标准模型安全的线性同态聚合签名

韩益亮[1,2,3]，李瑞峰[1,2]，周潭平[1,2]，汪晶晶[1,2]，杨晓元[1,2]
（1.武警工程大学密码工程学院，陕西 西安 710086；2.网络与信息安全武警部队重点实验室，陕西 西安 710086；
3.武警工程大学反恐指挥信息工程教育部重点实验室，陕西 西安 710086）

摘　要：现有格基线性同态签名方案难以兼顾多用户聚合与标准模型下的可证安全，限制了其在实际分布式场景中的应用。基于此，提出一种标准模型下可证安全的线性同态聚合签名方案。该方案采用格基左扩展（LeftExt）算法将多用户独立公钥整合为统一全局公钥矩阵，提供了聚合签名所需的密钥同态性；引入满秩差分哈希函数与格基右扩展（RightExt）算法，实现了标准模型下的签名模拟。所提方案可抵抗适应性选择消息攻击，将敌手的攻击优势严格规约至格上短整数解问题的困难性，为多源数据协同计算提供了更安全的保障。

关键词：格密码；同态签名；聚合签名；标准模型
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025187

Linearly homomorphic aggregate signature secure in the standard model

HAN Yiliang[1,2,3], LI Ruifeng[1,2], ZHOU Tanping[1,2], WANG Jingjing[1,2], YANG Xiaoyuan[1,2]
1. School of Cryptography and Engineering, Engineering University of PAP, Xi'an 710086, China
2. Key Lab of the Armed Police Force for Network and Information Security, Xi'an 710086, China
3. Key Laboratory of Counter-Terrorism Command & Information Engineering of Ministry of Education, Engineering University of PAP, Xi'an 710086, China

Abstract: Existing lattice-based linear homomorphic signature schemes have difficulty in balancing multi-user aggregation and provable security under the standard model, which limits their practical application in real-world distributed scenarios. A linearly homomorphic aggregate signature scheme with provable security under the standard model was proposed. The lattice-based left extension (LeftExt) algorithm was employed in the scheme to integrate the independent public keys of multiple users into a unified global public key matrix, which provided the key homomorphism required for aggregate signatures. A full-rank differential Hash function and the lattice-based right extension (RightExt) algorithm were introduced to achieve signature simulation under the standard model. The scheme can resist adaptive chosen-message attacks, and the adversary's attack advantage is strictly reduced to the hardness of the short integer solution problem on lattices, which provides more secure guarantees for multi-source data collaborative computing.

Keywords: lattice cryptography, homomorphic signature, aggregate signature, standard model

0　引言

随着云计算与物联网技术的快速发展，数据完整性验证需求已从单一源静态认证扩展到多源动态计算场景。同态签名技术因其支持对签名数据直接运算的特性，成为保障分布式计算可信性的重要工具[1]。其中，线性同态签名允许对签名数据执行线

收稿日期：2025–08–19；修回日期：2025–10–16
通信作者：杨晓元，yxyangyxyang@163.com
基金项目：国家自然科学基金资助项目（No.62172436, No.62102452）
Foundation Items：The National Natural Science Foundation of China (No.62172436, No.62102452)

性组合操作后仍保持可验证性，其应用场景广泛而深入。在网络编码中，中间节点可对收到的已签名数据包进行线性组合转发，接收方可直接验证组合后数据的完整性，极大提升了网络吞吐率。在边缘计算中，多个终端设备可将传感数据的签名上传至边缘节点，节点直接对签名数据执行求平均值、加权和等线性聚合运算，并生成可被云端验证的紧凑聚合签名，有效减轻通信开销。在分布式存储计算与联邦学习中，线性同态签名可用于验证来自不同工作节点的中间计算结果的正确性，确保分布式计算过程的可靠性。在区块链与数据审计领域，线性同态签名可实现对链上或云存储中线性处理后的数据的高效来源认证与完整性校验。然而，现有方案多基于传统数论难题[2-5]，其安全性面临量子计算威胁[6-7]。格密码凭借抗量子攻击特性与天然的线性代数结构，为构建新一代线性同态签名提供了理想载体。

格基线性同态签名的发展主线围绕提升效率与强化安全模型展开，其核心技术差异体现在如何将文件标识符与数据集在构造签名的过程中联系起来，以及如何生成签名的陷门。早期方案多基于随机预言模型设计。Boneh等[8]开创性地将格密码引入同态签名领域，其方案利用随机预言机模拟理想哈希函数来处理数据集标签，结合Cash等[9]的格基扩展算法与中国剩余定理[10]，采用GPV（Gentry-Peikert-Vaikuntanathan）签名[11]实现数据认证与线性同态性，提出了首个格基线性同态签名方案。文献[8]将文件标识符与验证矩阵绑定，并使用格基左扩展（LeftExt）算法生成陷门，这种构造算式导致验证矩阵扩展为公钥矩阵的2倍。为了提升验证效率，Boneh等[12]进一步提出两整数格相交法来建立文件标识符和数据集之间的联系，并摆脱了格基扩展算法，从而优化了验证矩阵维度，显著提升了运算效率。Wang等[13]基于文献[14]的同态哈希函数改进文献[8]中文件标识符的绑定机制，起到了与文献[12]中两整数格相交法同样提升效率的作用。

上述随机预言模型下的方案设计相对直接，哈希函数被抽象为一个“理想黑盒”，用于实现随机的、无冲突的映射，其安全性证明依赖于这一理想化假设。随机预言模型下的安全性证明无法完全等价于现实世界中的安全性。为构建标准模型下可证安全的方案，研究者必须采用具有可证明安全性的密码学原语来替代随机预言机的功能，这导致了根本性的设计差异。

