbol{C}}\|$.

(6) 输出私钥 $SK_w=\boldsymbol{T}_{\boldsymbol{F}}\in\mathbb{Z}_q^{(2l_1+2d)m\times(2l_1+2d)m}$.

Sign:输入公开参数 PP,用户私钥 SK_w 和签名消息 $\boldsymbol{u}\in\{0,1\}^{*}$. 用户利用属性子集 $w'\subseteq w$ 对消息 $\boldsymbol{u}$ 进行签名,可简记 $w'=\{1,2,\cdots,l'\}$,$1\leq l'\leq d$.

(1) 选取含有 $d-l'$ 个属性分量的默认属性子集 $U''\subseteq U'$,可简记 $U''=\{l+1,l+2,\cdots,l+d-l'\}$.

(2) 令 $\boldsymbol{F}'=[\boldsymbol{A}_1\|\boldsymbol{A}_2\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l'}]_{i\in w'\cup U''}$,现在构造格 $\Lambda_q^{\perp}(\boldsymbol{F}')$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{F}'}$.

(2.1) 令 $D=((l+d)!)^2$,计算拉格朗日插值系数 $L_i=\prod_{i,j\in w'\cup U'',i\neq j}\frac{j}{j-i}$,由引理 7 知,$DL_i$ 是整数.

(2.2) 令 $g_i=0$,$i\in(w-w')\cup(U'-U'')$.

(2.3) 令 $g_i=DL_i$,$i\in w'\cup U''$,$\boldsymbol{I}_n$ 表示 n 维单位矩阵,构造 $\boldsymbol{G}\in\mathbb{Z}_q^{n\times(l_1+d)n}$,

$$\boldsymbol{G}=[g_1\boldsymbol{I}_n\|g_2\boldsymbol{I}_n\|\cdots\|g_i\boldsymbol{I}_n\|\cdots\|g_{l+d}\boldsymbol{I}_n]_{i\in w\cup U'}.$$

(2.4) 由 $\boldsymbol{F}$ 的构造,易知 $\boldsymbol{G}\cdot\boldsymbol{F}\in\mathbb{Z}_q^{n\times(2l_1+2d)m}$,即有 $\boldsymbol{G}\cdot\boldsymbol{F}=[g_1\boldsymbol{A}_1\|\cdots\|g_i\boldsymbol{A}_i\|\cdots\|g_{l+d}\boldsymbol{A}_{l+d}\|\boldsymbol{0}\|\cdots\|\boldsymbol{0}]_{i\in w\cup U'}$,其中 $g_i\boldsymbol{A}_i=\boldsymbol{0}$,$i\in(w-w')\cup(U'-U'')$. 删除 $\boldsymbol{G}\cdot\boldsymbol{F}$ 中全零列得

$$\boldsymbol{F}''=[g_1\boldsymbol{A}_1\|\cdots\|g_i\boldsymbol{A}_i\|\cdots\|g_{l+d-l'}\boldsymbol{A}_{l+d-l'}]_{i\in w'\cup U''}.$$

(2.5) 矩阵 $\boldsymbol{T}_{\boldsymbol{F}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{F})$ 的陷门基,故 $\boldsymbol{T}_{\boldsymbol{F}}$ 也是格 $\Lambda_q^{\perp}(\boldsymbol{G}\cdot\boldsymbol{F})$ 的陷门基,删除 $\boldsymbol{T}_{\boldsymbol{F}}$ 中与 $\boldsymbol{G}\cdot\boldsymbol{F}$ 全零列相对应的行和列得 $\boldsymbol{T}_{\boldsymbol{F}''}\in\mathbb{Z}_q^{dm\times dm}$,且 $\boldsymbol{F}''\cdot\boldsymbol{T}_{\boldsymbol{F}''}=\boldsymbol{0}$,则 $\boldsymbol{T}_{\boldsymbol{F}''}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{F}'')$ 的陷门基,且 $\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}''}\|=\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}}\|$.

(2.6) 令 $\boldsymbol{I}_m$ 表示 m 维单位矩阵,构造 $\boldsymbol{G}'\in\mathbb{Z}_q^{dm\times dm}$,

$$\boldsymbol{G}'=\begin{pmatrix}g_1\boldsymbol{I}_m & & & & \\ & \ddots & & & \\ & & g_i\boldsymbol{I}_m & & \\ & & & \ddots & \\ & & & & g_{l+d-l'}\boldsymbol{I}_m\end{pmatrix}_{i\in w'\cup U''}.$$

(2.7) 易知 $\boldsymbol{F}''=\boldsymbol{F}'\cdot\boldsymbol{G}'$,又知 $\boldsymbol{F}''\cdot\boldsymbol{T}_{\boldsymbol{F}''}=\boldsymbol{0} \bmod q$. 令 $\boldsymbol{T}_{\boldsymbol{F}'}=\boldsymbol{G}'\cdot\boldsymbol{T}_{\boldsymbol{F}''}$,则 $\boldsymbol{T}_{\boldsymbol{F}'}\in\mathbb{Z}_q^{dm\times dm}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{F}')$ 的基矩阵,$\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}'}\|\leq\|\widetilde{\boldsymbol{G}}'\|\cdot\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}''}\|\leq\max\{g_i\}_{i\in w'\cup U''}\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}''}\|\leq D^2\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}''}\|$.

(3) 令高斯参数 $s\geq D^2\cdot\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}''}\|\cdot\omega(\sqrt{\log_2 dm})$,运行算法 $SampPre(\boldsymbol{F}',\boldsymbol{T}_{\boldsymbol{F}'},H(\boldsymbol{u}),s)$ 生成向量 $\boldsymbol{e}\in\mathbb{Z}^{dm}$.

(4) 输出签名 $\sigma=(\boldsymbol{u},\boldsymbol{e},w',U'')$.

Verify:输入公开参数 PP,签名 $\sigma=(\boldsymbol{u},\boldsymbol{e},w',U'')$.

(1) 重构矩阵 $\boldsymbol{F}'=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l'}]_{i\in w'\cup U''}$.

(2) 验证 $\|\boldsymbol{e}\|\leq D^2\cdot O(\sqrt{n\log_2 q})\cdot\omega(\sqrt{\log_2 dm})$,且 $\boldsymbol{F}'\cdot\boldsymbol{e}=H(\boldsymbol{u}) \bmod q$.

(3) 如果上述两个条件都满足,则接受签名;否则,拒绝.

4.2　正确性

定理 1.　签名接收者能有效验证签名的合法性.

证明.　令 $\sigma=(\boldsymbol{u},\boldsymbol{e},w',U'')$ 是隐藏的属性签名生成算法的输出,签名的合法性验证过程如下所述:

(1) 令 $i\in w'\cup U''$,验证者利用公开参数 PP 可构造矩阵 $\hat{\boldsymbol{F}}=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l'}]_{i\in w'\cup U''}$.

(2) 计算 $\hat{\boldsymbol{F}}\cdot\boldsymbol{e}=\boldsymbol{F}'\cdot\boldsymbol{e}=H(\boldsymbol{u})\bmod q$.

(3) 向量 $\boldsymbol{e}\in\mathbb{Z}^{dm}$ 是抽样算法 $SampPre(\cdot)$ 的输出,由引理 3 可知,$\boldsymbol{e}$ 以极大概率满足 $\|\boldsymbol{e}\|\leq s\sqrt{dm}$,在这里 $s\geq D^2O(\sqrt{n\log_2 q})\omega(\sqrt{\log_2 dm})\geq\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}'}\|\omega(\sqrt{\log_2 dm})$.

因此,签名接收者能够验证隐藏的属性签名的正确性. 证毕.

