Computer Science and Application 计算机科学与应用, 2025, 15(10), 52-66
Published Online October 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.1510250

Hans汉斯

层次型无证书全同态签名方案

李明祥*，李润亚

河北金融学院金融研究所，河北 保定

收稿日期：2025年9月7日；录用日期：2025年10月8日；发布日期：2025年10月15日

摘　要

公钥密码体制具体可分为基于PKI的公钥密码体制、基于身份的公钥密码体制和无证书公钥密码体制。基于PKI的密码体制存在公钥证书管理问题。基于身份的密码体制消除了公钥证书管理问题，但却引入了密钥托管问题。无证书密码体制消除了公钥证书管理问题，同时又避免了密钥托管问题，它是一种具有卓越性能的公钥密码体制。全同态签名体制允许在不知晓签名私钥的情况下对已签名的数据执行任意的计算操作，并同态地导出计算结果的有效签名。全同态签名体制在云计算、物联网等许多领域具有广泛的应用前景。目前，人们已提出了几个基于PKI的全同态签名方案和几个基于身份的全同态签名方案，却尚未提出无证书全同态签名方案。因此，本文首先给出了层次型无证书全同态签名方案的形式化定义和选择性选择身份和固定性选择消息攻击下的存在性不可伪造性(EU-sID-sCMA)的安全模型。其次，设计了一个基于格的层次型无证书全同态签名方案。再次，在标准模型下基于小整数解问题的困难性证明了所设计的方案满足EU-sID-sCMA安全性。最后，给出了所设计的方案的具体参数设置。

关键词

全同态签名，无证书，格，小整数解问题

Leveled Certificateless Fully Homomorphic Signature Scheme

Mingxiang Li*, Runya Li

Financial Research Institute, Hebei Finance University, Baoding Hebei

Received: September 7, 2025; accepted: October 8, 2025; published: October 15, 2025

Abstract

The public key cryptosystem can be divided into the PKI-based public key cryptosystem, the identity-based public key cryptosystem, and the certificateless public key cryptosystem. The PKI-based cryptosystem has a public key certificate management issue. The identity-based cryptosystem eliminates

*通讯作者。

文章引用: 李明祥, 李润亚. 层次型无证书全同态签名方案[J]. 计算机科学与应用, 2025, 15(10): 52-66.
DOI: 10.12677/csa.2025.1510250

the public key certificate management issue but introduces a key escrow problem. The certificateless cryptosystem eliminates the public key certificate management issue while avoiding the key escrow problem. Therefore, it is a public key cryptosystem with excellent properties. A fully homomorphic signature scheme allows anyone to perform arbitrary computations on signed data without having the private signing key and to derive a valid signature for the result homomorphically. The fully homomorphic signature scheme has significant potential applications in various fields, such as cloud computing and the Internet of Things. So far, several PKI-based and identity-based fully homomorphic signature schemes have been proposed, but no certificateless fully homomorphic signature scheme has been presented. As a result, this paper first gives a formal definition and a security model for existential unforgeability under selective chosen-identity and static chosen-message attacks (EU-sID-sCMA) for a leveled certificateless fully homomorphic signature scheme. Secondly, this paper designs a leveled certificateless fully homomorphic signature scheme from lattices. Thirdly, this paper proves that the proposed scheme satisfies the EU-sID-sCMA security based on the hardness of the small integer solution problem in the standard model. Finally, this paper provides the practical parameter settings of the proposed scheme.

Keywords

Fully Homomorphic Signature, Certificateless, Lattices, Small Integer Solution Problem

1. 引言

公钥密码体制(public key cryptosystem, PKC) [1]不仅具有加密功能，而且具有认证功能。在基于 PKI 的密码体制中，用户的公钥与其身份没有任何联系，他们通过证书机构(certificate authority, CA)发布的公钥证书联系起来。基于 PKI 的密码体制存在公钥证书管理问题。在基于身份的密码体制(identity-based cryptosystem, IBC) [2]中，用户的公钥由其身份派生出来，用户的私钥由私钥生成器(private key generator, PKG)生成。基于身份的密码体制消除了公钥证书管理问题，但引入了密钥托管问题。在无证书密码体制(certificateless cryptosystem, CLC) [3]中，用户的私钥由密钥生成中心(key generating center, KGC)和用户自身共同生成。无证书密码体制不仅消除了公钥证书管理问题，而且还避免了密钥托管问题，它是一种拥有卓越性能的公钥密码体制。目前，人们提出了一个基于格的无证书签名(certificateless signature, CLS)方案[4]。此外，人们还提出了几个基于格的 CLS 方案[5]-[8]。

具有同态性质的公钥密码体制在云计算、物联网和大数据等领域具有广泛的应用价值，它吸引了众多研究人员的目光。全同态加密(fully homomorphic encryption, FHE)允许对加密数据执行任意计算。2013 年，Gentry、Sahai 和 Waters [9]提出了近似特征向量技术，并设计了一个基于格的层次型 FHE 方案。在层次型 FHE 方案中，方案的参数依赖于方案所能计算的电路的深度。利用近似特征向量技术，人们提出了层次型基于身份的全同态加密(identity-based fully homomorphic encryption, IBFHE)方案[10]-[12]，提出了层次型无证书全同态加密(certificateless fully homomorphic encryption, CLFHE)方案[13]。全同态签名(fully homomorphic signature, FHS)允许对签名数据执行任意计算。FHS 的安全要求除不可伪造性之外还包括隐私性[14]。隐私性从弱到强可以分为弱上下文隐藏、强上下文隐藏和完全上下文隐藏。2015 年，Gorbunov、Vaikuntanathan 和 Wichs [15]提出了一个基于格的层次型 FHS 方案，并在标准模型下基于小整数解(small integer solution, SIS)问题的困难性证明了它满足固定性选择消息攻击下的存在性不可伪造性(EU-sCMA)。在

层次型 FHS 方案中，方案的参数依赖于方案所能计算的电路的深度。随后，Boyen、Fan 和 Shi [16]又提出了一个基于格的层次型 FHS 方案，并在标准模型下基于 SIS 问题的困难性证明了它满足适应性选择消息攻击下的存在性不可伪造性(EU-CMA)。Gorbunov 等人的 FHS 方案[15]能提供弱上下文隐藏的隐私性。Boyen 等人的 FHS 方案[16]不能提供任何程度的隐私性，它不适用于许多现实的应用场合。近年来，人们提出了几个层次型基于身份的全同态签名(identity-based fully homomorphic signature, IBFHS)方案[17]-[19]。但迄今为止，人们尚未提出层次型无证书全同态签名(certificateless fully homomorphic signature, CLFHS)方案。

我们可以把 FHS 方案与 CLS 方案结合起来设计 CLFHS 方案。人们提出的 CLS 方案[4]存在安全缺陷，攻击者能够成功伪造任何消息的签名，人们提出其他几个 CLS 方案[5]-[8]在签名时需要对消息进行哈希运算，它们也不适合用来设计 CLFHS 方案。于是，我们在 Gorbunov 等人的 FHS 方案[15]的基础上直接设计了基于格的层次型 CLFHS 方案。我们的主要工作如下：

① 给出了层次型 CLFHS 方案的形式化定义和选择性选择身份和固定性选择消息攻击下的存在性不可伪造性(existential unforgeability under selective chosen-identity and static chosen-message attacks, EU-sID-sCMA)的安全模型。

② 利用 Gorbunov 等人[15]提出的设计技术，构造了一个基于格的层次型 CLFHS 方案。并在标准模型下基于 SIS 问题的困难性证明了所构造的方案满足 EU-sID-sCMA 安全性。

③ 给出了所构造的 CLFHS 方案的具体参数设置，分析了所构造的 CLFHS 方案的有关性能。

2. 预备知识

2.1. 符号约定

首先介绍本文使用的符号，具体如表 1 所示。

Table 1. Notations and their descriptions
表 1. 符号及其说明

符号	说明
λ	安全参数
$\mathbb{Z}$	整数集
$\mathbb{R}$	实数集
$\mathbb{Z}_q$	模 q 剩余类环，且 $\mathbb{Z}_q=(-q/2,q/2]\cap\mathbb{Z}$
$\lvert S\rvert$	有限集合 S 中元素的个数
$[k]$	集合 $\{1,\cdots,k\}$
log	对数，且底为 2
$\mathrm{poly}(\lambda)$	多项式函数
$\mathrm{negl}(\lambda)$	可忽略的函数
$\tilde{O}(g(\lambda))$	$O(g(\lambda)\cdot\log^c\lambda)$，其中 c 为某一固定常数
$\boldsymbol{a}$	向量，默认为列向量形式
$\boldsymbol{A}$	矩阵，可看作其列向量的有序集合
$(\boldsymbol{A}\mid\boldsymbol{B})$	矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的水平连接
$\lVert\boldsymbol{a}\rVert$	向量 $\boldsymbol{a}$ 的欧式范数
$\lVert\boldsymbol{A}\rVert$	矩阵 $\boldsymbol{A}$ 的欧式范数
$\tilde{\boldsymbol{T}}$	矩阵 $\boldsymbol{T}$ 的 Gram-Schmidt 正交化

2.2. 熵与统计距离

定义 1. 对随机变量 $X \leftarrow X$ 和 $Y \leftarrow Y$，它们的统计距离定义为

$$\Delta(X,Y)=\frac{1}{2}\sum_{a\in X\cup Y}\left|\Pr[X=a]-\Pr[Y=a]\right|$$

如果 $\Delta(X,Y)=\mathrm{nelg}(\lambda)$，则称随机变量 X 和 Y 是统计接近的。

定义 2. 随机变量 X 的最小熵定义为 $\mathrm{H}_\infty(X)=-\log\left(\max_x \Pr[X=x]\right)$。$X$ 以 Y 为条件的平均最小熵定义为

$$\mathrm{H}_\infty(X\mid Y)=-\log\left(\mathrm{E}_{y\leftarrow Y}\left[\max_x \Pr[X=x\mid Y=y]\right]\right).$$

给定相关的 Y，敌手猜测 X 的最优概率为 $2^{-\mathrm{H}_\infty(X|Y)}$。

引理 1. [20] 假设 $X \leftarrow \mathcal{X}$ 和 $Y \leftarrow \mathcal{Y}$ 为两个任意的随机变量，那么

$$\mathrm{H}_\infty(X\mid Y)\geq \mathrm{H}_\infty(X)-\log\left(|\mathcal{Y}|\right).$$