Chen等[15]将两整数格相交法与盆景树格基扩展技术[16]结合，通过控制矩阵扩展的方式绑定文件标识符与数据集，使用LeftExt算法生成陷门。其安全性证明假设敌手进行的是静态选择消息攻击，即敌手在所有签名查询前提交全部消息集合。模拟器通过提前选择标签并利用格基陷门生成应答，避免了随机预言机的需要。然而，这种绑定文件标识符的方式导致了验证矩阵维度的扩展，对于敌手的静态选择消息攻击假设导致其在安全性上仅实现了非适应选择消息攻击下的不可伪造性。针对此问题，Lin等[17]引入了满秩差分哈希函数与格基右扩展（RightExt）算法构造了标准模型下安全的线性同态签名方案，该方案利用一个普通的数字签名来认证文件标识符，再利用基于格的陷门技术来认证数据本身。满秩差分哈希函数确保了任何两个不同标识符的哈希值之差是可逆的，RightExt算法使模拟器能够在没有主陷门的情况下，依然能为大多数文件生成有效的签名，从而应对敌手的查询。

Chen等[18]将紧致签名技术与现有同态签名框架相结合，构造了在标准模型下具有紧致安全性的格基线性同态签名。该方案中提出了右扩展采样（ExtSampleRight）算法，利用右侧矩阵的陷门模拟签名，使模拟器能够应答所有签名查询，最终将任何伪造有效地归约到解决底层格困难问题上，其安全损失仅为常数因子。然而，文献[18]的密钥生成过程较复杂、签名尺寸较大，且仅在选择性标签静态选择明文攻击（U-ST-SCMA, selective-tag static chosen-message-attack）模型下是紧致安全的。因此，Guo等[19]首次在多项式模数下，为伪随机函数、身份加密、数字签名等多种关键密码原语实现了近乎紧的安全规约。

上述方案均局限于单一数据源场景，其核心假设与真实网络中多用户协同签名需求存在矛盾。针对多用户场景，传统聚合签名技术虽可通过压缩验证提升效率，但其静态整合特性无法支持对聚合数据的动态计算。线性同态聚合签名（LHAS, linearly homomorphic aggregate signature）在此背景下实现了突破性创新，在保留了传统聚合签名对多用户签名的高效压缩能力的同时，通过引入同态运算

特性，使聚合后的复合签名仍能作为计算输入参与线性函数运算，并在验证过程中保持数学关系的一致性。Zhang 等[20]基于 GPV 签名[11]与文献[9]中的格基随机化算法，构造了首个格基线性同态聚合签名方案，能够实现二元域上的线性运算，安全性基于格上非齐次最小整数解问题。但该方案中多个用户对应同一公钥，可能会存在安全隐患。Jing[21]在 Wang 等[13]的线性同态签名中融入了聚合特性，同样构造了二元域上的格基线性同态聚合签名方案，其安全性基于最小整数解问题，但该方案的安全性证明依赖随机预言模型，存在理想化假设缺陷。Gu 等[22]设计了一种应用于电子医疗系统的线性同态聚合签名方案，实现了对数据的双重压缩。在安全性方面，基于计算性迪菲－赫尔曼假设证明了随机预言机模型下的不可伪造性，且能抵御合谋攻击，但其基于传统数论难题的设计无法抵御量子计算攻击。

当前线性同态聚合签名的研究仍面临两个方面的核心挑战。一方面，现有方案多基于随机预言模型设计，其安全性证明存在理想化假设缺陷[20-21]，而标准模型下的方案设计能够摆脱对理想哈希函数的依赖，提供更为严格的安全性保障[23]；另一方面，基于传统数论难题的构造难以满足后量子时代的安全需求[22]。

本文针对上述挑战展开研究，构造了标准模型下基于格的线性同态聚合签名。将复合格交空间结构应用于多用户签名聚合场景。通过在该空间内执行原像采样来生成满足模 p 约束的短向量签名。在功能架构上，本文方案实现了多用户密钥隔离与聚合支持。现有同态签名方案多局限于单用户场景[17-18]，而 LHAS 通过 LeftExt 算法将各用户的独立陷门整合为全局公钥矩阵，在不需要用户间共享密钥的前提下，支持来自多个独立用户的签名线性聚合与验证，解决了现有方案在密钥管理与聚合灵活性上的瓶颈。在安全模型上，本文方案在格基线性同态聚合签名中实现了标准模型下的可证明安全。与 Zhang 等[20]及 Jing[21]的方案依赖于随机预言机模型不同，LHAS 通过采用满秩差分哈希函数实现文件标识符与公钥的绑定，规避了理想哈希假设，使安全性建立在标准的短整数解（SIS, short integer solution）困难问题上，提升了安全保证的严格性。

1　预备知识

本文使用粗体小写字母表示向量，如向量 $\boldsymbol{b}$；使用粗体大写字母表示矩阵，如矩阵 $\boldsymbol{A}$；对于整数 $q \geqslant 2$，Z_q 表示模 q 整数环，若 q 为素数，则 F_q 表示模 q 有限域，$Z_q^{n\times m}$ 表示元素取自 Z_q 的 $n \times m$ 维矩阵的集合；$\mathrm{lb}(n)$ 表示以 2 为底、n 为真数的二进制对数运算；将维度相同的向量 $\boldsymbol{e}_1$ 与 $\boldsymbol{e}_2$ 的内积记为 $<\boldsymbol{e}_1,\boldsymbol{e}_2>$；用 $\|\cdot\|$ 表示向量的欧几里得范数，用 $\|\cdot\|_{\max}$ 表示无穷范数；定义矩阵 $\boldsymbol{S}=\{\boldsymbol{s}_1,\cdots,\boldsymbol{s}_k\}$ 的范数为最长列向量的长度，即 $\|\boldsymbol{S}\| = \max_{1\leqslant i\leqslant k}\|\boldsymbol{s}_i\|$；$\tilde{\boldsymbol{S}}$ 表示矩阵 $\boldsymbol{S}$ 经格拉姆–施密特（Gram-Schmidt）正交化后的结果，其 Gram-Schmidt 范数记为 $\|\tilde{\boldsymbol{S}}\|$。若存在常数 c 和整数 N，使对所有 $n \geqslant N$，有 $f(n) \leqslant c\cdot g(n)$，则称 $f(n)$ 为 $O(g(n))$；若存在常数 c'，使 $f(n) = O(g(n)\cdot \mathrm{lb}^{c'}(n))$，则称 $f(n)$ 为 $\tilde{O}(g(n))$；若对所有常数 $c>0$ 和足够大的 n，有 $g(n) \leqslant c\cdot f(n)$，则称 $f(n)$ 为 $\omega(g(n))$。$\mathrm{poly}(n)$ 表示关于 n 的多项式函数；$\mathrm{negl}(n)$ 表示关于 n 的可忽略函数（随 n 增大趋近于 0）；$1-\mathrm{negl}(n)$ 表示压倒性的概率。方案构造过程中涉及的具体符号及其定义如表 1 所示。