4.3 安全性证明

4.3.1 不可伪造性

定理 2. 如果存在 PPT 的伪造者 $\mathcal{A}$ 以概率 ε 成功伪造上述方案的一个签名,则利用 $\mathcal{A}$ 可构造 PPT 算法 $\mathcal{C}$ 以概率 $\varepsilon'=(1-2^{-\omega(\log_2 dn)})\cdot\varepsilon$ 求解 SIS 问题.

证明. 假设 $\mathcal{C}$ 获得 SIS 问题实例 $(\boldsymbol{S}\in\mathbb{Z}_q^{n\times m'},\beta)$,$m'=(l+d)m$,要求 $\mathcal{C}$ 通过模拟游戏利用 $\mathcal{A}$ 求解出一个非零向量 $\boldsymbol{e}$,使得 $\boldsymbol{S}\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q$ 且 $\|\boldsymbol{e}\|\leq\beta$.

初始化. 假设属性全集 $U=\{1,2,\cdots,l\}$.

(1) 令 $\boldsymbol{S}=[\boldsymbol{S}_1\|\boldsymbol{S}_2\|\cdots\|\boldsymbol{S}_i\|\cdots\|\boldsymbol{S}_{l+d}]\in\mathbb{Z}_q^{n\times m'}$,其中 $\boldsymbol{S}_i\in\mathbb{Z}_q^{n\times m}$,$i=1,2,\cdots,l+d$.

(2) $\mathcal{A}$ 选取签名策略 $w^*\subset U$,并发送给 $\mathcal{C}$,可简记 $w^*=\{1,2,\cdots,l^*\}$,$1\leq l^*\leq d$.

系统建立. 输入安全参数 n,$\mathcal{C}$ 模拟公开参数 PP,

(1) 令默认属性集 $U'=\{l+1,l+2,\cdots,l+d\}$.

(2) 选取含有 $d-l^*$ 个属性分量的默认属性子集 $U''\subseteq U'$,可简记 $U''=\{l+1,l+2,\cdots,l+d-l^*\}$.

(3) 若 $i\in w^*\cup U''$,令 $\boldsymbol{A}_i=\boldsymbol{S}_i$.

(4) 若 $i\in(U-w^*)\cup(U'-U'')$,运行陷门生成算法 $TrapGen(q,n)$ 生成 $\boldsymbol{A}_i\in\mathbb{Z}_q^{n\times m}$ 和 $\Lambda_q^{\perp}(\boldsymbol{A}_i)$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{A}_i}\in\mathbb{Z}_q^{m\times m}$,且 $\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}_i}\|\leq O(\sqrt{n\log_2 q})$.

(5) 选取抗碰撞 Hash 函数 $H:\{0,1\}^*\to\mathbb{Z}_q^{dn}$.

(6) 输出公开参数 $PP=(\{\boldsymbol{A}_i\}_{i\in U\cup U'},H,U,U')$.

询问阶段. $\mathcal{A}$ 进行如下多项式有界次适应性询问.

私钥询问:$\mathcal{A}$ 选取签名策略 $w\subset U$,$w^*\not\subset w$,可简记 $w=\{1,2,\cdots,l_1\}\cup\{l_0+1,\cdots,l_1'\}$,$l_1<l^*\leq l_0<l_1'\leq l$. $\mathcal{C}$ 模拟对应于 w 的私钥 SK_w.

(1) 令 $w'=(w\cap w^*)\cup U''$. 若 $i\in w'$,运行陷门生成算法 $TrapGen(q,n)$ 生成 $\boldsymbol{B}_i\in\mathbb{Z}_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{B}_i)$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{B}_i}\in\mathbb{Z}_q^{m\times m}$.

(2) 令 $w''=(w-w\cap w^*)\cup(U'-U'')$. 若 $i\in w''$,随机选取矩阵 $\boldsymbol{B}_i\in\mathbb{Z}_q^{n\times m}$.

(3) 令 $\boldsymbol{C}_0$ 是由 $\{\boldsymbol{A}_i\}_{i\in w'}$ 构成的对角矩阵,即

$$\boldsymbol{C}_0=\begin{pmatrix}\boldsymbol{A}_1 & & & & \\ & \ddots & & & \\ & & \boldsymbol{A}_i & & \\ & & & \ddots & \\ & & & & \boldsymbol{A}_{l+d-l^*}\end{pmatrix}_{i\in w'}.$$

(4) 令 $\boldsymbol{C}_0'$ 是由 $\{\boldsymbol{A}_i\}_{i\in w''}$ 构成的对角矩阵,即

$$\boldsymbol{C}_0'=\begin{pmatrix}\boldsymbol{A}_{l_0+1} & & & & \\ & \ddots & & & \\ & & \boldsymbol{A}_i & & \\ & & & \ddots & \\ & & & & \boldsymbol{A}_{l+d}\end{pmatrix}_{i\in w''}.$$

令 $\boldsymbol{T}_{\boldsymbol{C}_0'}$ 是由 $\{\boldsymbol{T}_{\boldsymbol{A}_i}\}_{i\in w''}$ 构成的对角矩阵,即

$$\boldsymbol{T}_{\boldsymbol{C}_0'}=\begin{pmatrix}\boldsymbol{T}_{\boldsymbol{A}_{l_0+1}} & & & & \\ & \ddots & & & \\ & & \boldsymbol{T}_{\boldsymbol{A}_i} & & \\ & & & \ddots & \\ & & & & \boldsymbol{T}_{\boldsymbol{A}_{l+d}}\end{pmatrix}_{i\in w''},$$

易知 $\boldsymbol{T}_{\boldsymbol{C}_0'}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{C}_0')$ 的陷门基.

(5) 随机选取 $l_1+l_1'+d-l_0$ 个最高次数不超过 $d-1$ 的多项式 $f_i(x)\in\mathbb{Z}_q[x]$,且满足 $f_i(0)=0\bmod q$,$i\in\{1,2,\cdots,l_1+l_1'+d-l_0\}$.

(6) 令 $l_2=l+d-l^*$,构造矩阵 $\boldsymbol{C}_1$,

$$\boldsymbol{C}_1=\begin{pmatrix}f_1(1)\boldsymbol{B}_1 & \cdots & f_j(1)\boldsymbol{B}_j & \cdots & f_{l_2}(1)\boldsymbol{B}_{l_2}\\ \vdots & & \vdots & & \vdots\\ f_1(i)\boldsymbol{B}_1 & \cdots & f_j(i)\boldsymbol{B}_j & \cdots & f_{l_2}(i)\boldsymbol{B}_{l_2}\\ \vdots & & \vdots & & \vdots\\ f_1(l_2)\boldsymbol{B}_1 & \cdots & f_j(l_2)\boldsymbol{B}_j & \cdots & f_{l_2}(l_2)\boldsymbol{B}_{l_2}\end{pmatrix}_{i\in w',j\in w'}.$$

令 $\boldsymbol{T}_{\boldsymbol{C}_1}$ 是由 $\{\boldsymbol{T}_{\boldsymbol{B}_i}\}_{i\in w'}$ 构成的对角矩阵,即

$$\boldsymbol{T}_{\boldsymbol{C}_1}=\begin{pmatrix}\boldsymbol{T}_{\boldsymbol{B}_1} & & & & \\ & \ddots & & & \\ & & \boldsymbol{T}_{\boldsymbol{B}_i} & & \\ & & & \ddots & \\ & & & & \boldsymbol{T}_{\boldsymbol{B}_{l+d-l^*}}\end{pmatrix}_{i\in w'},$$

易知 $\boldsymbol{T}_{\boldsymbol{C}_1}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{C}_1)$ 的陷门基.