2.3. 格

定义 3. 令矩阵 $\boldsymbol{B}=(\boldsymbol{b}_1\mid\cdots\mid\boldsymbol{b}_m)\in\mathbb{R}^{m\times m}$，其列向量 $\boldsymbol{b}_1,\cdots,\boldsymbol{b}_m$ 是一组线性无关向量，由基 $\boldsymbol{B}$ 产生的 m 维格 Λ 定义为

$$\Lambda=\left\{\boldsymbol{y}\in\mathbb{R}^m \text{ s.t. } \exists \boldsymbol{z}\in\mathbb{Z}^m,\ \boldsymbol{y}=\boldsymbol{B}\boldsymbol{z}=\sum_{i\in[m]} z_i\boldsymbol{b}_i\right\}.$$

定义 4. 对素数 q、矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，定义两个 m 维整数格：

$$\Lambda^\perp(\boldsymbol{A})=\left\{\boldsymbol{e}\in\mathbb{Z}^m \text{ s.t. } \boldsymbol{A}\boldsymbol{e}=\boldsymbol{0} \mod q\right\},$$

$$\Lambda_{\boldsymbol{u}}^\perp(\boldsymbol{A})=\left\{\boldsymbol{e}\in\mathbb{Z}^m \text{ s.t. } \boldsymbol{A}\boldsymbol{e}=\boldsymbol{u} \mod q\right\}.$$

可以看出，如果 $\boldsymbol{t}\in\Lambda_{\boldsymbol{u}}^\perp(\boldsymbol{A})$，则 $\Lambda_{\boldsymbol{u}}^\perp(\boldsymbol{A})=\Lambda^\perp(\boldsymbol{A})+\boldsymbol{t}$，因此 $\Lambda_{\boldsymbol{u}}^\perp(\boldsymbol{A})$ 是 $\Lambda^\perp(\boldsymbol{A})$ 的一个陪集。

定义 5. 对任意向量 $\boldsymbol{c}\in\mathbb{R}^m$、实数 $s>0$ 和 m 维格 Λ，Λ 上的离散高斯分布定义为

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

其中 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/s^2\right)$ 是 $\mathbb{R}^m$ 上以 $\boldsymbol{c}$ 和 s 分别为中心和参数的高斯函数。

引理 2. [21] 对任意 m 维格、向量 $\boldsymbol{c}\in\mathbb{R}^m$ 和实数 $0<\epsilon<1$、$s\geq\eta_\epsilon(\Lambda)$，有

$$\Pr_{\boldsymbol{x}\leftarrow D_{\Lambda,s,\boldsymbol{c}}}\left[\|\boldsymbol{x}-\boldsymbol{c}\|>s\sqrt{m}\right]\leq\frac{1+\epsilon}{1-\epsilon}\cdot 2^{-m},$$

其中 $\eta_\varepsilon(\Lambda)$ 是 Λ 的光滑参数，且对 Λ 的任意一组基 $\boldsymbol{B}$，$\eta_\varepsilon(\Lambda)\leq\|\tilde{\boldsymbol{B}}\|\cdot\omega\left(\sqrt{\log m}\right)$。

引理 3. [22] 令 n 和 m 为正整数，q 为素数，并且 $m\geq 2n\log q$。则对任意 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 以及对任意 $\sigma\geq\omega\left(\sqrt{\log m}\right)$，$\boldsymbol{u}=\boldsymbol{A}\boldsymbol{e} \mod q$ 统计接近于 $\mathbb{Z}_q^n$ 上的均匀分布，其中 $\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,\sigma}$。

引理 4. [23] 令 $\delta>0$ 为任一固定常数，存在一个概率多项式时间算法 $\mathrm{GenBasis}\left(1^n,1^m,q\right)$，它输入正整数 n、$q\geq 2$ 和 $m\geq(5+3\delta)\cdot n\log q$，输出一个矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\Lambda^\perp(\boldsymbol{A})$ 的一组基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$，满足 $\boldsymbol{A}$ 统计接近于 $\mathbb{Z}_q^{n\times m}$ 上的均匀分布以及 $\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\|\leq\tilde{L}=O\left(\sqrt{n\log q}\right)$。

引理 5. [22] 给定 $q\geq 2$ 和 $m\geq 2n\log q$，存在一个概率多项式时间算法 $\mathrm{SamplePre}\left(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},s,\boldsymbol{u}\right)$，它输入矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$、格 $\Lambda^\perp(\boldsymbol{A})$ 的一组基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$、高斯参数 $s\geq\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\|\cdot\omega\left(\sqrt{\log m}\right)$ 和向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，从统计接近于

$D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}),s}$ 的分布输出一个向量 $\boldsymbol{e}\in\mathbb{Z}^m$。

引理 6. [24] 给定 $q\geq 2$ 和 $m\geq 2n\log q$，存在一个固定的可计算的矩阵 $\boldsymbol{G}\in\mathbb{Z}_q^{n\times m}$ 和一个确定性的多项式时间算法 $\boldsymbol{G}^{-1}$，该算法输入矩阵 $\boldsymbol{V}\in\mathbb{Z}_q^{n\times k}$，其中 $k\geq 1$，输出一个比特矩阵 $\boldsymbol{G}^{-1}(\boldsymbol{V})\in\{0,1\}^{m\times k}$，满足 $\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{V})=\boldsymbol{V}$。

定义 6. 对于矩阵 $\boldsymbol{R}\in\mathbb{Z}^{m\times m}$，若 $\boldsymbol{R} \bmod q$ 作为 $\mathbb{Z}_q^{m\times m}$ 上的矩阵是可逆的，就称 $\boldsymbol{R}$ 为 $\mathbb{Z}_q$ 可逆的。我们定义 $\mathcal{D}^{m\times m}$ 为高斯分布 $\left(D_{\mathbb{Z}^m,s}\right)^m$，其中 $s\geq\tilde{L}\cdot\omega\left(\sqrt{\log m}\right)$，并且抽样矩阵为 $\mathbb{Z}_q$ 可逆的。

引理 7. [25] 给定 $q\geq 2$ 和 $m\geq 2n\log q$，存在一个概率多项式时间算法 $\mathrm{BasisDel}(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{R},s)$，它输入矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$、格 $\Lambda^{\perp}(\boldsymbol{A})$ 的一组基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$、从分布 $\mathcal{D}^{m\times m}$ 抽取的 $\mathbb{Z}_q$ 可逆矩阵 $\boldsymbol{R}\in\mathbb{Z}^{m\times m}$ 以及高斯参数 $s\geq\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\right\|\cdot\tilde{L}\cdot\sqrt{m}\cdot\omega\left(\sqrt{\log m}\right)^4$，输出格 $\Lambda^{\perp}(\boldsymbol{B})$ 的一组基 $\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}^{m\times m}$，其中 $\boldsymbol{B}=\boldsymbol{A}\boldsymbol{R}^{-1} \bmod q$，并且 $\boldsymbol{T}_{\boldsymbol{B}}$ 满足 $\left\|\boldsymbol{T}_{\boldsymbol{B}}\right\|\leq s\sqrt{m}$。

引理 8. [25] 给定 $q\geq 2$ 和 $m\geq 2n\log q$，存在一个概率多项式时间算法 $\mathrm{SampleRwithBasis}(\boldsymbol{A})$，它输入矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，从统计接近于 $\mathcal{D}^{m\times m}$ 的分布输出一个矩阵 $\boldsymbol{R}\in\mathbb{Z}^{m\times m}$，它还输出格 $\Lambda^{\perp}(\boldsymbol{B})$ 的一组基 $\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}^{m\times m}$，满足 $\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{B}}}\right\|\leq\tilde{L}=O\left(\sqrt{n\log q}\right)$，其中 $\boldsymbol{B}=\boldsymbol{A}\boldsymbol{R}^{-1} \bmod q$。

2.4. SIS 问题

定义 7. 小整数解(small integer solution, SIS)问题如下：给定整数 q、矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和实数 β，寻找一个非零向量 $\boldsymbol{e}\in\mathbb{Z}^m$，满足 $\boldsymbol{A}\boldsymbol{e}=\boldsymbol{0} \bmod q$ 和 $\|\boldsymbol{e}\|\leq\beta$。

对于函数 $q(n)$、$m(n)$ 和 $\beta(n)$，$\mathrm{SIS}_{q,m,\beta}$ 表示实例 $\left(q(n),\boldsymbol{A},\beta(n)\right)$ 的集合，其中 $\boldsymbol{A}\in\mathbb{Z}_{q(n)}^{n\times m(n)}$ 是均匀随机的。

引理 9. [21] [22] 对任意多项式界的 $m=\mathrm{poly}(n)$ 和 $\beta=\mathrm{poly}(n)$ 以及对任意素数 $q\geq\beta\cdot\omega\left(\sqrt{n\log n}\right)$，平均情况下的 $\mathrm{SIS}_{q,m,\beta}$ 问题与最差情况下的近似最短独立向量问题(shortest independent vector problem, SIVP)一样困难，其中近似因子 $\gamma=\beta\cdot\tilde{O}\left(\sqrt{n}\right)$。

3. 形式化定义与安全模型

3.1. 形式化定义

一个层次型 CLFHS 方案由系统设置 Setup、部分私钥提取 Extract、用户密钥设置 KeyGen、签名 Sign、同态运算 Eval 和验证 Verify 六个多项式时间算法组成。具体如下：

① $(pp,msk)\leftarrow\mathrm{Setup}\left(1^{\lambda},1^{d},1^{N}\right)$：输入安全参数 λ、电路的最大深度 d 和数据集的最大尺寸 N，输出公开参数 $param$ 和主密钥 msk。$param$ 包含消息空间 $\mathcal{M}$ 的描述。该算法由密钥生成中心 KGC 执行。

② $psk_{id}\leftarrow\mathrm{Extract}(param,msk,id)$：输入公开参数 $param$、主密钥 msk 和身份 id，输出部分私钥 psk_{id}。该算法由密钥生成中心 KGC 执行。

③ $(x_{id},pk_{id})\leftarrow\mathrm{KeyGen}(param,id)$：输入公开参数 $param$ 和身份 id，输出秘密值 x_{id} 和公钥 pk_{id}。

④ $(\sigma_1,\cdots,\sigma_N)\leftarrow\mathrm{Sign}(param,id,pk_{id},psk_{id},x_{id},\mu_1,\cdots,\mu_N)$：输入公开参数 $param$、身份 id、公钥 pk_{id}、部分私钥 psk_{id}、秘密值 x_{id} 和消息序列 $\mu_1,\cdots,\mu_N\in\mathcal{M}$，输出签名序列 $\sigma_1,\cdots,\sigma_N$。