格与格上困难问题：格是由一组线性无关向量通过所有整系数线性组合生成的向量集合。具体而言，给定 n 个线性无关向量 $\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$，其生成的 n 维格可表示为

$$L(\boldsymbol{B}) = \left\{\sum_{i=1}^{n} c_i\boldsymbol{b}_i \middle| c_i \in Z\right\} \tag{1}$$

其中，$\boldsymbol{B}$ 是以 $\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$ 为列向量的矩阵，该集合构成格的一组基，基的向量个数 n 称为格的维数。若格中所有向量均为整向量，则称其为整数格。

在密码学应用中，常关注定义于模 q 整数环 Z_q 上的特殊整数格及其陪集。设 $\boldsymbol{A}\in Z_q^{n\times m}$ 为矩阵，$\boldsymbol{y}\in Z_q^n$ 为向量，定义 $\Lambda_q^{\perp}(\boldsymbol{A}) = \left\{\boldsymbol{v}\in Z_q^m | \boldsymbol{A}\boldsymbol{v} \equiv \boldsymbol{0}\left(\mathrm{mod}\, q\right)\right\}$ 为正交对偶格，包含所有与 $\boldsymbol{A}$ 的行向量模 q 正交的向量。定义 $\Lambda_q^{y}(\boldsymbol{A}) = \left\{\boldsymbol{v}\in Z_q^m | \boldsymbol{A}\boldsymbol{v} \equiv \boldsymbol{y}\left(\mathrm{mod}\, q\right)\right\}$ 为陪集格，其也可表示为 $\Lambda_q^{\perp}(\boldsymbol{A}) + \boldsymbol{t}$，其中 $\boldsymbol{t}$ 满足 $\boldsymbol{A}\boldsymbol{t} \equiv \boldsymbol{y}\left(\mathrm{mod}\, q\right)$。

定义 1　SIS 问题[9]。给定均匀随机矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 及参数 n、m、q、β，SIS 问题的目标是找到非零向

表1 符号及其定义

符号	含义	符号	含义
$L(\boldsymbol{B})$	由基矩阵$\boldsymbol{B}$生成的整数格	$\Lambda_q^{\perp}(\boldsymbol{A})$	正交对偶格
$\Lambda_q^{y}(\boldsymbol{A})$	陪集格	$\boldsymbol{T}_{\boldsymbol{A}}$	$\Lambda_q^{\perp}(\boldsymbol{A})$的陷门基
s	离散高斯分布参数	β	SIS问题范数约束
γ	最短独立向量问题的近似因子	λ_n	格$L(\boldsymbol{A})$的第n个连续最小长度
$\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$	离散高斯函数	$D_{\Lambda,s,\boldsymbol{c}}$	格Λ上的离散高斯分布
$\eta_{\epsilon}(\Lambda)$	格的平滑参数	TrapGen	陷门生成算法
SamplePre	原像采样算法	LeftExt	格基左扩展算法
RightExt	格基右扩展算法	LHAS	线性同态聚合签名方案
id	文件标识符	$\boldsymbol{v}_i$	用户u_i签名的消息向量
σ_i	用户u_i的签名	$\boldsymbol{A}_0$	全局公钥矩阵
H	满秩差分哈希函数	$\boldsymbol{G}_{\mathrm{id}}$	哈希矩阵
$\Lambda_1 \cap \Lambda_2$	复合格交空间	$\boldsymbol{M}$	复合校验矩阵

量$\boldsymbol{v} \in Z_q^m$，使$\|\boldsymbol{v}\| \leqslant \beta$且$\boldsymbol{A}\boldsymbol{v} = \boldsymbol{0}(\bmod\ q)$。

定义2 最短独立向量问题（SIVP, shortest independent vector problem）[11]。给定均匀随机矩阵$\boldsymbol{A} \in Z_q^{n \times m}$及其生成的格$L(\boldsymbol{A})$，$\mathrm{SIVP}_{\gamma}$问题的目标是找到$n$个线性无关向量$\boldsymbol{A}\boldsymbol{x}_1,\cdots,\boldsymbol{A}\boldsymbol{x}_n$，使得$\max_{i=1}^{n}\|\boldsymbol{A}\boldsymbol{x}_i\| \leqslant \gamma\lambda_n$，其中$\gamma > 0$为近似因子，$\lambda_n$表示格$L(\boldsymbol{A})$的第$n$个连续最小长度。

引理1 格困难问题的归约关系[11,24]。对于任意多项式有界维数$m = \mathrm{poly}(n)$及任意$\beta > 0$，若模数q满足$q \geqslant \beta \cdot \omega(\sqrt{n\mathrm{lb}(n)})$，则平均情况下的$\mathrm{SIS}_{n,m,q,\beta}$问题至少与最坏情况下的$\mathrm{SIVP}_{\gamma}$具有相同的计算难度，其中近似因子$\gamma = \beta \cdot \tilde{O}(\sqrt{n})$。