(7) 令 $l_3=l_0+1$,$l_3'=l+d$,构造矩阵 $\boldsymbol{C}_1'$,

$$\boldsymbol{C}_1'=\begin{pmatrix} f_1(l_3)\boldsymbol{B}_1 & \cdots & f_j(l_3)\boldsymbol{B}_j & \cdots & f_{l_2}(l_3)\boldsymbol{B}_{l_2} \\ \vdots & & \vdots & & \vdots \\ f_1(i)\boldsymbol{B}_1 & \cdots & f_j(i)\boldsymbol{B}_j & \cdots & f_{l_2}(i)\boldsymbol{B}_{l_2} \\ \vdots & & \vdots & & \vdots \\ f_1(l_3')\boldsymbol{B}_1 & \cdots & f_j(l_3')\boldsymbol{B}_j & \cdots & f_{l_2}(l_3')\boldsymbol{B}_{l_2} \end{pmatrix}_{i\in w'',j\in w'}.$$

(8) 构造矩阵 $\boldsymbol{C}_2$，

$$\boldsymbol{C}_2=\begin{pmatrix} f_{l_3}(1)\boldsymbol{B}_{l_3} & \cdots & f_j(1)\boldsymbol{B}_j & \cdots & f_{l_3'}(1)\boldsymbol{B}_{l_3'} \\ \vdots & & \vdots & & \vdots \\ f_{l_3}(i)\boldsymbol{B}_{l_3} & \cdots & f_j(i)\boldsymbol{B}_j & \cdots & f_{l_3'}(i)\boldsymbol{B}_{l_3'} \\ \vdots & & \vdots & & \vdots \\ f_{l_3}(l_2)\boldsymbol{B}_{l_3} & \cdots & f_j(l_2)\boldsymbol{B}_j & \cdots & f_{l_3'}(l_2)\boldsymbol{B}_{l_3'} \end{pmatrix}_{i\in w',j\in w''}.$$

(9) 构造矩阵 $\boldsymbol{C}_2'$，

$$\boldsymbol{C}_2'=\begin{pmatrix} f_{l_3}(l_3)\boldsymbol{B}_{l_3} & \cdots & f_j(l_3)\boldsymbol{B}_j & \cdots & f_{l_3'}(l_3)\boldsymbol{B}_{l_3'} \\ \vdots & & \vdots & & \vdots \\ f_{l_3}(i)\boldsymbol{B}_{l_3} & \cdots & f_j(i)\boldsymbol{B}_j & \cdots & f_{l_3'}(i)\boldsymbol{B}_{l_3'} \\ \vdots & & \vdots & & \vdots \\ f_{l_3}(l_3')\boldsymbol{B}_{l_3} & \cdots & f_j(l_3')\boldsymbol{B}_j & \cdots & f_{l_3'}(l_3')\boldsymbol{B}_{l_3'} \end{pmatrix}_{i\in w'',j\in w''}.$$

(10) 令 $\boldsymbol{F}=\begin{pmatrix}\boldsymbol{C}_0 & \boldsymbol{0} & \boldsymbol{C}_1 & \boldsymbol{C}_2\\ \boldsymbol{0} & \boldsymbol{C}_0' & \boldsymbol{C}_1' & \boldsymbol{C}_2'\end{pmatrix}$.

(11) 重排 $\boldsymbol{F}$ 的列向量，$\boldsymbol{F}'=\begin{pmatrix}\boldsymbol{C}_1 & \boldsymbol{0} & \boldsymbol{C}_0 & \boldsymbol{C}_2\\ \boldsymbol{C}_1' & \boldsymbol{C}_0' & \boldsymbol{0} & \boldsymbol{C}_2'\end{pmatrix}$.

(12) 令 $\boldsymbol{F}_1'=\begin{pmatrix}\boldsymbol{C}_1 & \boldsymbol{0}\\ \boldsymbol{C}_1' & \boldsymbol{C}_0'\end{pmatrix}$，易知 $\boldsymbol{T}_{\boldsymbol{F}_1'}=\begin{pmatrix}\boldsymbol{T}_{\boldsymbol{C}_1} & \\ & \boldsymbol{T}_{\boldsymbol{C}_0'}\end{pmatrix}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{F}_1')$ 的陷门基. 由引理 4 和引理 5 知，利用 $\boldsymbol{T}_{\boldsymbol{F}_1'}$ 可得格 $\Lambda_q^{\perp}(\boldsymbol{F}')$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{F}'}$，将 $\boldsymbol{T}_{\boldsymbol{F}'}$ 的行向量重排可得格 $\Lambda_q^{\perp}(\boldsymbol{F})$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{F}}\in\mathbb{Z}_q^{(2l_1+2l_1'+2d-2l_0)m\times(2l_1+2l_1'+2d-2l_0)m}$.

(13) 输出私钥 $SK_w=\boldsymbol{T}_{\boldsymbol{F}}$.

$\mathcal{C}$ 模拟对消息 $\boldsymbol{u}$ 及签名策略 $w\subset U$ 的签名 $\boldsymbol{e}$，可简记 $w=\{1,2,\cdots,l'\}$，$l'\leq d$. 不失一般性，假设 $\mathcal{A}$ 在签名询问和输出伪造签名前对消息进行过 Hash 询问.

Hash 询问：$\mathcal{C}$ 对每一个不同的消息 $\boldsymbol{u}$ 模拟 H.

(1) 选取含有 $d-l'$ 个属性分量的默认属性子集 $U''\subseteq U'$，可简记 $U''=\{l+1,l+2,\cdots,l+d-l'\}$.

(2) 令 $\boldsymbol{F}''=[\boldsymbol{A}_1\|\boldsymbol{A}_2\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l'}]_{i\in w\cup U''}$.

(3) 查找 Hash 询问列表中是否存在对 $\boldsymbol{u}$ 的应答，若存在，直接返回；否则，运行算法 $SampDom(n)$，输出统计接近 $D_{\mathbb{Z}_q^{dm},s}$ 的向量 $\boldsymbol{e}_{\boldsymbol{u}}\in\mathbb{Z}_q^{dm}$，存储 $(\boldsymbol{u},w,\boldsymbol{e}_{\boldsymbol{u}})$，并将 $\boldsymbol{F}''\cdot\boldsymbol{e}_{\boldsymbol{u}}$ 作为 Hash 询问的结果返回给 $\mathcal{A}$.

签名询问：$\mathcal{C}$ 首先查找 Hash 询问列表中存储的 $(\boldsymbol{u},w,\boldsymbol{e}_{\boldsymbol{u}})$，并将 $\boldsymbol{e}_{\boldsymbol{u}}$ 作为 $(\boldsymbol{u},w)$ 的签名返回给 $\mathcal{A}$.