⑤ $\sigma_f\leftarrow\mathrm{Eval}\left(param,id,f,\{(\mu_i,\sigma_i)\}_{i\in[N]}\right)$：输入公开参数 $param$、身份 id、电路 $f:\mathcal{M}^N\rightarrow\mathcal{M}$ 和消息－签名对的集合 $\{(\mu_i,\sigma_i)\}_{i\in[N]}$，输出签名 σ_f。

⑥ accept/reject $\leftarrow \mathrm{Verify}\left(param, id, pk_{id}, f, \mu_f, \sigma_f\right)$：输入公开参数 $param$、身份 id、公钥 pk_{id}、电路 $f:\mathcal{M}^N \to \mathcal{M}$、消息 $\mu_f \in \mathcal{M}$ 和签名 σ_f，若 σ_f 是 id 和 pk_{id} 对 μ_f 的有效签名，则输出 accept，否则输出 reject。

若对任意的身份 id、消息序列 $\mu_1,\cdots,\mu_N \in \mathcal{M}$ 和电路 $f:\mathcal{M}^N \to \mathcal{M}$，其中电路 f 的深度 $\mathrm{depth}(f) \le d$，给定

$$\begin{aligned}
&\left(param, msk\right) \leftarrow \mathrm{Setup}\left(1^{\lambda}, 1^{d}, 1^{N}\right)\\
&psk_{id} \leftarrow \mathrm{Extract}\left(param, msk, id\right)\\
&\left(x_{id}, pk_{id}\right) \leftarrow \mathrm{KeyGen}\left(param, id\right)\\
&\left(\sigma_1,\cdots,\sigma_N\right) \leftarrow \mathrm{Sign}\left(param, id, pk_{id}, psk_{id}, x_{id}, \mu_1,\cdots,\mu_N\right)
\end{aligned}$$

有

$$\mathrm{Verify}\left(param, id, pk_{id}, f, \mu_f, \sigma_f\right) = \mathrm{accept}$$

其中

$$\begin{aligned}
&\mu_f = f\left(\mu_1,\cdots,\mu_N\right)\\
&\sigma_f = \mathrm{Eval}\left(param, id, f, \left\{\left(\mu_i, \sigma_i\right)\right\}_{i\in[N]}\right)
\end{aligned}$$

则称这个层次型 CLFHS 方案是正确的。

3.2. 安全模型

层次型 CLFHS 方案的攻击者包括第 1 类攻击者 $\mathcal{A}_{\mathrm{I}}$ 和第 2 类攻击者 $\mathcal{A}_{\mathrm{II}}$。$\mathcal{A}_{\mathrm{I}}$ 模拟外部攻击者，它不知道系统主密钥，但可以任意替换用户的公钥；$\mathcal{A}_{\mathrm{II}}$ 模拟诚实但好奇的密钥生成中心 KGC，它知道系统主密钥，但不能替换目标用户的公钥。层次型 CLFHS 方案在选择性选择身份和固定性选择消息攻击下的存在性不可伪造性(existential unforgeability under selective chosen-identity and static chosen-message attacks, EU-sID-sCMA)可由攻击者 $\mathcal{A}_{\mathrm{I}}$ 或 $\mathcal{A}_{\mathrm{II}}$ 与挑战者之间的两个游戏刻画。具体如下：

游戏 1 (适用于攻击者 $\mathcal{A}_{\mathrm{I}}$)：

初始化：$\mathcal{A}_{\mathrm{I}}$ 输出身份 id^*、公钥 pk'_{id^*} 和消息序列 $\mu_1,\cdots,\mu_N \in \mathcal{M}$。这里，$pk'_{id^*}$ 是 $\mathcal{A}_{\mathrm{I}}$ 替换的用户 id^* 的公钥。

设置：挑战者执行 $\left(param, msk\right) \leftarrow \mathrm{Setup}\left(1^{\lambda}, 1^{d}, 1^{N}\right)$，把 $param$ 发送给 $\mathcal{A}_{\mathrm{I}}$。

询问：$\mathcal{A}_{\mathrm{I}}$ 可以适应性地向挑战者发出以下几种询问：

部分私钥询问：$\mathcal{A}_{\mathrm{I}}$ 提交身份 id，其中 $id \ne id^*$，挑战者执行 $psk_{id} \leftarrow \mathrm{Extract}\left(param, msk, id\right)$，把 psk_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$。

秘密值询问：挑战者维护一个元组列表 $L = \left\{\left(id, x_{id}, pk_{id}\right)\right\}$。$\mathcal{A}_{\mathrm{I}}$ 提交身份 id。挑战者首先在表 L 中查找元组 $\left(id, x_{id}, pk_{id}\right)$。若找到该元组，把 x_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$；若未找到，执行 $\left(x_{id}, pk_{id}\right) \leftarrow \mathrm{KeyGen}\left(param, id\right)$，把 x_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$，并把 $\left(id, x_{id}, pk_{id}\right)$ 添加到表 L 中。

公钥询问：$\mathcal{A}_{\mathrm{I}}$ 提交身份 id。挑战者首先在表 L 中查找元组 $\left(id, x_{id}, pk_{id}\right)$。若找到该元组，把 pk_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$；若未找到，执行 $\left(x_{id}, pk_{id}\right) \leftarrow \mathrm{KeyGen}\left(param, id\right)$，把 pk_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$，并把 $\left(id, x_{id}, pk_{id}\right)$ 添加到表 L 中。

签名询问：挑战者按公钥 pk'_{id^*} 对应的秘密值 x'_{id^*} 产生签名序列 $\sigma_1,\cdots,\sigma_N$，把 $\sigma_1,\cdots,\sigma_N$ 发送给 $\mathcal{A}_{\mathrm{I}}$。

伪造：最后，$\mathcal{A}_{\mathrm{I}}$ 输出电路 $f^*:\mathcal{M}^N \to \mathcal{M}$、消息 μ^* 和签名 σ^*。如果满足以下条件，称 $\mathcal{A}_{\mathrm{I}}$ 赢得游戏 1。

① $\mu^* \ne \mu_{f^*}$，其中 $\mu_{f^*} = f^*\left(\mu_1,\cdots,\mu_N\right)$；

② $\mathrm{Verify}\left(param, id^*, pk'_{id^*}, f^*, \mu^*, \sigma^*\right) = \mathrm{accept}$。

$\mathcal{A}_{\mathrm{I}}$攻击一个层次型 CLFHS 方案的优势定义为 $\mathrm{Adv}_{\mathrm{CLFHS}}^{\text{EU-sID-sCMS}}\left(\mathcal{A}_{\mathrm{I}}\right) = \Pr\left[\mathcal{A}_{\mathrm{I}} \text{ wins the game 1}\right]$。

定义 8. 如果对任意多项式时间攻击者 $\mathcal{A}_{\mathrm{I}}$，$\mathrm{Adv}_{\mathrm{CLFHS}}^{\text{EU-sID-sCMS}}\left(\mathcal{A}_{\mathrm{I}}\right) = \mathrm{negl}\left(\lambda\right)$，我们就称这个层次型 CLFHS 方案对第 1 类攻击者是 EU-sID-sCMA 安全的。

游戏 2 (适用于攻击者 $\mathcal{A}_{\mathrm{II}}$)：

初始化：$\mathcal{A}_{\mathrm{II}}$输出身份 id^* 和消息序列 $\mu_1, \cdots, \mu_N \in \mathcal{M}$。

设置：挑战者执行 $\left(param, msk\right) \leftarrow \mathrm{Setup}\left(1^{\lambda}, 1^{d}, 1^{N}\right)$，把 $param$ 和 msk 发送给 $\mathcal{A}_{\mathrm{II}}$。

询问：$\mathcal{A}_{\mathrm{II}}$可以适应性地向挑战者发出以下几种询问：

秘密值询问：挑战者维护一个元组列表 $L = \left\{\left(id, x_{id}, pk_{id}\right)\right\}$。$\mathcal{A}_{\mathrm{II}}$提交身份 id，其中 $id \neq id^*$。挑战者首先在表 L 中查找元组 $\left(id, x_{id}, pk_{id}\right)$。若找到该元组，把 x_{id} 发送给 $\mathcal{A}_{\mathrm{II}}$；若未找到，执行 $\left(x_{id}, pk_{id}\right) \leftarrow \mathrm{KeyGen}\left(param, id\right)$，把 x_{id} 发送给 $\mathcal{A}_{\mathrm{II}}$，并把 $\left(id, x_{id}, pk_{id}\right)$ 添加到表 L 中。

公钥询问：$\mathcal{A}_{\mathrm{II}}$提交身份 id。挑战者首先在表 L 中查找元组 $\left(id, x_{id}, pk_{id}\right)$。若找到该元组，把 pk_{id} 发送给 $\mathcal{A}_{\mathrm{II}}$；若未找到，执行 $\left(x_{id}, pk_{id}\right) \leftarrow \mathrm{KeyGen}\left(param, id\right)$，把 pk_{id} 发送给 $\mathcal{A}_{\mathrm{II}}$，并把 $\left(id, x_{id}, pk_{id}\right)$ 添加到表 L 中。

签名询问：假定 $\mathcal{A}_{\mathrm{II}}$ 已询问过 id^* 的公钥。挑战者执行 $\left(\sigma_1, \cdots, \sigma_N\right) \leftarrow \mathrm{Sign}\left(param, id^*, pk_{id^*}, psk_{id^*}, x_{id^*}, \mu_1, \cdots, \mu_N\right)$，把产生的签名序列 $\sigma_1, \cdots, \sigma_N$ 发送给 $\mathcal{A}_{\mathrm{II}}$。

伪造：最后，$\mathcal{A}_{\mathrm{II}}$输出电路 $f^*: \mathcal{M}^N \to \mathcal{M}$、消息 μ^* 和签名 σ^*。如果满足以下条件，称 $\mathcal{A}_{\mathrm{II}}$ 赢得游戏 2。

① $\mu^* \neq \mu_{f^*}$，其中 $\mu_{f^*} = f^*\left(\mu_1, \cdots, \mu_N\right)$；

② $\mathrm{Verify}\left(param, id^*, pk_{id^*}, f^*, \mu^*, \sigma^*\right) = \mathrm{accept}$，其中 pk_{id^*} 为表 L 中用户 id^* 的公钥。