格上高斯分布：格上高斯分布是一种在格结构上定义的概率分布，其概率密度函数与连续域高斯函数具有类似形式。早期研究中，格上高斯分布主要用于分析格的基本特性。近年来，其随机性特征被应用于密码学领域，通过掩盖格中陷门结构的统计特性，有效抵御基于公开格信息的攻击。

对于参数$s > 0$和中心$\boldsymbol{c} \in R^m$，定义R^m上的离散高斯函数为

$$\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) = \exp\left(-\pi\left\|\frac{(\boldsymbol{x}-\boldsymbol{c})}{s}\right\|^2\right) \tag{2}$$

格$\Lambda_q^{\perp}(\boldsymbol{A})$上的离散高斯分布的定义为

$$D_{\Lambda_q^{\perp}(\boldsymbol{A}),s,\boldsymbol{c}}(\boldsymbol{x}) = \frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}\left(\Lambda_q^{\perp}(\boldsymbol{A})\right)} \tag{3}$$

其中，$\rho_{s,\boldsymbol{c}}(\Lambda_q^{\perp}(\boldsymbol{A})) = \sum_{\boldsymbol{y} \in \Lambda_q^{\perp}(\boldsymbol{A})}\rho_{s,\boldsymbol{c}}(\boldsymbol{y})$为归一化因子。该分布可视为从参数为$s$、中心为$\boldsymbol{c}$的高斯函数中抽取满足$\boldsymbol{x} \in \Lambda_q^{\perp}(\boldsymbol{A})$的向量的条件分布。

定义3 平滑参数[23]。对于n维格Λ和正实数$\epsilon > 0$，其平滑参数$\eta_{\epsilon}(\Lambda)$定义为最小的正数s，使$\rho_{\frac{1}{s}}\left(\Lambda^* \setminus \{0\}\right) \leqslant \epsilon$，其中$\Lambda^*$为$\Lambda$的对偶格，定义为$\Lambda^* = \left\{\boldsymbol{v} \in R^n \middle| \forall \boldsymbol{w} \in \Lambda, <\boldsymbol{v},\boldsymbol{w}> \in Z\right\}$。对于几乎所有矩阵$\boldsymbol{A} \in Z_q^{n \times m}$，平滑参数满足$\eta_{\epsilon}(\Lambda_q^{\perp}(\boldsymbol{A})) < \omega(\sqrt{\mathrm{lb}(m)})$。平滑参数是格理论中刻画格点分布与高斯函数关系的关键指标，在基于格的密码方案设计中起核心作用。

定义4 满秩差分哈希函数[17]。设$n \in Z$为一正整数，$q \geqslant 2$为素数。若哈希函数H: $\{0,1\}^n \to Z_q^{n \times n}$满足以下2个条件，称$H$为满秩差分哈希函数。

1) 高效可计算性：存在概率多项式时间算法，对任意输入$\mathrm{id} \in \{0,1\}^n$，可计算输出$H(\mathrm{id})$。

2) 满秩差分性：对于所有互不相同的$\mathrm{id},\mathrm{id}' \in \{0,1\}^n$，其输出差值矩阵$\boldsymbol{\Delta} = H(\mathrm{id}) - H(\mathrm{id}')$在模$q$下是满秩的，即$\mathrm{rank}(\boldsymbol{\Delta}) = n$。

满秩差分性是一种强代数性质，其满秩差分性在信息论意义上已蕴含了抗碰撞性，即任何碰撞的存在都会直接破坏该满秩条件。在标准模型下的不可伪造性证明中，满秩差分哈希函数确保了对于任意不同的标识符，其哈希值之差$\boldsymbol{\Delta} = H(\mathrm{id}) -$

$H(\mathrm{id}')$是一个可逆矩阵，从而使模拟器能够从敌手对未知标识符id的伪造签名中，提取出格上SIS问题的解，从而将敌手的攻击优势归约到格难题的困难性上。若使用普通哈希函数，差值矩阵几乎必然不可逆，整个归约证明将无法成立。

引理2　陷门生成**TrapGen**算法[25-26]。给定矩阵维度参数n、m、q，满足$q=\mathrm{poly}(n)$且$m\geqslant 6n\,\mathrm{lb}(q)$，存在一个概率多项式时间算法TrapGen$(m,n,q)$，其输出如下。

1) 一个统计上接近均匀分布的矩阵$\boldsymbol{A}\in Z_q^{n\times m}$。

2) 一个满秩集合$\boldsymbol{S}\subset \Lambda^{\perp}(\boldsymbol{A})$，该集合可通过高效变换转化为格$\Lambda_q^{\perp}(\boldsymbol{A})$的陷门基$\boldsymbol{T}$[27]，且以压倒性的概率满足$\|\boldsymbol{T}\|\leqslant O(n\,\mathrm{lb}(q))$与$\|\tilde{\boldsymbol{T}}\|\leqslant O(\sqrt{n\,\mathrm{lb}(q)})$[28]。

引理3　原像可采样（SamplePre）函数[11]。存在一个概率多项式时间算法$\mathrm{SamplePre}(\boldsymbol{T}_{\boldsymbol{A}},s,\boldsymbol{y})$，其输入为矩阵$\boldsymbol{A}\in\boldsymbol{Z}_q^{n\times m}$、$m$维格$\Lambda_q^{\perp}(\boldsymbol{A})$的基$\boldsymbol{T}_{\boldsymbol{A}}$、向量$\boldsymbol{y}\in R^m$以及参数$s\geqslant\|\boldsymbol{T}_{\boldsymbol{A}}\|\cdot\omega(\sqrt{\mathrm{lb}(m)})$，输出一个分布统计接近(m,n,q)于$D_{\Lambda_q^{\perp}(\boldsymbol{A})+\boldsymbol{y},s}$的向量$\boldsymbol{x}$。