伪造. $\mathcal{A}$ 输出消息 $\boldsymbol{u}^*$，签名策略 w^*，默认属性子集 $U''=\{l+1,\cdots,l+d-l^*\}$ 及伪造签名 $\boldsymbol{e}_{\boldsymbol{u}^*}^*$. 不失一般性，假设在输出伪造之前，$\mathcal{A}$ 已对 $\boldsymbol{u}^*$ 进行过 Hash 询问，并得到询问结果 $H(\boldsymbol{u}^*)=\boldsymbol{F}^*\boldsymbol{e}_{\boldsymbol{u}^*}\in\mathbb{Z}_q^{dn}$，在这里，矩阵 $\boldsymbol{F}^*=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l^*}]_{i\in w^*\cup U''}$. 由 Hash 函数的原像极小熵性质，给定 $\boldsymbol{F}^*\cdot\boldsymbol{e}_{\boldsymbol{u}^*}$，向量 $\boldsymbol{e}_{\boldsymbol{u}^*}$ 的极小熵为 $\omega(\log_2 dn)$. 从而，$\boldsymbol{e}_{\boldsymbol{u}^*}^*\neq\boldsymbol{e}_{\boldsymbol{u}^*}$ 以接近 $1-2^{-\omega(\log_2 dn)}$ 的概率成立. $\boldsymbol{e}_{\boldsymbol{u}^*}^*$ 是 $\boldsymbol{u}^*$ 的伪造签名，$\mathcal{C}$ 查找 Hash 询问列表中存储的 $(\boldsymbol{u}^*,w^*,\boldsymbol{e}_{\boldsymbol{u}^*})$，则 $\boldsymbol{F}^*\boldsymbol{e}_{\boldsymbol{u}^*}^*=H(\boldsymbol{u}^*)=\boldsymbol{F}^*\boldsymbol{e}_{\boldsymbol{u}^*}\bmod q$. 由于 $\boldsymbol{e}_{\boldsymbol{u}^*}^*\neq\boldsymbol{e}_{\boldsymbol{u}^*}$，令 $\boldsymbol{e}^*=\boldsymbol{e}_{\boldsymbol{u}^*}^*-\boldsymbol{e}_{\boldsymbol{u}^*}$，可得 $\boldsymbol{F}^*\cdot\boldsymbol{e}^*=\boldsymbol{0}\bmod q$，且 $0<\|\boldsymbol{e}^*\|\leq\|\boldsymbol{e}_{\boldsymbol{u}^*}^*\|+\|\boldsymbol{e}_{\boldsymbol{u}^*}\|\leq 2s\sqrt{dm}$. $\boldsymbol{F}^*$ 是 $\boldsymbol{S}$ 的子矩阵，在 $\boldsymbol{e}^*\in\mathbb{Z}_q^{dm}$ 中插入 l 个 m 维零向量可得 $\boldsymbol{e}'\in\mathbb{Z}_q^{(l+d)m}$，$\boldsymbol{S}\cdot\boldsymbol{e}'=\boldsymbol{0}\bmod q$，且 $0<\|\boldsymbol{e}'\|\leq 2s\sqrt{dm}$.

故若存在 PPT 的伪造者 $\mathcal{A}$ 以概率 ε 成功伪造上述签名方案的一个签名，则 $\mathcal{C}$ 可利用 $\mathcal{A}$ 以概率 $\varepsilon'=(1-2^{-\omega(\log_2 dn)})\cdot\varepsilon$ 求得 SIS 问题实例 $\boldsymbol{S}\in\mathbb{Z}_q^{n\times(l+d)m}$，$\beta=2s\sqrt{dm}$ 的一个解 $\boldsymbol{e}'$. 证毕.

4.3.2 匿名性

定理 3. 上述 HABS 方案满足匿名性.

证明. 挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$ 进行如下游戏.

系统建立. 挑战者 $\mathcal{C}$ 输入安全参数 n，属性全集 $U=\{1,2,\cdots,l\}$，默认属性集 $U'=\{l+1,\cdots,l+d\}$，选取抗碰撞 Hash 函数 $H:\{0,1\}^*\to\mathbb{Z}_q^{dn}$，运行 Setup 算法生成公开参数 PP 和权威中心主私钥 MSK，即

$$PP=(\{\boldsymbol{A}_i\}_{i\in U\cup U'},H,U,U'),$$

$$MSK=(\{\boldsymbol{T}_{\boldsymbol{A}_i}\}_{i\in U\cup U'}),$$

并将 PP 和 MSK 发送给 $\mathcal{A}$.

$\mathcal{A}$ 可以利用 MSK 生成对应于任意属性集的私钥和对任意消息进行签名.

挑战阶段. $\mathcal{A}$ 选取挑战消息 $\boldsymbol{u}^*$，两个不同属性集 $w_0,w_1\subset U$，签名策略 $w^*\subset w'$，$w'=w_0\cap w_1$，可简记 $w^*=\{1,2,\cdots,l^*\}$. $\mathcal{C}$ 利用 MSK 分别生成对应于 w_0,w_1 的私钥 SK_{w_0},SK_{w_1}. $\mathcal{C}$ 随机选取默认属性子集 U''，可简记 $U''=\{l+1,l+2,\cdots,l+d-l^*\}$. 然后，$\mathcal{C}$ 随机选取 $b\in\{0,1\}$，利用私钥 SK_{w_b}，运行 Sign 算法获得对消息 $\boldsymbol{u}^*$ 和签名策略 w^* 的签名 $\boldsymbol{e}_b^*$，并返回给 $\mathcal{A}$.

现在对签名阶段进行分析.

令签名矩阵 $\boldsymbol{F}'=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l^*}]_{i\in w^*\cup U''}$，

签名私钥 $SK_{w_b}=\mathrm{KeyGen}(PP,MSK,w_b)$ 和生成签名 $e_b^*=\mathrm{Sign}(PP,SK_{w_b},w^*,\boldsymbol{u}^*)$. 由于向量 $\boldsymbol{e}_0^*,\boldsymbol{e}_1^*\in\mathbb{Z}_q^{dm}$ 统计接近 $D_{\Lambda_q^{H(\boldsymbol{u}^*)}(\boldsymbol{F}'),s}$，故 $\boldsymbol{e}_0^*,\boldsymbol{e}_1^*$ 的分布统计不可区分，且 $\|\boldsymbol{e}_0^*\|,\|\boldsymbol{e}_1^*\|\leq s\sqrt{dm}$，从而敌手 $\mathcal{A}$ 正确猜测 b 的优势是可忽略的.

综上可得，上述 HABS 方案满足匿名性要求.

证毕.

4.4 效率分析

该属性签名方案与随机预言机模型下支持门限签名策略的属性签名方案[15]一样，都使用了高斯抽样算法和小整数上的矩阵-向量的模乘运算，其计算复杂度分别为 $\tilde{O}(n^2)$，$O(n^2)$. 将本方案与采用零知识证明非交互协议的文献[15]进行比较，结果如表 1 所示.

表 1 随机预言机模型下不同方案的效率对比

	文献[15]	本文方案
公钥尺寸	$\tilde{O}(ln^2)$	$\tilde{O}((l+d)n^2)$
私钥尺寸	$\tilde{O}(ln^2)$	$\tilde{O}((l+d)n^2)$
签名尺寸	$\tilde{O}((l+t'-t)n\log_2\beta)$	$\tilde{O}(dn)$
签名的计算复杂度	$O(n^2)$	$\tilde{O}(n^2)$
验证的计算复杂度	$O(n^2)$	$O(n^2)$
抗适应性选择消息攻击	是	是
支持属性任意子集签名	否	是

文献[15]的公私钥尺寸中隐含着一个常数因子 2. 由比较可得，本文的属性签名方案的公私钥尺寸和签名尺寸较文献[15]占用更少的存储空间，其中 $t\leq t'$，$d<l$. 而且，本方案的签名者可以灵活地利用其属性的任意子集来签署消息，这个特性是文献[15]不能达到的.

5 标准模型下 HABS 方案

与第 4 节一样，预先固定一个满足实际应用的常数 $d<l$. 签名者可以灵活利用其属性集的 $1,2,\cdots,d$ 个属性分量对消息进行签名. 在下文中，固定签名消息 $\boldsymbol{u}=(u_0,u_1,\cdots,u_k)\in\{0\}\times\{0,1\}^k$.

5.1 方案构造

Setup：输入安全参数 n，属性全集 $U=\{1,\cdots,l\}$.

(1) 令默认属性集 $U'=\{l+1,l+2,\cdots,l+d\}$.

(2) 令 $i\in U\cup U'$，运行算法 $TrapGen(q,n)$ 生成矩阵 $\boldsymbol{A}_i\in\mathbb{Z}_q^{n\times m}$ 和格 $\Lambda_q^{\perp}(\boldsymbol{A}_i)$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{A}_i}\in\mathbb{Z}_q^{m\times m}$.