$\mathcal{A}_{\mathrm{II}}$攻击一个层次型 CLFHS 方案的优势定义为 $\mathrm{Adv}_{\mathrm{CLFHS}}^{\text{EU-sID-sCMS}}\left(\mathcal{A}_{\mathrm{II}}\right) = \Pr\left[\mathcal{A}_{\mathrm{II}} \text{ wins the game 2}\right]$。

定义 9. 如果对任意多项式时间攻击者 $\mathcal{A}_{\mathrm{II}}$，$\mathrm{Adv}_{\mathrm{CLFHS}}^{\text{EU-sID-sCMS}}\left(\mathcal{A}_{\mathrm{II}}\right) = \mathrm{negl}\left(\lambda\right)$，我们就称这个层次型 CLFHS 方案对第 2 类攻击者是 EU-sID-sCMA 安全的。

4. 构造与安全性证明

4.1. 构造

在人们提出的 CLS 方案[4]中，用户的公钥为 $\boldsymbol{A} = \left(\boldsymbol{A}_1 \mid \boldsymbol{A}_2\right) \in \mathbb{Z}_q^{n \times 4m}$，私钥为 $\boldsymbol{T}_{\boldsymbol{A}} = \begin{pmatrix} \boldsymbol{T}_{\boldsymbol{A}_1} & \\ & \boldsymbol{T}_{\boldsymbol{A}_2} \end{pmatrix} \in \mathbb{Z}^{4m \times 4m}$，公钥的这种形式使得第 1 类攻击者 $\mathcal{A}_{\mathrm{I}}$ 和第 2 类攻击者 $\mathcal{A}_{\mathrm{II}}$ 都能够生成用户的私钥 $\boldsymbol{T}'$，从而成功伪造任何消息的签名。若把用户的公钥设置为 $\boldsymbol{A} = \begin{pmatrix} \boldsymbol{A}_1 & \\ & \boldsymbol{A}_2 \end{pmatrix} \in \mathbb{Z}_q^{2n \times 4m}$，$\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$ 就无法生成用户的私钥 $\boldsymbol{T}'$ 了。下面我们以 Gorbunov 等人[15]的 FHS 方案为基础，构建一个基于格的层次型 CLFHS 方案，其中我们把用户的公钥设置为 $\boldsymbol{F} = \begin{pmatrix} \boldsymbol{B} & \\ & \boldsymbol{C} \end{pmatrix} \in \mathbb{Z}_q^{2n \times 2m}$，私钥设置为 $\boldsymbol{T}_{\boldsymbol{F}} = \begin{pmatrix} \boldsymbol{T}_{\boldsymbol{B}} & \\ & \boldsymbol{T}_{\boldsymbol{C}} \end{pmatrix} \in \mathbb{Z}^{2m \times 2m}$。

$\left(pp, msk\right) \leftarrow \mathrm{Setup}\left(1^{\lambda}, 1^{d}, 1^{N}\right)$：给定安全参数 λ、电路的最大深度 d 和数据集的最大尺寸 N，执行：

① 设置 n、$q \geq 2$ 和 $m = O\left(n \log q\right)$，设置高斯参数 s_1 和 s_2。

② 设置消息空间 $\mathcal{M} = \left\{0,1\right\}$，设置身份空间 $\mathcal{ID} = \left\{0,1\right\}^{\ell}$，其中 $\ell \geq 1$。

③ 调用 $\mathrm{GenBasis}\left(1^n, 1^m, q\right)$ 产生一个矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ 和格 $\Lambda^{\perp}\left(\boldsymbol{A}\right)$ 的一组基 $\boldsymbol{T}_{\boldsymbol{A}} \in \mathbb{Z}^{m \times m}$，满足 $\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\right\| \leq \tilde{L} = O\left(\sqrt{n \log q}\right)$。

④ 选取 2ℓ 个矩阵 $\boldsymbol{R}_{i,0},\boldsymbol{R}_{i,1}\leftarrow\mathcal{D}^{m\times m}$，其中 $i\in[\ell]$。

⑤ 选取 N 个矩阵 $\boldsymbol{V}_i\in\mathbb{Z}_q^{2n\times 2m}$，其中 $i\in[N]$。

⑥ 输出公开参数 $param=\left(\boldsymbol{A},\left\{\boldsymbol{R}_{i,0},\boldsymbol{R}_{i,1}\right\}_{i\in[\ell]},\left\{\boldsymbol{V}_i\right\}_{i\in[N]}\right)$ 和主密钥 $msk=\boldsymbol{T}_{\boldsymbol{A}}$。

$psk_{id}\leftarrow\mathrm{Extract}\left(param,msk,id\right)$：给定公开参数 $param$、主密钥 $msk=\boldsymbol{T}_{\boldsymbol{A}}$ 和身份 $id\in\{0,1\}^{\ell}$，执行：

① 计算 $\boldsymbol{R}=\boldsymbol{R}_{\ell,id_\ell}\cdots\boldsymbol{R}_{1,id_1}\in\mathbb{Z}^{m\times m}$。

② 调用 $\mathrm{BasisDel}\left(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{R},s_1\right)$ 产生格 $\Lambda^{\perp}\left(\boldsymbol{B}\right)$ 的一组基 $\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}^{m\times m}$，其中 $\boldsymbol{B}=\boldsymbol{A}\boldsymbol{R}^{-1}\in\mathbb{Z}_q^{n\times m}$。

③ 输出部分私钥 $psk_{id}=\boldsymbol{T}_{\boldsymbol{B}}$。

$\left(x_{id},pk_{id}\right)\leftarrow\mathrm{KeyGen}\left(param,id\right)$：给定公开参数 $param$ 和身份 $id\in\{0,1\}^{\ell}$，执行：

① 调用 $\mathrm{GenBasis}\left(1^n,1^m,q\right)$ 产生一个矩阵 $\boldsymbol{C}\in\mathbb{Z}_q^{n\times m}$ 和格 $\Lambda^{\perp}\left(\boldsymbol{C}\right)$ 的一组基 $\boldsymbol{T}_{\boldsymbol{C}}\in\mathbb{Z}^{m\times m}$，满足 $\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{C}}}\right\|\le\tilde{L}=O\left(\sqrt{n\log q}\right)$。

② 输出秘密值 $x_{id}=\boldsymbol{T}_{\boldsymbol{C}}$ 和公钥 $pk_{id}=\boldsymbol{C}$。

$\left(\sigma_1,\cdots,\sigma_N\right)\leftarrow\mathrm{Sign}\left(param,id,pk_{id},psk_{id},x_{id},\mu_1,\cdots,\mu_N\right)$：给定公开参数 $param$、身份 $id\in\{0,1\}^{\ell}$、公钥 $pk_{id}=\boldsymbol{C}$、部分私钥 $psk_{id}=\boldsymbol{T}_{\boldsymbol{B}}$、秘密值 $x_{id}=\boldsymbol{T}_{\boldsymbol{C}}$ 和消息集合 $\{\mu_i\in\mathcal{M}\}_{i\in[N]}$，执行：

① 计算 $\boldsymbol{R}=\boldsymbol{R}_{\ell,id_\ell}\cdots\boldsymbol{R}_{1,id_1}\in\mathbb{Z}^{m\times m}$，计算 $\boldsymbol{B}=\boldsymbol{A}\boldsymbol{R}^{-1}\in\mathbb{Z}^{n\times m}$。

② 令 $\boldsymbol{F}=\begin{pmatrix}\boldsymbol{B}&\\&\boldsymbol{C}\end{pmatrix}\in\mathbb{Z}_q^{2n\times 2m}$。令 $\boldsymbol{T}_{\boldsymbol{F}}=\begin{pmatrix}\boldsymbol{T}_{\boldsymbol{B}}&\\&\boldsymbol{T}_{\boldsymbol{C}}\end{pmatrix}\in\mathbb{Z}^{2m\times 2m}$。不难看出，$\boldsymbol{T}_{\boldsymbol{F}}$ 为格 $\Lambda^{\perp}\left(\boldsymbol{F}\right)$ 的一组基。

③ 对 $i\in[N]$，令 $\boldsymbol{Y}_i=\boldsymbol{V}_i-\mu_i\cdot\boldsymbol{G}\mod q$，调用 $\mathrm{SamplePre}\left(\boldsymbol{F},\boldsymbol{T}_{\boldsymbol{F}},s_2,\boldsymbol{Y}_i\right)$ 产生一个矩阵 $\boldsymbol{U}_i\in\mathbb{Z}^{2m\times 2m}$，其中 $\boldsymbol{G}\in\mathbb{Z}_q^{2n\times 2m}$。

④ 输出签名集合 $\left\{\sigma_i=\boldsymbol{U}_i\right\}_{i\in[N]}$。

$\sigma_f\leftarrow\mathrm{Eval}\left(param,id,f,\left\{\left(\mu_i,\sigma_i\right)\right\}_{i\in[N]}\right)$：给定公开参数 $param$、身份 $id\in\{0,1\}^{\ell}$、电路 $f:\mathcal{M}^N\to\mathcal{M}$ 和消息－签名对的集合 $\left\{\left(\mu_i\in\mathcal{M},\sigma_i=\boldsymbol{U}_i\right)\right\}_{i\in[N]}$，执行：

① 对加法门 $f\left(\mu_1,\mu_2\right)=\mu_1+\mu_2$，定义 $\boldsymbol{U}_f=\boldsymbol{U}_1+\boldsymbol{U}_2$；对乘法门 $f\left(\mu_1,\mu_2\right)=\mu_1\cdot\mu_2$，定义 $\boldsymbol{U}_f=\boldsymbol{U}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)+\mu_1\cdot\boldsymbol{U}_2$。对电路 $f:\mathcal{M}^N\to\mathcal{M}$，通过迭代调用加法门和乘法门计算 $\boldsymbol{U}_f\in\mathbb{Z}^{2m\times 2m}$。

② 输出签名 $\sigma_f=\boldsymbol{U}_f$。

$\mathrm{accept/reject}\leftarrow\mathrm{Verify}\left(param,id,pk_{id},f,\mu_f,\sigma_f\right)$：给定公开参数 $param$、身份 $id\in\{0,1\}^{\ell}$、公钥 $pk_{id}=\boldsymbol{C}$、电路 $f:\mathcal{M}^N\to\mathcal{M}$、消息 $\mu_f\in\mathcal{M}$ 和签名 $\sigma_f=\boldsymbol{U}_f\in\mathbb{Z}^{2m\times 2m}$，执行：