引理4　高斯采样尾部界[29]。对于任意的m维格Λ、Λ的基$\boldsymbol{T}$、向量$\boldsymbol{y}\in R^m$，以及参数s满足$s\geqslant\|\boldsymbol{T}\|\cdot\omega(\sqrt{\mathrm{lb}(m)})$，当从分布$D_{\Lambda,s,\boldsymbol{y}}$中随机采样一个向量$\boldsymbol{x}$时，有：$\Pr[\|\boldsymbol{x}-\boldsymbol{y}\|>s\sqrt{m}:\boldsymbol{x}\leftarrow D_{\Lambda,s,\boldsymbol{y}}]\leqslant\mathrm{negl}(m)$。

引理5　LeftExt算法[9]。对于秩为n的矩阵$\boldsymbol{A}\in Z_q^{n\times m}$，设$\boldsymbol{T}_{\boldsymbol{A}}\in Z^{m\times m}$为格$\Lambda_q^{\perp}(\boldsymbol{A})$的任意基。令$\boldsymbol{A}'\in Z_q^{n\times m'}\boldsymbol{A}'\in Z_q^{n\times m'}$为任意矩阵。存在一个确定性多项式时间算法$\mathrm{LeftExt}(\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{B}=\boldsymbol{A}\|\boldsymbol{A}')$，该算法输出格$\Lambda_q^{\perp}(\boldsymbol{B})\subset Z^{(m+m')\times(m+m')}$的一个基$\boldsymbol{T}_{\boldsymbol{B}}$，使$\|\tilde{\boldsymbol{T}}_{\boldsymbol{B}}\|=\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|$。

引理6　RightExt算法[17,26-27]。存在一个概率多项式时间算法$\boldsymbol{T}_{\boldsymbol{M}}\leftarrow\mathrm{RightExt}(\boldsymbol{T}_{\boldsymbol{B}},\boldsymbol{M}=\boldsymbol{A}\|(\boldsymbol{AR}+\boldsymbol{\Delta B}))$，输入满足以下条件。

1) 矩阵$\boldsymbol{A},\boldsymbol{B}\in Z_q^{n\times m}$，其中$\boldsymbol{B}$列满秩。

2) 随机矩阵$\boldsymbol{R}\in\{-1,1\}^{m\times m}$和满秩矩阵$\boldsymbol{\Delta}\in Z_2^{n\times n}$。

3) 格$\Lambda_q^{\perp}(\boldsymbol{B})$的一组短基$\boldsymbol{T}_{\boldsymbol{B}}\in Z^{m\times m}$，且$\|\boldsymbol{T}_{\boldsymbol{B}}\|$可高效计算。

该算法输出格$\Lambda_q^{\perp}(\boldsymbol{M})$的一组基$\boldsymbol{T}_{\boldsymbol{M}}\in Z^{2m\times 2m}$，满足$\|\boldsymbol{T}_{\boldsymbol{M}}\|\leqslant\|\boldsymbol{T}_{\boldsymbol{B}}\|\cdot m\cdot\omega(\sqrt{\mathrm{lb}(m)})$。

2　形式化定义与安全模型

2.1　形式化定义

定义5　线性同态聚合签名。LHAS由以下4个概率多项式时间算法组成。

1)LHAS.Setup$(1^n,L)$:系统初始化算法，以安全参数n,最大用户数L为输入，输出用户私钥$\{\mathrm{sk}_i\}_{i=1}^{L}$、用户公钥$\{\mathrm{pk}_i\}_{i=1}^{L}$。

2)LHAS.Sign$(\mathrm{pk}_i,\mathrm{sk}_i,\mathrm{id},\boldsymbol{v}_i)$：签名生成算法，以公钥$\mathrm{pk}_i$、私钥$\mathrm{sk}_i$、文件标识符id与消息向量$\boldsymbol{v}_i$为输入，输出签名$\sigma_i$。

3)LHAS.Combine$(\mathrm{id},\{\boldsymbol{v}_i,\sigma_i,c_i\}_{i=1}^{l})$：聚合算法，以文件标识符id、$l\leqslant L$个三元组$\{\boldsymbol{v}_i,\sigma_i,c_i\}$为输入，输出聚合签名$\sigma_{\mathrm{agg}}$和聚合消息$\boldsymbol{v}_{\mathrm{agg}}$。

4)LHAS.Verify$(\{\mathrm{pk}_i,c_i\}_{i=1}^{l},\mathrm{id},\boldsymbol{v}_{\mathrm{agg}},\sigma_{\mathrm{agg}})$：签名验证算法，以公钥集合$\{\mathrm{pk}_i\}_{i=1}^{l}$、文件标识符id、聚合消息$\boldsymbol{v}_{\mathrm{agg}}$、与聚合签名$\sigma_{\mathrm{agg}}$为输入，输出1表示接受，输出0表示拒绝。

2.2　安全模型

定义6　线性同态聚合签名的不可伪造性。在以下交互式游戏中，如果在任意多项式时间内，敌手获胜的优势可以忽略不计，则说明LHAS是适应性选择消息攻击存在性不可伪造（EUF-CMA, existential unforgeability under adaptive chosen-message attack）安全的。

1)初始化阶段：挑战者运行LHAS.Setup算法生成并公开公共参数。

2)公钥模拟阶段：挑战者接收Q个不同的消息集合$\{V_i\}_{i=1}^{Q}$，对于每个$\{V_i\}_{i=1}^{Q}$，为其选择随机的标识符$\{\mathrm{id}_i\}_{i=1}^{Q}$，运行LHAS.Setup算法生成并公开各用户的公钥。

3)签名询问阶段：运行LHAS.Sign算法为敌手提供标签为id_i的待签名消息向量$\{\boldsymbol{v}_{i1},\cdots,\boldsymbol{v}_{il}\}\in V_i$对应的签名。