(3) 随机选取 $k+1$ 个矩阵 $\boldsymbol{Y}_i\in\mathbb{Z}_q^{n\times m}$，$i\in\{0,\cdots,k\}$.

(4) 输出公开参数 PP 和权威中心主私钥 MSK，

$$PP=(\{\boldsymbol{A}_i\}_{i\in U\cup U'},\{\boldsymbol{Y}_i\}_{i\in\{0,1,\cdots,k\}},U,U'),$$

$$MSK=(\{\boldsymbol{T}_{\boldsymbol{A}_i}\}_{i\in U\cup U'}).$$

KeyGen：输入公开参数 PP，主私钥 MSK 和用户属性集 $w\subset U$，可简记 $w=\{1,2,\cdots,l_1\}$，$d\leq l_1\leq l$.

与 4.1 节 KeyGen 相同，不再赘述.

最终输出私钥 $SK_w=\boldsymbol{T}_{\boldsymbol{F}}\in\mathbb{Z}_q^{(2l_1+2d)m\times(2l_1+2d)m}$.

Sign：输入公开参数 PP，用户私钥 SK_w 和消息 $\boldsymbol{u}$. 用户利用属性子集 $w'\subseteq w$ 对消息 $\boldsymbol{u}$ 进行签名，可简记 $w'=\{1,2,\cdots,l'\}$，$1\leq l'\leq d$.

(1)～(2.7)与 4.1 节 Sign 中相同，不再赘述.

(3) 令 $\boldsymbol{Y}_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}\boldsymbol{Y}_i\in\mathbb{Z}_q^{n\times m}$.

(4) 令 $\boldsymbol{F}'''=[\boldsymbol{F}'\|\boldsymbol{Y}_{\boldsymbol{u}}]\in\mathbb{Z}_q^{n\times(d+1)m}$，由引理 4 和引理 5 知，利用 $\Lambda_q^{\perp}(\boldsymbol{F}')$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{F}'}$，可得格 $\Lambda_q^{\perp}(\boldsymbol{F}''')$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{F}'''}\in\mathbb{Z}_q^{(d+1)m\times(d+1)m}$，且 $\|\tilde{\boldsymbol{T}}_{\boldsymbol{F}'''}\|=\|\tilde{\boldsymbol{T}}_{\boldsymbol{F}'}\|$.

(5) 令高斯参数 $s\geq\|\tilde{\boldsymbol{T}}_{\boldsymbol{F}'''}\|\cdot\omega(\sqrt{\log_2(d+1)m})$，运行算法 $SampPre(\boldsymbol{F}''',\boldsymbol{T}_{\boldsymbol{F}'''},s,\boldsymbol{0})$ 生成向量 $\boldsymbol{e}\in\mathbb{Z}^{(d+1)m}$.

(6) 输出签名 $\sigma=(\boldsymbol{u},\boldsymbol{e},w',U'')$.

Verify：输入公开参数 PP，签名 $\sigma=(\boldsymbol{u},\boldsymbol{e},w',U'')$.

(1) 验证 $\boldsymbol{u}\in\{0\}\times\{0,1\}^k$.

(2) 令 $\boldsymbol{Y}_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}\boldsymbol{Y}_i$.

(3) 重构 $\boldsymbol{F}'''=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l'}\|\boldsymbol{Y}_{\boldsymbol{u}}]_{i\in w'\cup U''}$.

(4) 验证 $\|\boldsymbol{e}\|\leq s\sqrt{(d+1)m}$，且 $\boldsymbol{F}'''\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q$.

(5) 如果上述条件满足，则接受签名；否则，拒绝.

5.2 正确性

定理 4. 签名接收者能有效地验证签名的合法性.

证明. 令 $\sigma=(\boldsymbol{u},\boldsymbol{e},w',U'')$ 是隐藏的属性签名生成算法的输出，签名的合法性验证过程如下所述：

(1) 验证者利用公开参数 PP 和签名所对应的消息 $\boldsymbol{u}\in\{0\}\times\{0,1\}^k$，计算 $\boldsymbol{Y}_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}\boldsymbol{Y}_i$.

(2) 令 $i\in w'\cup U''$，验证者利用公开参数 PP 可构造矩阵 $\bar{\boldsymbol{F}}=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l'}]_{i\in w'\cup U''}$.

(3) 令 $\hat{\boldsymbol{F}}=[\bar{\boldsymbol{F}}\|\boldsymbol{Y}_{\boldsymbol{u}}]$，计算 $\hat{\boldsymbol{F}}\cdot\boldsymbol{e}=\boldsymbol{F}'''\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q$.

(4) 向量 $\boldsymbol{e}\in\mathbb{Z}^{(d+1)m}$ 是抽样算法 $SampPre(\cdot)$ 的输出，由引理 3 知，$\boldsymbol{e}$ 以极大概率满足 $\|\boldsymbol{e}\|\leq s\sqrt{(d+1)m}$，在这里，高斯参数 s 满足：

$$s\geq D^2\cdot O(\sqrt{n\log_2 q})\cdot\omega(\sqrt{\log_2(d+1)m})$$

$$\geq\|\tilde{\boldsymbol{T}}_{\boldsymbol{F}'''}\|\cdot\omega(\sqrt{\log_2(d+1)m}).$$

因此，签名接收者能够验证隐藏的属性签名的正确性. 证毕.

5.3 安全性证明

5.3.1 不可伪造性

定理 5. 如果存在 PPT 的伪造者 $\mathcal{A}$ 至多进行 $Q\leq q/2$ 次签名询问，以概率 ε 成功伪造上述方案的一个签名，则利用 $\mathcal{A}$ 可以构造 PPT 算法 $\mathcal{C}$ 以概率 $\varepsilon'\geq\varepsilon/3q$ 求解 SIS 问题.

证明. 假设 $\mathcal{C}$ 获得SIS问题实例$(\boldsymbol{S}\in\mathbb{Z}_q^{n\times m'},\beta)$，$m'=(l+d)m$，要求 $\mathcal{C}$ 通过模拟游戏利用 $\mathcal{A}$ 求出一个非零向量 $\boldsymbol{e}$，使得 $\boldsymbol{S}\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q$ 且 $\|\boldsymbol{e}\|\leq\beta$.

初始化. 假设属性全集 $U=\{1,2,\cdots,l\}$.

(1) 令 $\boldsymbol{S}=[\boldsymbol{S}_1\|\boldsymbol{S}_2\|\cdots\|\boldsymbol{S}_i\|\cdots\|\boldsymbol{S}_{l+d}]\in\mathbb{Z}_q^{n\times m'}$，其中 $\boldsymbol{S}_i\in\mathbb{Z}_q^{n\times m}$，$i\in\{1,2,\cdots,l+d\}$.

(2) $\mathcal{A}$ 选取签名策略 $w^*\subset U$，并发送给 $\mathcal{C}$，可简记 $w^*=\{1,2,\cdots,l^*\}$，$1\leq l^*\leq d$.

系统建立. 输入安全参数 n，$\mathcal{C}$ 模拟公开参数 PP，

(1) 令默认属性集 $U'=\{l+1,l+2,\cdots,l+d\}$.

(2) 选取含有 $d-l^*$ 个属性分量的默认属性子集 $U''\subseteq U'$，可简记 $U''=\{l+1,l+2,\cdots,l+d-l^*\}$.

(3) 若 $i\in w^*\cup U''$，令 $\boldsymbol{A}_i=\boldsymbol{S}_i$.