① 对加法门 $f\left(\mu_1,\mu_2\right)=\mu_1+\mu_2$，定义 $\boldsymbol{V}_f=\boldsymbol{V}_1+\boldsymbol{V}_2$；对乘法门 $f\left(\mu_1,\mu_2\right)=\mu_1\cdot\mu_2$，定义 $\boldsymbol{V}_f=\boldsymbol{V}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)$。对电路 $f:\mathcal{M}^N\to\mathcal{M}$，通过迭代调用加法门和乘法门计算 $\boldsymbol{V}_f\in\mathbb{Z}_q^{n\times m}$。

② 计算 $\boldsymbol{F}=\begin{pmatrix}\boldsymbol{A}\boldsymbol{R}^{-1}&\\&\boldsymbol{C}\end{pmatrix}\in\mathbb{Z}_q^{2n\times 2m}$，其中 $\boldsymbol{R}=\boldsymbol{R}_{\ell,id_\ell}\cdots\boldsymbol{R}_{1,id_1}\in\mathbb{Z}^{m\times m}$。

③ 如果满足 $\boldsymbol{F}\boldsymbol{U}_f=\boldsymbol{V}_f-\mu_f\cdot\boldsymbol{G}\mod q$ 和 $\left\|\boldsymbol{U}_f\right\|\le\left(2m+1\right)^{\mathrm{depth}(f)}\cdot s_2\sqrt{2m}$，其中 $\mathrm{depth}\left(f\right)\le d$ 表示电路 f 的深度，则输出 accept，否则输出 reject。

定理 1. 所提出 CLFHS 方案是正确的。

证明. 对于签名 $\boldsymbol{U}_1$ 和 $\boldsymbol{U}_2$，假定 $\boldsymbol{F}\boldsymbol{U}_1=\boldsymbol{V}_1-\mu_1\cdot\boldsymbol{G}\mod q$ 和 $\boldsymbol{F}\boldsymbol{U}_2=\boldsymbol{V}_2-\mu_2\cdot\boldsymbol{G}\mod q$，并且假定 $\left\|\boldsymbol{U}_1\right\|\le\theta$ 和 $\left\|\boldsymbol{U}_2\right\|\le\theta$。则

对加法门 $f\left(\mu_1,\mu_2\right)=\mu_1+\mu_2$，有

$$\boldsymbol{F}\boldsymbol{U}_f=\boldsymbol{F}\left(\boldsymbol{U}_1+\boldsymbol{U}_2\right)=\boldsymbol{F}\boldsymbol{U}_1+\boldsymbol{F}\boldsymbol{U}_2=\boldsymbol{V}_1-\mu_1\cdot\boldsymbol{G}+\boldsymbol{V}_2-\mu_2\cdot\boldsymbol{G}=\left(\boldsymbol{V}_1+\boldsymbol{V}_2\right)-\left(\mu_1+\mu_2\right)\cdot\boldsymbol{G}=\boldsymbol{V}_f-\mu_f\cdot\boldsymbol{G}$$

并且

$$\left\|\boldsymbol{U}_f\right\|=\left\|\boldsymbol{U}_1+\boldsymbol{U}_2\right\|\le\left\|\boldsymbol{U}_1\right\|+\left\|\boldsymbol{U}_2\right\|\le\theta+\theta=2\theta$$

对乘法门 $f\left(\mu_1,\mu_2\right)=\mu_1\cdot\mu_2$，有

$$\begin{aligned}\boldsymbol{F}\boldsymbol{U}_f&=\boldsymbol{F}\left(\boldsymbol{U}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)+\mu_1\cdot\boldsymbol{U}_2\right)\\&=\boldsymbol{F}\boldsymbol{U}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)+\mu_1\cdot\boldsymbol{F}\boldsymbol{U}_2\\&=\left(\boldsymbol{V}_1-\mu_1\cdot\boldsymbol{G}\right)\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)+\mu_1\cdot\left(\boldsymbol{V}_2-\mu_2\cdot\boldsymbol{G}\right)\\&=\boldsymbol{V}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)-\mu_1\cdot\boldsymbol{G}\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)+\mu_1\cdot\boldsymbol{V}_2-\mu_1\mu_2\cdot\boldsymbol{G}\\&=\boldsymbol{V}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)-\mu_1\cdot\boldsymbol{V}_2+\mu_1\cdot\boldsymbol{V}_2-\mu_1\mu_2\cdot\boldsymbol{G}\\&=\boldsymbol{V}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)-\mu_1\mu_2\cdot\boldsymbol{G}\\&=\boldsymbol{V}_f-\mu_f\cdot\boldsymbol{G}\end{aligned}$$

并且

$$\begin{aligned}\left\|\boldsymbol{U}_f\right\|&=\left\|\boldsymbol{U}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)+\mu_1\cdot\boldsymbol{U}_2\right\|\\&\le\left\|\boldsymbol{U}_1\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)\right\|+\mu_1\cdot\left\|\boldsymbol{U}_2\right\|\\&\le\sqrt{2m}\cdot\left\|\boldsymbol{U}_1\right\|\cdot\left\|\boldsymbol{G}^{-1}\left(\boldsymbol{V}_2\right)\right\|+\mu_1\cdot\left\|\boldsymbol{U}_2\right\|\\&\le2m\cdot\left\|\boldsymbol{U}_1\right\|+\mu_1\cdot\left\|\boldsymbol{U}_2\right\|\\&\le\left(2m+1\right)\cdot\theta\end{aligned}$$

对于 Sign 算法产生的签名 $\boldsymbol{U}_i$，有 $\boldsymbol{F}\boldsymbol{U}_i=\boldsymbol{V}_i-\mu_i\cdot\boldsymbol{G}\ \bmod q$，并且 $\left\|\boldsymbol{U}_i\right\|\le s_2\cdot\sqrt{2m}$。所以对于 Eval 算法产生的签名 $\boldsymbol{U}_f$，它是通过迭代调用加法门和乘法门得到的，于是有 $\boldsymbol{F}\boldsymbol{U}_f=\boldsymbol{V}_f-f\left(\mu_1,\cdots,\mu_N\right)\cdot\boldsymbol{G}\ \bmod q$，并且 $\left\|\boldsymbol{U}_f\right\|\le\left(2m+1\right)^{\mathrm{depth}(f)}\cdot s_2\cdot\sqrt{2m}$，其中 $\mathrm{depth}\left(f\right)\le d$ 表示电路 f 的深度。

4.2. 安全性证明

我们在标准模型下证明所提出的 CLFHS 方案满足 EU-sID-sCMA 安全性。

定理 2. 如果存在一个多项式时间攻击者 $\mathcal{A}_{\mathrm{I}}$ 在游戏 1 中以优势 ε 攻击所提出的 CLFHS 方案，则存在一个多项式时间算法 $\mathcal{B}$ 以概率 $\varepsilon'=\varepsilon-\mathrm{negl}\left(\lambda\right)$ 解决 $\mathrm{SIS}_{q,m,\beta}$ 问题。

证明. 假设存在这样的敌手 $\mathcal{A}_{\mathrm{I}}$，我们构造算法 $\mathcal{B}$，它模拟 $\mathcal{A}_{\mathrm{I}}$ 的挑战者并利用 $\mathcal{A}_{\mathrm{I}}$ 的伪造解决 $\mathrm{SIS}_{q,m,\beta}$ 问题。$\mathcal{B}$ 执行的各项操作如下：

假设 $\mathcal{B}$ 收到一个 $\mathrm{SIS}_{q,m,\beta}$ 问题实例 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$，希望找到一个非零向量 $\boldsymbol{e}\in\mathbb{Z}^m$，满足 $\boldsymbol{A}_0\boldsymbol{e}=\boldsymbol{0}\ \bmod q$ 和 $\left\|\boldsymbol{e}\right\|\le\beta$。

初始化：$\mathcal{A}_{\mathrm{I}}$ 输出身份 $id^*=\left(id_1^*,\cdots,id_\ell^*\right)\in\left\{0,1\right\}^\ell$、公钥 pk'_{id^*} 和消息集合 $\left\{\mu_i\in\mathcal{M}\right\}_{i\in[N]}$。

设置：$\mathcal{B}$ 设置系统公开参数如下：

① 选取 ℓ 个矩阵 $\boldsymbol{R}_{i,id_i^*}\leftarrow\mathcal{D}^{m\times m}$，其中 $i\in\left[\ell\right]$。

② 令 $\boldsymbol{A}=\boldsymbol{A}_0\cdot\boldsymbol{R}_{\ell,id_\ell^*}\cdots\boldsymbol{R}_{1,id_1^*}\ \bmod q$。

③ 对 $i\in\left[\ell\right]$，若 $i=1$，则 $\boldsymbol{P}_i=\boldsymbol{A}$，若 $2\le i\le\ell$，则 $\boldsymbol{P}_i=\boldsymbol{A}\left(\boldsymbol{R}_{i-1,id_{i-1}^*}\cdots\boldsymbol{R}_{1,id_1^*}\right)^{-1}\ \bmod q$。

④ 对 $\boldsymbol{P}_i\in\mathbb{Z}_q^{n\times m}$，其中 $i\in\left[\ell\right]$，调用 $\mathrm{SampleRwithBasis}\left(\boldsymbol{P}_i\right)$ 产生一个矩阵 $\boldsymbol{R}_{i,1-id_i^*}\in\mathbb{Z}^{m\times m}$ 和格 $\Lambda^{\perp}\left(\boldsymbol{W}_i\right)$ 的

一组基 $\boldsymbol{T}_{\boldsymbol{W}_i}\in\mathbb{Z}^{m\times m}$，其中 $\boldsymbol{W}_i=\boldsymbol{P}_i\boldsymbol{R}^{-1}_{i,1-id_i^*} \bmod q$。

⑤ 选取 N 个矩阵 $\boldsymbol{U}_i\leftarrow\left(D_{\mathbb{Z}^{2m},s_2}\right)^{2m}$，其中 $i\in[N]$。

⑥ 对每一 $i\in[N]$，令 $\boldsymbol{V}_i=\begin{pmatrix}\boldsymbol{A}_0 & \\ & pk'_{id^*}\end{pmatrix}\boldsymbol{U}_i+\mu_i\cdot\boldsymbol{G}\in\mathbb{Z}_q^{2n\times 2m}$，其中 $\boldsymbol{G}\in\mathbb{Z}_q^{2n\times 2m}$。