4)伪造阶段：敌手最终输出伪造$(\{c_j\}_{j=1}^{l},\mathrm{id}^*,\boldsymbol{v}^*,\sigma^*)$，若$1\leftarrow\mathrm{LHAS.Verify}(\{c_j\}_{j=1}^{l},\mathrm{id}^*,\boldsymbol{v}^*,\sigma^*)$，且满足以下条件之一，则敌手获胜：

第一类伪造：对于任意$i\in\{1,\cdots,Q\}$，均有$\mathrm{id}^*\neq\mathrm{id}_i$，且$\boldsymbol{v}^*\neq\vec{0}$。

第二类伪造：存在$i\in\{1,\cdots,Q\}$，使$\mathrm{id}^*=\mathrm{id}_i$，且$\boldsymbol{v}^*\neq\mathrm{LHAS.Combine}(\mathrm{id}_i,\{\boldsymbol{v}_{ij},\sigma_{ij},c_{ij}\}_{j=1}^{l})$。

3 标准模型下基于格的线性同态聚合签名方案

本节基于文献[17]的格基线性同态签名框架，实现了标准模型下的多用户线性同态聚合签名。LHAS引入全局公钥矩阵$\boldsymbol{A}_0=\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_L$，结合LeftExt算法为每个用户生成独立陷门基$\boldsymbol{T}_{\boldsymbol{A}_i}$，从而消除多用户场景下的密钥共享风险；通过设计满秩差分哈希函数H，将文件标识符id嵌入哈希矩阵$\boldsymbol{G}_{\mathrm{id}}=\boldsymbol{U}+H(\mathrm{id})\boldsymbol{V}$（$\boldsymbol{U}$和$\boldsymbol{V}$是随机矩阵），在复合格交空间$\Lambda_1\cap\Lambda_2$中通过原像采样生成满足模$p$约束的短签名，从而规避随机预言假设；聚合过程中，通过线性系数对多用户签名进行加权组合，最终验证时同步检查聚合签名的范数约束、模p一致性及线性关系。此外，证明了方案的正确性，并通过引入不可伪造的聚合签名（AS, aggregate signature）作为安全支撑方案，证明了LHAS在标准模型下的EUF-CMA安全。

3.1 方案构造

设AS为消息空间$\{0,1\}^n$的聚合数字签名方案。构造消息空间为$Z_p^{(L+1)m}$的线性同态聚合签名方案LHAS，具体流程如下。

1)LHAS.Setup$(1^n,L)\rightarrow\left(\{\mathrm{sk}_i,\mathrm{pk}_i\}_{i=1}^{L}\right)$。输入安全参数$n$，最大用户数$L$，执行以下步骤。

①对每个用户u_i，运行$(\mathrm{sk}_i',\mathrm{pk}_i')\leftarrow$AS.KeyGen$(1^n)$生成AS的密钥对。

②选择$p=2$与素数$q=\mathrm{poly}(n)$，满足$q\geqslant\beta\cdot\omega(\sqrt{n(\mathrm{lb})n})$，其中$\beta=13p^2ml(l+1)\sqrt{m\,\mathrm{lb}(q)}\,\mathrm{lb}(m)$。设定$m=6n\,\mathrm{lb}(q)$，高斯参数$s=p\sqrt{m\,\mathrm{lb}(q)}\,\mathrm{lb}(m)$，定义格$\Lambda_1=pZ^{(L+1)m}$。

③对每个用户u_i，运行$(\boldsymbol{A}_i,\boldsymbol{T}_{\boldsymbol{A}_i})\leftarrow$TrapGen$(q,m,n)$，生成校验矩阵$\boldsymbol{A}_i\in Z_q^{n\times m}$及$\Lambda_q^{\perp}(\boldsymbol{A}_i)$的陷门基$\boldsymbol{T}_{\boldsymbol{A}_i}$。

④选择满秩差分哈希函数$H\colon\{0,1\}^n\rightarrow Z_2^{n\times n}$，随机选取$\boldsymbol{U},\boldsymbol{V}\leftarrow Z_q^{n\times m}$与向量$\{\alpha_i\}_{i=1}^{k}\leftarrow Z_q^n$。构造全局公钥矩阵$\boldsymbol{A}_0=\boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_L\in Z_q^{n\times Lm}$。

输出用户u_i的私钥$\mathrm{sk}_i=(\mathrm{sk}_i',\boldsymbol{T}_{\boldsymbol{A}_i})$和公钥$\mathrm{pk}_i=(\mathrm{pk}_i',p,q,s,k,\boldsymbol{A}_i,\boldsymbol{A}_0,\boldsymbol{U},\boldsymbol{V},H,\alpha_i)$。

2)LHAS.Sign$(\mathrm{pk}_i,\mathrm{sk}_i,\mathrm{id},\boldsymbol{v}_i)\rightarrow(\sigma_{\mathrm{id}_i},\sigma_{\boldsymbol{v}_i})$。输入公钥$\mathrm{pk}_i$，私钥$\mathrm{sk}_i$，文件标识符$\mathrm{id}\in\{0,1\}^n$，消息向量$\boldsymbol{v}_i\in\boldsymbol{Z}_p^{(L+1)m}$，执行以下步骤。

①使用AS对id签名得到$\sigma_{\mathrm{id}_i}\leftarrow$AS.Sign$(\mathrm{sk}_i',\mathrm{id})$。

②计算$\boldsymbol{G}_{\mathrm{id}}=\boldsymbol{U}+H(\mathrm{id})\boldsymbol{V}\bmod q$。