(4) 若 $i\in(U-w^*)\cup(U'-U'')$，运行陷门生成算法 $TrapGen(q,n)$生成矩阵$\boldsymbol{A}_i\in\mathbb{Z}_q^{n\times m}$和格 $\Lambda_q^{\perp}(\boldsymbol{A}_i)$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{A}_i}\in\mathbb{Z}_q^{m\times m}$.

(5) 运行算法 $TrapGen(q,n)$生成 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$和格 $\Lambda_q^{\perp}(\boldsymbol{A}_0)$的陷门基 $\boldsymbol{T}_{\boldsymbol{A}_0}\in\mathbb{Z}_q^{m\times m}$.

(6) 随机选取矩阵 $\boldsymbol{R}_i\in\{1,-1\}^{m\times m}$，$i\in\{0,1,\cdots,k\}$.

(7) 随机选取标量$h_i\in\mathbb{Z}_q$，$i\in\{1,\cdots,k\}$. 令$h_0=1$.

(8) 令 $\boldsymbol{Y}_i=\boldsymbol{A}_{l+1}\boldsymbol{R}_i+h_i\boldsymbol{A}_0\bmod q$，$i\in\{0,1,\cdots,k\}$.

(9) 输出公开参数 PP，

$PP=(\{\boldsymbol{A}_i\}_{i\in U\cup U'},\{\boldsymbol{Y}_i\}_{i\in\{0,1,\cdots,k\}},U,U')$.

询问阶段. $\mathcal{A}$ 进行如下多项式有界次适应性询问.

私钥询问：$\mathcal{A}$ 选取签名策略 $w\subset U$，$w^*\not\subset w$，可简记 $w=\{1,2,\cdots,l_1\}\cup\{l_0+1,\cdots,l_1'\}$，$l_1<l^*\leq l_0<l_1'\leq l$. $\mathcal{C}$ 模拟对应于 w 的私钥 SK_w.

与 4.3.1 节询问阶段的私钥询问模拟相同，不再赘述.

输出$SK_w=\boldsymbol{T}_{\boldsymbol{F}}\in\mathbb{Z}_q^{(2l_1+2l_1'+2d-2l_0)m\times(2l_1+2l_1'+2d-2l_0)m}$.

签名询问：$\mathcal{C}$ 模拟对 $\boldsymbol{u}$ 及签名策略 $w\subset U$ 的签名 $\boldsymbol{e}$，可简记 $w=\{1,2,\cdots,l'\}$，$l'\leq d$. 选取默认属性子集 $U''\subseteq U'$，可简记 $U''=\{l+1,l+2,\cdots,l+d-l'\}$. 令矩阵 $\boldsymbol{F}''=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l'}]_{i\in w\cup U''}$.

I. 若 $w^*\not\subset w$，则对 w 进行签名私钥模拟 SK_w. 利用 SK_w易得格 $\Lambda_q^{\perp}(\boldsymbol{F}'')$的陷门基 $\boldsymbol{T}_{\boldsymbol{F}''}$.

(1) 令 $\boldsymbol{R}_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}\boldsymbol{R}_i$，$h_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}h_i$，则 $\boldsymbol{Y}_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}\boldsymbol{Y}_i=\boldsymbol{A}_{l+1}\boldsymbol{R}_{\boldsymbol{u}}+h_{\boldsymbol{u}}\boldsymbol{A}_0$.

(2) 令 $\boldsymbol{F}'''=[\boldsymbol{F}''\|\boldsymbol{Y}_{\boldsymbol{u}}]$，由引理 4 和引理 5 知，利用 $\Lambda_q^{\perp}(\boldsymbol{F}'')$的陷门基 $\boldsymbol{T}_{\boldsymbol{F}''}$，可得格 $\Lambda_q^{\perp}(\boldsymbol{F}''')$的陷门基矩阵 $\boldsymbol{T}_{\boldsymbol{F}'''}\in\mathbb{Z}_q^{(d+1)m\times(d+1)m}$，且$\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}'''}\|=\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}''}\|$.

(3) 令高斯参数 $s\geq\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}'''}\|\cdot\omega(\sqrt{\log_2(d+1)m})$，运行算法 $SampPre(\boldsymbol{F}''',\boldsymbol{T}_{\boldsymbol{F}'''},s,\boldsymbol{0})$ 生成向量 $\boldsymbol{e}\in\mathbb{Z}^{(d+1)m}$.

(4) 输出签名 $\sigma=(\boldsymbol{u},\boldsymbol{e},w,U'')$.

II. 若 $w^*\subseteq w$，则无法对 w 进行如上签名私钥模拟.

(1) 令 $\boldsymbol{R}_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}\boldsymbol{R}_i$，$h_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}h_i$，则 $\boldsymbol{Y}_{\boldsymbol{u}}=\sum_{i=0}^{k}(-1)^{u_i}\boldsymbol{Y}_i=\boldsymbol{A}_{l+1}\boldsymbol{R}_{\boldsymbol{u}}+h_{\boldsymbol{u}}\boldsymbol{A}_0$.

(2) 若 $h_{\boldsymbol{u}}=0\bmod q$，则放弃模拟.

(3) 令 $\hat{\boldsymbol{F}}=[\boldsymbol{A}_{l+1}\|\boldsymbol{Y}_{\boldsymbol{u}}]\in\mathbb{Z}_q^{n\times 2m}$，由引理 6 知，利用 $\Lambda_q^{\perp}(\boldsymbol{A}_0)$的陷门基 $\boldsymbol{T}_{\boldsymbol{A}_0}$可得格 $\Lambda_q^{\perp}(\hat{\boldsymbol{F}})$的陷门基矩阵 $\boldsymbol{T}_{\hat{\boldsymbol{F}}}\in\mathbb{Z}_q^{2m\times 2m}$.

(4) 令 $\boldsymbol{F}'''=[\boldsymbol{F}''\|\boldsymbol{Y}_{\boldsymbol{u}}]$，由引理 4 和引理 5 知，利用 $\Lambda_q^{\perp}(\hat{\boldsymbol{F}})$的陷门基 $\boldsymbol{T}_{\hat{\boldsymbol{F}}}$可得格 $\Lambda_q^{\perp}(\boldsymbol{F}''')$的陷门基矩阵 $\boldsymbol{T}_{\boldsymbol{F}'''}\in\mathbb{Z}_q^{(d+1)m\times(d+1)m}$.

(5) 令高斯参数 $s\geq\|\widetilde{\boldsymbol{T}}_{\boldsymbol{F}'''}\|\cdot\omega(\sqrt{\log_2(d+1)m})$，运行算法 $SampPre(\boldsymbol{F}''',\boldsymbol{T}_{\boldsymbol{F}'''},s,\boldsymbol{0})$ 生成向量 $\boldsymbol{e}\in\mathbb{Z}^{(d+1)m}$.

(6) 输出签名 $\sigma=(\boldsymbol{u},\boldsymbol{e},w,U'')$.

伪造. $\mathcal{A}$ 输出消息 $\boldsymbol{u}^*=(u_0^*,u_1^*,\cdots,u_k^*)$，签名策略 w^*，默认属性子集 $U''=\{l+1,\cdots,l+d-l^*\}$及伪造签名 $\boldsymbol{e}^*=(\boldsymbol{e}_1,\cdots,\boldsymbol{e}_i,\cdots,\boldsymbol{e}_{l+d-l^*},\hat{\boldsymbol{e}})_{i\in w^*\cup U''}$，其中 $\boldsymbol{e}_i,\hat{\boldsymbol{e}}\in\mathbb{Z}^m$.

(1) 令 $\boldsymbol{R}_{\boldsymbol{u}^*}=\sum_{i=0}^{k}(-1)^{u_i^*}\boldsymbol{R}_i$，$h_{\boldsymbol{u}^*}=\sum_{i=0}^{k}(-1)^{u_i^*}h_i$.