⑦ 令 $param=\left(\boldsymbol{A},\left\{\boldsymbol{R}_{i,id_i^*},\boldsymbol{R}_{i,1-id_i^*}\right\}_{i\in[\ell]},\left\{\boldsymbol{V}_i\right\}_{i\in[N]}\right)$，并把它发送给 $\mathcal{A}_{\mathrm{I}}$。

询问：$\mathcal{A}_{\mathrm{I}}$ 适应性地向挑战者发出以下询问：

部分私钥询问：$\mathcal{A}_{\mathrm{I}}$ 提交身份 $id=(id_1,\cdots,id_\ell)\in\{0,1\}^\ell$，其中 $id\neq id^*$。令 $i\in[\ell]$ 使得 $id_i\neq id_i^*$，且对任意 $1\le k\le i-1$，有 $id_k=id_k^*$。若 $1\le i\le\ell-1$，令 $\boldsymbol{R}'=\boldsymbol{R}_{\ell,id_\ell}\cdots\boldsymbol{R}_{i+1,id_{i+1}}\in\mathbb{Z}^{m\times m}$，调用 $\mathrm{BasisDel}\left(\boldsymbol{W}_i,\boldsymbol{T}_{\boldsymbol{W}_i},\boldsymbol{R}',s_1\right)$ 产生格 $\Lambda^{\perp}(\boldsymbol{B})$ 的一组基 $\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}^{m\times m}$，其中 $\boldsymbol{B}=\boldsymbol{W}_i\cdot(\boldsymbol{R}')^{-1} \bmod q$，令 $psk_{id}=\boldsymbol{T}_{\boldsymbol{B}}$；若 $i=\ell$，令 $psk_{id}=\boldsymbol{T}_{\boldsymbol{W}_\ell}$。把 psk_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$。

秘密值询问：$\mathcal{B}$ 维护一个元组列表 $L=\left\{(id,x_{id},pk_{id})\right\}$。$\mathcal{A}_{\mathrm{I}}$ 提交身份 id。$\mathcal{B}$ 首先在表 L 中查找元组 (id,x_{id},pk_{id})。若找到该元组，把 x_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$；若未找到，执行 $(x_{id},pk_{id})\leftarrow\mathrm{KeyGen}(param,id)$，把 x_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$，并把 (id,x_{id},pk_{id}) 添加到表 L 中。

公钥询问：$\mathcal{A}_{\mathrm{I}}$ 提交身份 id。$\mathcal{B}$ 首先在表 L 中查找元组 (id,x_{id},pk_{id})。若找到该元组，把 pk_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$；若未找到，执行 $(x_{id},pk_{id})\leftarrow\mathrm{KeyGen}(param,id)$，把 pk_{id} 发送给 $\mathcal{A}_{\mathrm{I}}$，并把 (id,x_{id},pk_{id}) 添加到表 L 中。

签名询问：把 $\{\sigma_i=\boldsymbol{U}_i\}_{i\in[N]}$ 发送给 $\mathcal{A}_{\mathrm{I}}$。对于 $\boldsymbol{U}_i\in\{\boldsymbol{U}_1,\cdots,\boldsymbol{U}_N\}$，因为 $\boldsymbol{R}^*=\boldsymbol{R}_{\ell,id_\ell^*}\cdots\boldsymbol{R}_{1,id_1^*}\in\mathbb{Z}^{m\times m}$，所以

$$\boldsymbol{F}^*=\begin{pmatrix}\boldsymbol{A}\cdot(\boldsymbol{R}^*)^{-1} & \\ & pk'_{id^*}\end{pmatrix}=\begin{pmatrix}\boldsymbol{A}_0\cdot\boldsymbol{R}_{\ell,id_\ell^*}\cdots\boldsymbol{R}_{1,id_1^*}\cdot\left(\boldsymbol{R}_{\ell,id_\ell^*}\cdots\boldsymbol{R}_{1,id_1^*}\right)^{-1} & \\ & pk'_{id^*}\end{pmatrix}=\begin{pmatrix}\boldsymbol{A}_0 & \\ & pk'_{id^*}\end{pmatrix}\in\mathbb{Z}_q^{2n\times 2m}$$

所以 $\boldsymbol{F}^*\boldsymbol{U}_i=\boldsymbol{V}_i-\mu_i\cdot\boldsymbol{G} \bmod q$；对于 $\boldsymbol{U}_i\in\{\boldsymbol{U}_1,\cdots,\boldsymbol{U}_N\}$，因为 $\boldsymbol{U}_i\leftarrow\left(D_{\mathbb{Z}^{2m},s_2}\right)^{2m}$，所以 $\|\boldsymbol{U}_i\|\le s_2\cdot\sqrt{2m}$。故而，$\boldsymbol{U}_i\in\{\boldsymbol{U}_1,\cdots,\boldsymbol{U}_N\}$ 是 id^* 和 pk'_{id^*} 对 $\mu_i\in\{\mu_1,\cdots,\mu_N\in\mathcal{M}\}$ 的有效签名。

伪造：$\mathcal{A}_{\mathrm{I}}$ 输出电路 $f^*:\mathcal{M}^N\to\mathcal{M}$、消息 $\mu^*\in\{0,1\}$ 和签名 $\boldsymbol{U}^*$，其中 $\mathrm{depth}\left(f^*\right)\le d$。若 $\mathcal{A}_{\mathrm{I}}$ 赢得了游戏，$\mathcal{B}$ 利用 $\mathcal{A}_{\mathrm{I}}$ 的伪造能够求得 $\mathrm{SIS}_{q,m,\beta}$ 问题实例 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$ 的解答。求解过程具体如下：

因为 $\mathcal{A}_{\mathrm{I}}$ 伪造的签名 $\boldsymbol{U}^*$ 是有效的，所以 $\boldsymbol{F}^*\boldsymbol{U}^*=\boldsymbol{V}_{f^*}-\mu^*\cdot\boldsymbol{G} \bmod q$ 和 $\|\boldsymbol{U}^*\|\le(2m+1)^{\mathrm{depth}(f^*)}\cdot s_2\cdot\sqrt{2m}$，其中 $\mu^*\neq\mu_{f^*}=f^*(\mu_1,\cdots,\mu_N)$。因为 $\mathrm{depth}\left(f^*\right)\le d$，计算的签名 $\boldsymbol{U}_{f^*}\leftarrow\mathrm{Eval}\left(param,id^*,f^*,\left\{(\mu_i,\sigma_i)\right\}_{i\in[N]}\right)$ 亦是有效的，所以 $\boldsymbol{F}^*\boldsymbol{U}_{f^*}=\boldsymbol{V}_{f^*}-\mu_{f^*}\cdot\boldsymbol{G} \bmod q$ 和 $\left\|\boldsymbol{U}_{f^*}\right\|\le(2m+1)^{\mathrm{depth}(f^*)}\cdot s_2\cdot\sqrt{2m}$。

故而 $\boldsymbol{F}^*\left(\boldsymbol{U}^*-\boldsymbol{U}_{f^*}\right)=\left(\mu_{f^*}-\mu^*\right)\cdot\boldsymbol{G} \bmod q$ 和 $\left\|\boldsymbol{U}^*-\boldsymbol{U}_{f^*}\right\|\le 2(2m+1)^{\mathrm{depth}(f^*)}\cdot s_2\cdot\sqrt{2m}$，其中 $\mu_{f^*}-\mu^*\neq 0$。令 $\boldsymbol{U}^*-\boldsymbol{U}_{f^*}=\begin{pmatrix}\boldsymbol{U}_1' & \boldsymbol{U}_2'\\ \boldsymbol{U}_1'' & \boldsymbol{U}_2''\end{pmatrix}\in\mathbb{Z}^{2m\times 2m}$，其中 $\boldsymbol{U}_1',\boldsymbol{U}_1'',\boldsymbol{U}_2',\boldsymbol{U}_2''\in\mathbb{Z}^{m\times m}$，令 $\boldsymbol{G}=\begin{pmatrix}\boldsymbol{G}_0 & \\ & \boldsymbol{G}_0\end{pmatrix}\in\mathbb{Z}_q^{2n\times 2m}$，其中 $\boldsymbol{G}_0\in\mathbb{Z}_q^{n\times m}$。则

$$\begin{pmatrix}\boldsymbol{A}_0 & \\ & pk'_{id^*}\end{pmatrix}\begin{pmatrix}\boldsymbol{U}_1' & \boldsymbol{U}_2'\\ \boldsymbol{U}_1'' & \boldsymbol{U}_2''\end{pmatrix}=\left(\mu_{f^*}-\mu^*\right)\cdot\begin{pmatrix}\boldsymbol{G}_0 & \\ & \boldsymbol{G}_0\end{pmatrix} \bmod q.$$

因而 $\boldsymbol{A}_0\boldsymbol{U}_1'=\left(\mu_{f^*}-\mu^*\right)\cdot\boldsymbol{G}_0 \mod q$。$\mathcal{B}$ 均匀随机地选取 $\boldsymbol{z}\in\{0,1\}^m$。令 $\boldsymbol{e}=\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)-\boldsymbol{z}$。下面证明 $\boldsymbol{e}$ 为 $\mathrm{SIS}_{q,m,\beta}$ 问题实例 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$ 的一个解答。可以看出

$$\begin{aligned}\boldsymbol{A}_0\boldsymbol{e}&=\boldsymbol{A}_0\left(\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)-\boldsymbol{z}\right)\\&=\boldsymbol{A}_0\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)-\boldsymbol{A}_0\boldsymbol{z}\\&=\left(\mu_{f^*}-\mu^*\right)\cdot\boldsymbol{G}_0\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)-\boldsymbol{A}_0\boldsymbol{z}\\&=\left(\mu_{f^*}-\mu^*\right)\cdot\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)-\boldsymbol{A}_0\boldsymbol{z}\\&=\boldsymbol{A}_0\boldsymbol{z}-\boldsymbol{A}_0\boldsymbol{z}\\&=\boldsymbol{0}\end{aligned}$$

$$\begin{aligned}\|\boldsymbol{e}\|&=\left\|\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)-\boldsymbol{z}\right\|\\&\le\left\|\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)\right\|+\|\boldsymbol{z}\|\\&\le\sqrt{m}\cdot\|\boldsymbol{U}_1'\|\cdot\left\|\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)\right\|+\|\boldsymbol{z}\|\\&\le\sqrt{m}\cdot\left\|\boldsymbol{U}^*-\boldsymbol{U}_{f^*}\right\|\cdot\sqrt{m}+\sqrt{m}\\&\le\sqrt{m}\cdot2\left(2m+1\right)^{\mathrm{depth}\left(f^*\right)}\cdot s_2\sqrt{2m}\cdot\sqrt{m}+\sqrt{m}\\&\le2m\left(2m+1\right)^{\mathrm{depth}\left(f^*\right)}\cdot s_2\sqrt{2m}+\sqrt{m}\\&\le\left(2m+1\right)\cdot\left(2m+1\right)^{\mathrm{depth}\left(f^*\right)}\cdot s_2\sqrt{2m}\\&\le\left(2m+1\right)^{\mathrm{depth}\left(f^*\right)+1}\cdot s_2\sqrt{2m}\\&\le\beta.\end{aligned}$$