③运行$\boldsymbol{T}_{\boldsymbol{M}_i}\leftarrow\mathrm{LeftExt}(\boldsymbol{T}_{\boldsymbol{A}_i},\boldsymbol{M}=\boldsymbol{A}_0\|\boldsymbol{G}_{\mathrm{id}})$，生成$\Lambda_q^{\perp}(\boldsymbol{M})$的基$\boldsymbol{T}_{\boldsymbol{M}_i}$。定义复合格$\Lambda_2=\Lambda_q^{\perp}(\boldsymbol{M})$，其交空间为$\Lambda_1\cap\Lambda_2=p\Lambda_2$，对应短基$\boldsymbol{T}_i=p\boldsymbol{T}_{\boldsymbol{M}_i}$。

④计算$\boldsymbol{y}_i\in Z^{(L+1)m}$，满足$\boldsymbol{y}_i\bmod p=\boldsymbol{v}_i$且$\boldsymbol{M}\boldsymbol{y}_i=\alpha_i\bmod q$。基于引理3生成签名向量$\sigma_{\boldsymbol{v}_i}\leftarrow\mathrm{SamplePre}(\Lambda_1\cap\Lambda_2,\boldsymbol{T}_i,\boldsymbol{y}_i,s)$。输出向量$\boldsymbol{v}_i$的签名$\sigma_i=(\sigma_{\mathrm{id}_i},\sigma_{\boldsymbol{v}_i})$。

3)LHAS.Combine$(\mathrm{id},\{\boldsymbol{v}_i,\sigma_i,c_i\}_{i=1}^{l})\rightarrow\left(\sigma_{\mathrm{agg}},\boldsymbol{v}_{\mathrm{agg}}\right)$。以文件标识符id与三元组$\{\boldsymbol{v}_i,\sigma_i,c_i\}$为输入，其中$l\leqslant L$，$|c_i|\leqslant\dfrac{p}{2}$，计算线性组合$\sigma_{\mathrm{agg}}=\sum_{i=1}^{l}c_i\sigma_{\boldsymbol{v}_i}$与$\boldsymbol{v}_{\mathrm{agg}}=\sum_{i=1}^{l}c_i\boldsymbol{v}_i$。

4)LHAS.Verify$(\{\mathrm{pk}_i,c_i\}_{i=1}^{l},\mathrm{id},\boldsymbol{v}_{\mathrm{agg}},\sigma_{\mathrm{agg}})\rightarrow(0,1)$。以公钥集合$\{\mathrm{pk}_i\}_{i=1}^{l}$、系数$\{c_i\}$、标识符id，聚合消息$\boldsymbol{v}_{\mathrm{agg}}$，聚合签名$\sigma_{\mathrm{agg}}$为输入，验证以下内容。

①$1\leftarrow$AS.Verify$(\{\mathrm{pk}_i'\}_{i=1}^{l},$AS.Combine$(\mathrm{id},\{\sigma_{\mathrm{id}_i},c_i\}_{i=1}^{l}))$。

②$\|\sigma_{\mathrm{agg}}\|\leqslant l\cdot\dfrac{p}{2}s\sqrt{(L+1)m}$。

③$\sigma_{\mathrm{agg}}\bmod p=\boldsymbol{v}_{\mathrm{agg}}\bmod p$。

④$\boldsymbol{M}\sigma_{\mathrm{agg}}\bmod q=\sum_{i=1}^{l}c_i\alpha_i\bmod q$。

若以上内容均成立，则输出1表示接受签名；否则，输出0表示拒绝签名。

3.2 正确性

1) 根据聚合数字签名方案AS=(AS.KeyGen, AS.Sign, AS.Combine, AS.Verify)的正确性，有$1\leftarrow$AS.Verify$(\{\mathrm{pk}_i'\}_{i=1}^{l},$AS.Combine$(\mathrm{id},\{\sigma_{\mathrm{id}_i},c_i\}_{i=1}^{l}))$。

2) 根据引理2与引理5，有$\|\boldsymbol{T}_{\boldsymbol{A}_i}\|\leqslant O(\sqrt{n\,\mathrm{lb}(q)})$与$\|\boldsymbol{T}_{\boldsymbol{M}}\|=\|\boldsymbol{T}_{\boldsymbol{A}_i}\|$，因此$s=p\sqrt{m\,\mathrm{lb}(q)}\,\mathrm{lb}(m)$满足引理4的应用条件，除可忽略不计的概率外，$\|\sigma_{\boldsymbol{v}_i}\|\leqslant s\sqrt{(L+1)m}$成立，且对所有$i$均有$|c_i|\leqslant\dfrac{p}{2}$，因此

$$\left\|\sigma_{\text{agg}}\right\|=\left\|\sum_{i=1}^{l}c_i\sigma_{\boldsymbol{v}_i}\right\|\leqslant l\cdot\frac{p}{2}\cdot\max_{1\leqslant i\leqslant k}\left\|\sigma_{\boldsymbol{v}_i}\right\|=$$

$$l\cdot\frac{p}{2}\cdot s\sqrt{(L+1)m}\tag{4}$$

3)对于每个$i\in\{1,\cdots,l\}$，由于$\sigma_{\boldsymbol{v}_i}\in(\Lambda_1\cap\Lambda_2)+\boldsymbol{y}_i$，故$\sigma_{\boldsymbol{v}_i}\bmod p=\boldsymbol{v}_i$，且$\boldsymbol{M}\sigma_{\boldsymbol{v}_i}\bmod q=\alpha_i$。因此

$$\sigma_{\text{agg}}\bmod p=\sum_{i=1}^{l}c_i\sigma_{\boldsymbol{v}_i}\bmod p=$$

$$\sum_{i=1}^{l}c_i\boldsymbol{v}_i\bmod p=\boldsymbol{v}_{\text{agg}}\bmod p\tag{5}$$

并且有

$$\boldsymbol{M}\sigma_{\text{agg}}\bmod q=\sum_{i=1}^{l}c_i\boldsymbol{M}\sigma_{\boldsymbol{v}_i}\bmod q=\sum_{i=1}^{l}c_i\alpha_i\bmod q\tag{6}$$