(2) 若 $h_{\boldsymbol{u}}\neq 0\bmod q$，则放弃模拟.

(3) 令 $\boldsymbol{Y}_{\boldsymbol{u}^*}=\boldsymbol{A}_{l+1}\boldsymbol{R}_{\boldsymbol{u}^*}+h_{\boldsymbol{u}^*}\boldsymbol{A}_0$，则$\boldsymbol{Y}_{\boldsymbol{u}^*}=\boldsymbol{A}_{l+1}\boldsymbol{R}_{\boldsymbol{u}^*}$.

(4) 令$\boldsymbol{F}^*=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l^*}\|\boldsymbol{Y}_{\boldsymbol{u}^*}]_{i\in w^*\cup U''}$.

(5) $\boldsymbol{e}^*$ 可以通过验证，则 $\boldsymbol{F}^*\cdot\boldsymbol{e}^*=\boldsymbol{0}\bmod q$.

(6) 令 $\boldsymbol{F}_1^*=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l^*}]_{i\in w^*\cup U''}$.

(7) 令 $\boldsymbol{e}_1^*=(\boldsymbol{e}_1+\boldsymbol{R}_{\boldsymbol{u}^*}\hat{\boldsymbol{e}},\boldsymbol{e}_2,\cdots,\boldsymbol{e}_i,\cdots,\boldsymbol{e}_{l+d-l^*})_{i\in w^*\cup U''}$.

(8) $\boldsymbol{F}_1^*\cdot\boldsymbol{e}_1^*=\boldsymbol{F}^*\cdot\boldsymbol{e}^*=\boldsymbol{0}\bmod q$, 且有

$$\|\boldsymbol{e}_1^*\|\leq\sqrt{d}\|\boldsymbol{e}_1+\boldsymbol{R}_u\hat{\boldsymbol{e}}\|$$
$$\leq\sqrt{d}(1+\sqrt{(k+1)m})\cdot s\cdot\sqrt{(d+1)m}.$$

现在证明 $\boldsymbol{e}_1^*\neq\boldsymbol{0}\bmod q$.

$\boldsymbol{e}^*=(\boldsymbol{e}_1,\cdots,\boldsymbol{e}_i,\cdots,\boldsymbol{e}_{l+d-l^*},\hat{\boldsymbol{e}})_{i\in w^*\cup U''}$ 可以通过验证, 故 $\boldsymbol{e}^*\neq\boldsymbol{0}$. 如果 $\boldsymbol{e}_2=\boldsymbol{e}_3=\cdots=\boldsymbol{e}_{l+d-l^*}=\hat{\boldsymbol{e}}=\boldsymbol{0}$, 则 $\boldsymbol{e}_1\neq\boldsymbol{0}$, 从而 $\boldsymbol{e}_1^*\neq\boldsymbol{0}$. 如果存在 $\{\boldsymbol{e}_i\neq\boldsymbol{e}_1\}_{i\in w^*\cup U''}\neq\boldsymbol{0}$, 则 $\boldsymbol{e}_1^*\neq\boldsymbol{0}$. 如果 $\boldsymbol{e}_2=\boldsymbol{e}_3=\cdots=\boldsymbol{e}_{l+d-l^*}=\boldsymbol{0}$, $\hat{\boldsymbol{e}}\neq\boldsymbol{0}$, 由文献[11]引理 26 知, $\Pr[\boldsymbol{e}_1+\boldsymbol{R}_u\hat{\boldsymbol{e}}\neq\boldsymbol{0}]\geq 2/3$, 从而 $\Pr[\boldsymbol{e}_1^*\neq\boldsymbol{0}]\geq 2/3$.

(9) $\boldsymbol{F}_1^*$ 是 $\boldsymbol{S}$ 的子矩阵, 在 $\boldsymbol{e}_1^*$ 中相应位置插入 l 个 m 维零向量可得向量 $\boldsymbol{e}'\in\mathbb{Z}_q^{(l+d)m}$, 则 $\boldsymbol{S}\cdot\boldsymbol{e}'=\boldsymbol{0}\bmod q$, 且 $0<\|\boldsymbol{e}'\|=\|\boldsymbol{e}_1^*\|\leq\sqrt{d}\cdot(1+\sqrt{(k+1)m})\cdot s\sqrt{(d+1)m}$.

又由文献[11]引理 27 知, 若敌手进行签名询问的次数 $Q\leq q/2$, 上述方案模拟中不存在放弃模拟的概率 $\hat{\varepsilon}$ 满足 $1/2q\leq\hat{\varepsilon}\leq 1/q$.

故若存在 PPT 的伪造者 $\mathcal{A}$ 至多进行 $Q\leq q/2$ 次签名询问, 以概率 ε 成功伪造一个签名, 则 $\mathcal{C}$ 利用 $\mathcal{A}$ 以概率 $\varepsilon'\geq\Pr[\boldsymbol{e}_1^*\neq\boldsymbol{0}]\cdot 1/2q\cdot\varepsilon\geq\varepsilon/3q$ 求得 SIS 问题实例 $\boldsymbol{S}\in\mathbb{Z}_q^{n\times(l+d)m}$, $\beta=\sqrt{d}(1+\sqrt{(k+1)m})\cdot s\sqrt{(d+1)m}$ 的一个解 $\boldsymbol{e}'$. 证毕.

5.3.2 匿名性

定理 6. 上述 HABS 方案满足匿名性.

证明. 挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$ 进行如下游戏,

系统建立. 挑战者 $\mathcal{C}$ 输入安全参数 n, 属性全集 $U=\{1,2,\cdots,l\}$, 默认属性集 $U'=\{l+1,\cdots,l+d\}$, 运行 Setup 算法生成公开参数 PP 和主私钥 MSK, 即

$$PP=(\{\boldsymbol{A}_i\}_{i\in U\cup U'},\{\boldsymbol{Y}_i\}_{i=0,1,\cdots,k},U,U'),$$
$$MSK=(\{\boldsymbol{T}_{\boldsymbol{A}_i}\}_{i\in U\cup U'}).$$

并将 PP 和 MSK 发送给敌手 $\mathcal{A}$.

$\mathcal{A}$ 可以利用 MSK 生成对应于任意属性集的私钥和对任意消息进行签名.

挑战阶段. $\mathcal{A}$ 选取挑战消息 $\boldsymbol{u}^*$, 两个不同属性集 $w_0,w_1\subset U$, 签名策略 $w^*\subset w'$, $w'=w_0\cap w_1$, 可简记 $w^*=\{1,\cdots,l^*\}$. $\mathcal{C}$ 利用 MSK 分别生成对应于 w_0,w_1 的私钥 SK_{w_0},SK_{w_1}. $\mathcal{C}$ 选取默认属性子集 U'', 可简记 $U''=\{l+1,\cdots,l+d-l^*\}$. $\mathcal{C}$ 随机选取 $b\in\{0,1\}$, 利用 SK_{w_b}, 运行 Sign 算法获得签名 $\boldsymbol{e}_b^*$, 并返回给 $\mathcal{A}$.

现在对签名阶段进行分析.