还需证明 $\boldsymbol{e}\neq\boldsymbol{0}$，即 $\boldsymbol{z}\neq\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)$。在给定 $\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)$ 的情况下 $\boldsymbol{z}$ 的最小熵为 $\mathrm{H}_\infty\left(\boldsymbol{z}\,|\,\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)\right)\ge\mathrm{H}_\infty\left(\boldsymbol{z}\,|\,\boldsymbol{A}_0\boldsymbol{z}\right)\ge m-n\log q=O\left(n\log q\right)-n\log q\ge\omega\left(\log\lambda\right)$，其中第二个不等式根据引理 1 得到，因此 $\Pr\left[\boldsymbol{z}=\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)\right]\le2^{-\omega(\log\lambda)}=\mathrm{negl}\left(\lambda\right)$，因此 $\boldsymbol{z}\neq\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)$，即 $\boldsymbol{e}\neq\boldsymbol{0}$。因此 $\boldsymbol{e}=\boldsymbol{U}_1'\cdot\boldsymbol{G}_0^{-1}\left(\boldsymbol{A}_0\boldsymbol{z}/\left(\mu_{f^*}-\mu^*\right)\right)-\boldsymbol{z}$ 为 $\mathrm{SIS}_{q,m,\beta}$ 问题实例 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$ 的一个解答。

由引理 3 和 5 可知，$\mathcal{B}$ 模拟的挑战者与真实挑战者是统计不可区分的，因此敌手 $\mathcal{A}_\mathrm{I}$ 在模拟游戏中攻击所提出的 CLFHS 方案的优势为 $\varepsilon-\mathrm{negl}\left(\lambda\right)$。故 $\mathcal{B}$ 成功求解 $\mathrm{SIS}_{q,m,\beta}$ 问题的概率为 $\varepsilon-\mathrm{negl}\left(\lambda\right)$。

定理 3. 如果存在一个多项式时间敌手 $\mathcal{A}_\mathrm{II}$ 在游戏 2 中以优势 ε 攻击所提出的 CLFHS 方案，则存在一个多项式时间算法 $\mathcal{B}$ 以概率 $\varepsilon'=\varepsilon-\mathrm{negl}\left(\lambda\right)$ 解决 $\mathrm{SIS}_{q,m,\beta}$ 问题。

证明. 假设存在这样的敌手 $\mathcal{A}_\mathrm{II}$，我们构造算法 $\mathcal{B}$，它模拟 $\mathcal{A}_\mathrm{II}$ 的挑战者并利用 $\mathcal{A}_\mathrm{II}$ 的伪造解决 $\mathrm{SIS}_{q,m,\beta}$ 问题。$\mathcal{B}$ 执行的各项操作如下：

假设 $\mathcal{B}$ 收到一个 $\mathrm{SIS}_{q,m,\beta}$ 问题实例 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$，希望找到一个非零向量 $\boldsymbol{e}\in\mathbb{Z}^m$，满足 $\boldsymbol{A}_0\boldsymbol{e}=\boldsymbol{0} \mod q$ 和 $\|\boldsymbol{e}\|\le\beta$。

初始化：$\mathcal{A}_{\text{II}}$ 输出身份 $id^* \in \{0,1\}^{\ell}$ 和消息集合 $\{\mu_i \in \mathcal{M}\}_{i\in[N]}$。

设置：$\mathcal{B}$ 设置系统公开参数如下：

① 调用 $\text{GenBasis}\left(1^n,1^m,q\right)$ 产生一个矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和格 $\Lambda^{\perp}\left(\boldsymbol{A}\right)$ 的一组基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$，满足 $\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\right\|\le\tilde{L}=O\left(\sqrt{n\log q}\right)$。

② 选取 2ℓ 个矩阵 $\boldsymbol{R}_{i,0},\boldsymbol{R}_{i,1}\leftarrow\mathcal{D}^{m\times m}$，其中 $i\in[\ell]$。

③ 计算 $\boldsymbol{R}^*=\boldsymbol{R}_{\ell,id_{\ell}^*}\cdots\boldsymbol{R}_{1,id_1^*}\in\mathbb{Z}^{m\times m}$。

④ 选取 N 个矩阵 $\boldsymbol{U}_i\leftarrow\left(D_{\mathbb{Z}^{2m},s_2}\right)^{2m}$，其中 $i\in[N]$。

⑤ 对每一 $i\in[N]$，令 $\boldsymbol{V}_i=\begin{pmatrix}\boldsymbol{A}\left(\boldsymbol{R}^*\right)^{-1}\\ &\boldsymbol{A}_0\end{pmatrix}\boldsymbol{U}_i+\mu_i\cdot\boldsymbol{G}\in\mathbb{Z}_q^{2n\times 2m}$，其中 $\boldsymbol{G}\in\mathbb{Z}_q^{2n\times 2m}$。

⑥ 令 $param=\left(\boldsymbol{A},\left\{\boldsymbol{R}_{i,0},\boldsymbol{R}_{i,1}\right\}_{i\in[\ell]},\left\{\boldsymbol{V}_i\right\}_{i\in[N]}\right)$ 和 $msk=\boldsymbol{T}_{\boldsymbol{A}}$，并把它们发送给 $\mathcal{A}_{\text{II}}$。

询问：$\mathcal{A}_{\text{II}}$ 适应性地向挑战者发出以下询问：

秘密值询问：$\mathcal{B}$ 维护一个元组列表 $L=\left\{\left(id,x_{id},pk_{id}\right)\right\}$。$\mathcal{A}_{\text{II}}$ 提交身份 id，其中 $id\ne id^*$。首先在表 L 中查找元组 $\left(id,x_{id},pk_{id}\right)$。若找到该元组，把 x_{id} 发送给 $\mathcal{A}_{\text{II}}$；若未找到，执行 $\left(x_{id},pk_{id}\right)\leftarrow\text{KeyGen}\left(param,id\right)$，把 x_{id} 发送给 $\mathcal{A}_{\text{II}}$，并把 $\left(id,x_{id},pk_{id}\right)$ 添加到表 L 中。

公钥询问：$\mathcal{A}_{\text{II}}$ 提交身份 id。首先在表 L 中查找元组 $\left(id,x_{id},pk_{id}\right)$。若找到该元组，把 pk_{id} 发送给 $\mathcal{A}_{\text{II}}$；若未找到，如果 $id=id^*$，则令 $pk_{id^*}=\boldsymbol{A}_0$，把 pk_{id^*} 发送给 $\mathcal{A}_{\text{II}}$，并把 $\left(id^*,\perp,pk_{id^*}\right)$ 添加到表 L 中，否则执行 $\left(x_{id},pk_{id}\right)\leftarrow\text{KeyGen}\left(param,id\right)$，把 pk_{id} 发送给 $\mathcal{A}_{\text{II}}$，并把 $\left(id,x_{id},pk_{id}\right)$ 添加到表 L 中。

签名询问：把 $\left\{\sigma_i=\boldsymbol{U}_i\right\}_{i\in[N]}$ 发送给 $\mathcal{A}_{\text{II}}$。对于 $\boldsymbol{U}_i\in\left\{\boldsymbol{U}_1,\cdots,\boldsymbol{U}_N\right\}$，因为

$$\boldsymbol{F}^*=\begin{pmatrix}\boldsymbol{A}\left(\boldsymbol{R}^*\right)^{-1}\\ &pk_{id^*}\end{pmatrix}=\begin{pmatrix}\boldsymbol{A}\left(\boldsymbol{R}^*\right)^{-1}\\ &\boldsymbol{A}_0\end{pmatrix}$$

所以 $\boldsymbol{F}^*\boldsymbol{U}_i=\boldsymbol{V}_i-\mu_i\cdot\boldsymbol{G}\mod q$；对于 $\boldsymbol{U}_i\in\left\{\boldsymbol{U}_1,\cdots,\boldsymbol{U}_N\right\}$，因为 $\boldsymbol{U}_i\leftarrow\left(D_{\mathbb{Z}^{2m},s_2}\right)^{2m}$，所以 $\left\|\boldsymbol{U}_i\right\|\le s_2\cdot\sqrt{2m}$。故而，$\boldsymbol{U}_i\in\left\{\boldsymbol{U}_1,\cdots,\boldsymbol{U}_N\right\}$ 是 id^* 和 pk_{id^*} 对 $\mu_i\in\left\{\mu_1,\cdots,\mu_N\in\mathcal{M}\right\}$ 的有效签名。

伪造：$\mathcal{A}_{\text{II}}$ 输出电路 $f^*:\mathcal{M}^N\to\mathcal{M}$、消息 $\mu^*\in\{0,1\}$ 和签名 $\boldsymbol{U}^*$，其中 $\text{depth}\left(f^*\right)\le d$。若 $\mathcal{A}_{\text{II}}$ 赢得了游戏，$\mathcal{B}$ 利用 $\mathcal{A}_{\text{II}}$ 的伪造能够求得 $\text{SIS}_{q,m,\beta}$ 问题实例 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$ 的解答。求解思路与定理 2 基本相同，不再赘述具体过程。

由引理 3 和 5 可知，$\mathcal{B}$ 模拟的挑战者与真实挑战者是统计不可区分的，因此敌手 $\mathcal{A}_{\text{II}}$ 在模拟游戏中攻击所提出的 CLFHS 方案的优势为 $\varepsilon-\text{negl}(\lambda)$。故 $\mathcal{B}$ 成功求解 $\text{SIS}_{q,m,\beta}$ 问题的概率为 $\varepsilon-\text{negl}(\lambda)$。