令矩阵 $\boldsymbol{F}'''=[\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_i\|\cdots\|\boldsymbol{A}_{l+d-l^*}\|\boldsymbol{Y}_{\boldsymbol{u}^*}]_{i\in w^*\cup U''}$, 签名私钥 $SK_{w_b}=\mathrm{KeyGen}(PP,MSK,w_b)$, 最终生成签名 $\boldsymbol{e}_b^*=\mathrm{Sign}(PP,SK_{w_b},w^*,\boldsymbol{u}^*)$. 由于 $\boldsymbol{e}_0^*,\boldsymbol{e}_1^*\in\mathbb{Z}_q^{(d+1)m}$ 的分布统计接近 $D_{\Lambda_q^\perp(\boldsymbol{F}'''),s}$, 故 $\boldsymbol{e}_0^*,\boldsymbol{e}_1^*$ 的分布统计不可区分, 且 $\|\boldsymbol{e}_0^*\|,\|\boldsymbol{e}_1^*\|\leq s\sqrt{(d+1)m}$, 从而敌手 $\mathcal{A}$ 正确猜测 b 的优势是可忽略的,

综上可得, 上述 HABS 方案满足匿名性要求.

证毕.

5.4 效率分析

该属性签名方案与标准模型下支持 And 门签名策略的属性签名方案[13]和支持门限签名策略的属性基签名方案[14]一样, 仅仅使用了小整数上的矩阵-向量的模乘运算、高斯抽样算法以及基扩展算法. 将本方案与文献[13-14]进行比较, 结果如表 2 所示.

表 2 标准模型下不同方案的效率对比

	文献[13]	文献[14]	本文方案
公钥尺寸	$\tilde{O}((l+k)n^2)$	$\tilde{O}((l+k)n^2)$	$\tilde{O}((l+d+k)n^2)$
私钥尺寸	$\tilde{O}(n^2)$	$\tilde{O}(ln^2)$	$\tilde{O}((l+d)n^2)$
签名尺寸	$\tilde{O}((l+k)n)$	$\tilde{O}((l+k)n)$	$\tilde{O}(dn)$
签名的计算复杂度	$\tilde{O}(n^2)$	$\tilde{O}(n^2)$	$\tilde{O}(n^2)$
验证的计算复杂度	$O(n^2)$	$O(n^2)$	$O(n^2)$
抗适应性选择消息攻击	否	否	是
支持属性任意子集签名	否	否	是

文献[13-14]的公钥尺寸中都隐含着一个常数因子 2, 文献[14]的私钥尺寸中隐含着常数因子 2. 由此比较可得, 本文的属性签名方案的公钥尺寸和签名尺寸较文献[13-14]占用更少的存储空间, 并且获得了更强的安全性, 即抗适应性选择消息攻击不可伪造的. 特别地, 本方案支持签名者灵活地利用其属性的任意子集来签署消息.

6 结束语

隐藏的属性签名可使得签名者利用其属性的任意子集来签署消息, 同时验证者可以有效地判定该消息的确是由拥有某些属性的签名者签署, 而无法确定签名者的具体身份. 本文利用 Boyen 提出的格基剪接技术, 构造出第 1 个随机预言机模型下格上无匿名性撤销的隐藏的属性签名方案, 同时利用格

混合和陷门消失的完全安全的格基短签名方案，本文给出了标准模型下格上无匿名性撤销的隐藏的属性签名方案.本文丰富了格上属性签名方案的研究，并基于格上 SIS 困难问题严格证明了两个构造是抵抗选择属性和适应性选择消息攻击存在性不可伪造的，从而保证了在量子环境下利用生物学特征构造实用性密码系统的安全性.

致　谢　感谢各位评审专家和编辑部老师为本文提出的宝贵意见和建议！

参　考　文　献

[1] Maji H K, Prabhakaran M, Rosulek M. Attribute-based signature: Achieving attribute privacy and collusion-resistance //Proceedings of the Cryptographers' Track at the RSA Conference 2011. San Francisco, USA, 2011: 376-392

[2] Shamir A. Identity based cryptosystems and signature schemes//Proceedings of the 4th Annual International Cryptology Conference. Santa Barbara, USA, 1984: 47-53

[3] Chaum D, Heyst E V. Group signature//Proceedings of the 11th Annual International Cryptology Conference. Santa Barbara, USA, 1991: 257-265

[4] Rivest R L, Shamir A, Tauman Y. How to leak a secret//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia, 2001: 552-565

[5] Li J, Kim K. Hidden attribute-based signatures without anonymity revocation. Information Sciences, 2010, 180(9): 1681-1689

[6] Gentry C, Peikert C, Vaikuntanathan V. Trapdoor for hard lattices and new cryptographic constructions//Proceedings of the 40th ACM Symposium on Theory of Computing. New York, USA, 2008: 197-206

[7] Alwen J, Peikert C. Generating shorter bases for hard random lattices. International Theory of Computing Systems, 2011, 48(3): 535-553

[8] Cash D, Hofheinz D, Kilte E, et al. Bonsai trees, or how to delegate a lattice basis//Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Riviera, French, 2010: 523-552

[9] Agrawal S, Boneh D, Boyen X. Efficient lattice (H)IBE in the standard model//Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Riviera, French, 2010: 553-572

[10] Gordon S D, Katzl J, Vaikuntanathan V. A group signature scheme from lattice assumptions//Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore, 2010: 395-412

[11] Boyen X. Lattice mixing and vanishing trapdoors: A framework for fully secure short signature and more//Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography. Paris, France, 2010: 499-517

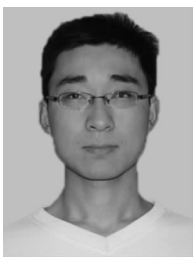
[12] Agrawal S, Boyen X, Vaikunthanathan V, et al. Functional encryption for threshold functions (or fuzzy IBE) from lattices//Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography. Darmstadt, Germany, 2012: 280-297

[13] Miao X, Chen K, Long Y, et al. Attribute-based signature on lattices. Journal of Shanghai Jiaotong University (Science), 2014, 19(4): 406-411

[14] Wang Q, Chen S. Attribute-based signature for threshold predicates from lattices. Security and Communication Networks, 2015, 8(5): 811-821

[15] Wang Q, Chen S, Ge A. A new lattice-based threshold attribute-based signature scheme//Proceedings of the 11th International Conference. Beijing, China, 2015: 406-420

[16] Boyen X. Attribute-based functional encryption on lattices//Proceedings of the 10th Theory of Cryptography Conference. Tokyo, Japan, 2013: 122-142



ZHANG Yan-Hua, born in 1989, Ph. D., lecturer. His main research interests include public key cryptography based on lattice and provable security.

HU Yu-Pu, born in 1955, professor, Ph. D. supervisor. His main research interests include multilinear map, public key cryptography.

CHEN Jiang-Shan, born in 1981, Ph. D. candidate. His research interests include multilinear map and obfuscation.

Background

Attribute-based cryptography offers a powerful alternative for fine-grained access control with respect to security policies. As for hidden attribute-based signature, each user receives from a master entity a secret key which depends on the attributes that he possesses. A signer can sign any message with any subset of his attributes. Then everybody can convince that the message is indeed signed by the signer who owns certain attributes, while cannot determine the specific identity of the real signer.

In recent years, lattice-based cryptography has attracted significant interest, due to several potential benefits: asymptotic efficiency, worst-case hardness assumption and security against quantum attacks. To design powerful and efficient lattice-based cryptographic constructions is interesting and challenging.

Inspired by the basis-splicing technique due to Boyen, and based on the small integer solution (SIS) problem, we construct the first HABS without anonymity revocation from lattices in random oracle model and prove it is existentially unforgeable against selective-attribute and adaptive chosen message attacks (EUF-sA-CMA). Further, using the fully secure short signature with lattice mixing and vanishing trapdoors, another scheme in the standard model is also constructed.

This research is supported by the National Natural Science Foundation of China No. 61472309. It aims at making a further exploration for various applications of lattice cryptography, and designing more secure and efficient lattice-based cryptographic schemes. This research is also supported by China Scholarship Council Postgraduate Scholarship Program, which sponsors Ph. D. candidates to study abroad.