4.3. 参数设置

所提出的 CLFHS 方案要正确运行，需满足以下约束条件：

① 对于 GenBasis 算法，$m\ge 5n\log q$。

② 对于 BasisDel 算法，$s_1\ge\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\right\|\cdot\tilde{L}\cdot\sqrt{m}\cdot\omega\left(\sqrt{\log m}\right)^4$，其中 $\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{A}}}\right\|\le\tilde{L}=O\left(\sqrt{n\log q}\right)$。

③ 对于 SamplePre 算法，$s_2\ge\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{F}}}\right\|\cdot\omega\left(\sqrt{\log m}\right)$，其中 $\left\|\widetilde{\boldsymbol{T}_{\boldsymbol{F}}}\right\|\le\left\|\boldsymbol{T}_{\boldsymbol{F}}\right\|\le s_1\sqrt{m}$。

④ 对于安全性归约证明， $\beta \geq (2m+1)^{\mathrm{depth}(f^*)+1} \cdot s_2\sqrt{2m}$ ，其中 $\mathrm{depth}(f^*) \leq d$ 。

⑤ 对于 SIS 问题的困难性， $m = \mathrm{poly}(n)$ ， $\beta = \mathrm{poly}(n)$ ， $q \geq \beta \cdot \omega\left(\sqrt{n \log n}\right)$ 。

在这些约束条件下，方案的参数可设置如下：

$n = \lambda$	$m = \lceil 5n \log q \rceil$
$s_1 = m^{3/2} \cdot \omega\left(\sqrt{\log m}\right)^4$	$s_2 = m^2 \cdot \omega\left(\sqrt{\log m}\right)^5$
$\beta = \sqrt{2} \cdot m^{5/2}(2m+1)^{d+1} \cdot \omega\left(\sqrt{\log m}\right)^5$	$q = \sqrt{2} \cdot m^3(2m+1)^{d+1} \cdot \omega\left(\sqrt{\log m}\right)^6$

假如给定安全参数 $\lambda = 80$ 、电路的最大深度 $d = 5$ ，方案的参数具体为：

$n = 80$	$m = 62563$
$s_1 = 3.9726 \times 10^9$	$s_2 = 3.9663 \times 10^{12}$
$\beta = 5.3847 \times 10^{45}$	$q = 1.21 \times 10^{47}$

4.4. 性能分析

目前人们还没有提出层次型 CLFHS 方案。于是，将所提出的 CLFHS 方案与层次型 IBFHS 方案[17]-[19]进行比较。有关结果如表 2 所示，其中 β_{init} 表示 Sign 算法产生的签名的噪声级，如在所提出的 CLFHS 方案中， $\beta_{\mathrm{init}} = s_2\sqrt{2m}$ 。从表 2 可以看出，所提出的 CLFHS 方案比 IBFHS 方案[17]-[19]的公开参数尺寸大，这主要是由于无证书密码方案比基于身份的密码方案结构复杂的缘故。从表 2 还可以看出，所提出的 CLFHS 方案的安全性比 IBFHS 方案[17]-[19]弱，最大噪声级比 IBFHS 方案[17]-[19]大。

Table 2. Comparison of performance
表 2. 性能比较

方案	公开参数尺寸	签名尺寸	不可伪造性	隐私性	最大噪声级
[17]	$\tilde{O}(N\lambda^2)$	$\tilde{O}(\lambda^2)$	SU-sID-sCMA	弱上下文隐藏	$O(4^d m\beta_{\mathrm{init}})$
[18]	$\tilde{O}(N\lambda^2)$	$\tilde{O}(\lambda^2)$	SU-sID-sCMA	弱上下文隐藏	$O(2^d \beta_{\mathrm{init}})$
[19]	$\tilde{O}(\lambda^2)$	$\tilde{O}(\lambda^2)$	SU-ID-CMA	无	$O(4^d m\beta_{\mathrm{init}})$
本文方案	$\tilde{O}((N+\ell)\lambda^2)$	$\tilde{O}(\lambda^2)$	EU-sID-sCMA	弱上下文隐藏	$O(m^d \beta_{\mathrm{init}})$

5. 结束语

本文利用格提出了第一个层次型 CLFHS 方案，并在标准模型下基于 SIS 问题的困难性证明了它满足 EU-sID-sCMA 安全性。本文所提出的 CLFHS 方案还有可改进提高的方面，如存在性不可伪造性等。作者接下来将致力于构造强不可伪造的格上层次型 CLFHS 方案。此外，作者还将致力于利用所提出的 CLFHS 方案设计电子投票系统、电子健康记录系统等。

基金项目

本文得到河北金融学院支持硕士点建设“揭榜挂帅”课题(JB2025004)资助。

参考文献

[1] Diffie, W. and Hellman, M. (1976) New Directions in Cryptography. *IEEE Transactions on Information Theory*, **22**, 644-654.

[2] Shamir, A. (2000) Identity-Based Cryptosystems and Signature Schemes. In: Blakley, G.R. and Chaum, D., Eds., *Advances in Cryptology*, Springer, 47-53. https://doi.org/10.1007/3-540-39568-7_5

[3] Al-Riyami, S.S. and Paterson, K.G. (2003) Certificateless Public Key Cryptography. In: Laih, C.S., Ed., *Advances in Cryptology—ASIACRYPT* 2003, Springer, 452-473. https://doi.org/10.1007/978-3-540-40061-5_29

[4] 王艳, 江明明, 郭宇燕, 等. 基于格密码的高效无证书签名方案[J]. 江苏师范大学学报(自然科学版), 2019, 37(2): 63-66.

[5] Kim, K.S. and Jeong, I.R. (2014) A New Certificateless Signature Scheme under Enhanced Security Models. *Security and Communication Networks*, **8**, 801-810. https://doi.org/10.1002/sec.1036

[6] 梁红梅. 格上无陷门的无证书签名[J]. 闽南师范大学学报(自然科学版), 2021, 34(4): 32-38.

[7] Yu, S., Dou, K., Zhao, H. and Han, Y. (2023) An Efficient Certificateless Signature Scheme on Lattice. *Second International Conference on Electronic Information Technology* (*EIT* 2023), Wuhan, 17-19 March 2023, 662-667. https://doi.org/10.1117/12.2685750

[8] Xu, S., Yu, S., Yue, Z. and Liu, Y. (2024) CLLS: Efficient Certificateless Lattice-Based Signature in VANETs. *Computer Networks*, **255**, Article ID: 110858. https://doi.org/10.1016/j.comnet.2024.110858

[9] Gentry, C., Sahai, A. and Waters, B. (2013) Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-based. In: Canetti, R. and Garay, J.A., Eds., *Advances in Cryptology—CRYPTO* 2013, Springer, 75-92. https://doi.org/10.1007/978-3-642-40041-4_5

[10] Wang, F., Wang, K. and Li, B. (2015) An Efficient Leveled Identity-Based FHE. In: Qiu, M., Xu, S., Yung, M. and Zhang, H., Eds., *Network and System Security*, Springer, 303-315. https://doi.org/10.1007/978-3-319-25645-0_20

[11] 康元基, 顾纯祥, 郑永辉, 等. 利用特征向量构造基于身份的全同态加密体制[J]. 软件学报, 2016, 27(6): 1487-1497.

[12] 辛丹, 顾纯祥, 郑永辉, 等. 利用 RLWE 构造基于身份的全同态加密体制[J]. 电子学报, 2016, 44(12): 2887-2893.

[13] Li, M. (2020) Leveled Certificateless Fully Homomorphic Encryption Schemes from Learning with Errors. *IEEE Access*, **8**, 26749-26763. https://doi.org/10.1109/access.2020.2971342

[14] 吴华麟, 陈文彬, 高崇志, 等. 同态签名研究综述[J]. 密码学报, 2021, 8(5): 758-777.

[15] Gorbunov, S., Vaikuntanathan, V. and Wichs, D. (2015) Leveled Fully Homomorphic Signatures from Standard Lattices. *Proceedings of the Forty-Seventh Annual ACM symposium on Theory of Computing*, Portland, 14-17 June 2015, 469-477. https://doi.org/10.1145/2746539.2746576

[16] Boyen, X., Fan, X. and Shi, E. (2014) Adaptively Secure Fully Homomorphic Signatures Based on Lattices. http://eprint.iacr.org/2014/916.pdf

[17] Wang, F., Wang, K., Li, B. and Gao, Y. (2015) Leveled Strongly-Unforgeable Identity-Based Fully Homomorphic Signatures. In: Lopez, J. and Mitchell, C., Eds., *Information Security*, Springer, 42-60. https://doi.org/10.1007/978-3-319-23318-5_3

[18] Wang, Y. and Wang, M. (2020) A New Fully Homomorphic Signatures from Standard Lattices. In: Yu, D., Dressler, F. and Yu, J., Eds., *Wireless Algorithms*, *Systems*, *and Applications*, Springer, 494-506. https://doi.org/10.1007/978-3-030-59016-1_41

[19] Wang, C., Wu, B. and Yao, H. (2020) Leveled Adaptively Strong-Unforgeable Identity-Based Fully Homomorphic Signatures. *IEEE Access*, **8**, 119431-119447. https://doi.org/10.1109/access.2020.3003685

[20] Dodis, Y., Reyzin, L. and Smith, A. (2004) Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In: Cachin, C. and Camenisch, J.L., Eds., *Advances in Cryptology—EUROCRYPT* 2004, Springer, 523-540. https://doi.org/10.1007/978-3-540-24676-3_31

[21] Micciancio, D. and Regev, O. (2007) Worst-Case to Average-Case Reductions Based on Gaussian Measures. *SIAM Journal on Computing*, **37**, 267-302. https://doi.org/10.1137/s0097539705447360

[22] Gentry, C., Peikert, C. and Vaikuntanathan, V. (2008) Trapdoors for Hard Lattices and New Cryptographic Constructions. *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, Victoria, 17-20 May 2008, 197-206. https://doi.org/10.1145/1374376.1374407

[23] Alwen, J. and Peikert, C. (2010) Generating Shorter Bases for Hard Random Lattices. *Theory of Computing Systems*, **48**, 535-553. https://doi.org/10.1007/s00224-010-9278-3

[24] Micciancio, D. and Peikert, C. (2012) Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In: Pointcheval, D. and

Johansson, T., Eds., *Advances in Cryptology—EUROCRYPT* 2012, Springer, 700-718. https://doi.org/10.1007/978-3-642-29011-4_41

[25] Agrawal, S., Boneh, D. and Boyen, X. (2010) Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE. In: Rabin, T., Ed., *Advances in Cryptology—CRYPTO* 2010, Springer, 98-115. https://doi.org/10.1007/978-3-642-14623-7_6