3.3　不可伪造性

定理1　LHAS方案的不可伪造性。如果AS是一个不可伪造的聚合数字签名，且当$\beta=13p^2ml(l+1)\sqrt{m\,\text{lb}(q)}\,\text{lb}(m)$时，$\text{SIS}_{n,m,q,\beta}$问题是困难的，那么在标准模型下，LHAS是EUF-CMA安全的。

具体而言，设$\mathcal{A}$是一个多项式时间敌手，最多向挑战者$\mathcal{C}$发起Q次不同的签名查询。在伪造阶段，如果$\mathcal{A}$以概率ε_1生成第一类伪造，那么$\mathcal{C}$能够构造多项式时间算法$\mathcal{B}_1$以概率ε_1生成聚合数字签名方案AS的伪造。如果$\mathcal{A}$以概率ε_2生成第二类伪造，那么$\mathcal{C}$能够构造多项式时间算法$\mathcal{B}_2$以概率$\frac{\varepsilon_2}{Q}$解决一个随机的$\text{SIS}_{n,m,q,\beta}$问题实例。

证明　在不可伪造性交互式证明实验中，挑战者$\mathcal{C}$接收到Q个不同的消息集合$\{V_i\}_{i=1}^{Q}$，每个V_i包括l个消息向量$\boldsymbol{v}_{i1},\cdots,\boldsymbol{v}_{il}\in Z_p^{(l+1)m}$，并为每个$V_i$选择一个文件标识符$\text{id}_i$。设$\vec{\sigma}_i=(\sigma_{i1},\cdots,\sigma_{il})$为发送给敌手$\mathcal{A}$的$V_i$的签名。本文假设$\mathcal{A}$最终输出一个有效的伪造$(\{c_j\}_{j=1}^{l},\text{id}^*,\boldsymbol{v}^*,\sigma^*)$，满足$1\leftarrow\text{LHAS.Verify}(\{c_j\}_{j=1}^{l},\text{id}^*,\boldsymbol{v}^*,\sigma^*)$。该伪造属于以下列出的类型之一。

第一类伪造：对于任意$i\in\{1,\cdots,Q\}$，均有$\text{id}^*\neq\text{id}_i$，且$\boldsymbol{v}^*\neq\boldsymbol{0}$。

第二类伪造：存在$i\in\{1,\cdots,Q\}$，使$\text{id}^*=\text{id}_i$，且$\boldsymbol{v}^*\neq\text{LHAS.Combine}(\text{id}_i,\{\boldsymbol{v}_{ij},\sigma_{ij},c_{ij}\}_{j=1}^{l})$。

1)初始化阶段：给定随机的$\text{SIS}_{n,m,q,\beta}$挑战矩阵$\boldsymbol{A}\in Z_q^{n\times m}$。$\mathcal{C}$运行LHAS.Setup算法，生成素数$p,q$、高斯参数$s$与满秩差分哈希函数$H:\{0,1\}^n\leftarrow Z_2^{n\times n}$，公开公共参数$(p,q,s,l,H)$。

2)公钥模拟阶段：挑战者$\mathcal{C}$在接收到Q个不同消息集合$\{V_i\}_{i=1}^{Q}$后，为每个$\{V_i\}_{i=1}^{Q}$选择一个随机的标识符$\{\text{id}_i\}_{i=1}^{Q}\in\{0,1\}^n$。运行AS.KeyGen算法，生成$l$个用户$\{u_j\}_{j=1}^{l}$在聚合签名方案中的$l$对密钥$\{\text{sk}_j',\text{pk}_j'\}_{j=1}^{l}$。运行算法$(\boldsymbol{B}_j,\boldsymbol{T}_{\boldsymbol{B}_j})\leftarrow\text{TrapGen}(q,m,n)$生成$l$个矩阵$\boldsymbol{B}_j\in Z_q^{n\times m}$与$\Lambda_q^{\perp}(\boldsymbol{B}_j)$的基$\boldsymbol{T}_{\boldsymbol{B}_j}$，使$\|\boldsymbol{T}_{\boldsymbol{B}_j}\|\leqslant O(\sqrt{n\,\text{lb}(q)})$，定义$\boldsymbol{B}=(\boldsymbol{B}_1\|\cdots\|\boldsymbol{B}_l)\in Z_q^{n\times lm}$，使用$\text{LeftExt}(\boldsymbol{T}_{\boldsymbol{B}_j},\boldsymbol{B}=\boldsymbol{B}_1\|\cdots\|\boldsymbol{B}_l)$算法计算$\Lambda_q^{\perp}(\boldsymbol{B})$的基$\boldsymbol{T}_{\boldsymbol{B}}$。$\mathcal{C}$猜测标识符$\text{id}'\in\{\text{id}_1,\cdots,\text{id}_Q\}$，选择矩阵$\boldsymbol{R}_{\boldsymbol{U}'}\in Z_{\{-1,1\}}^{m\times lm}$，并定义$\boldsymbol{U}'=\boldsymbol{A}\boldsymbol{R}_{\boldsymbol{U}'}-H(\text{id}')\boldsymbol{B}$与$\boldsymbol{V}=\boldsymbol{B}$。假设标识符为$\text{id}'$的消息集合$V'$包含向量$\{\boldsymbol{v}_j'\}_{j=1}^{l}$。对于每个$j\in\{1,\cdots,l\}$，选择随机向量$\boldsymbol{y}_j'\in\Lambda_1+\boldsymbol{v}_j'$，并计算$\boldsymbol{w}_j'\leftarrow\text{SamplePre}(\Lambda_1,\boldsymbol{T}_{\Lambda_1},\boldsymbol{y}_j',s)$，其中$\boldsymbol{T}_{\Lambda_1}=\{p\boldsymbol{e}_i\}_{i=1}^{(l+1)m}$是$\Lambda_1$的一个短基。对于每个$j\in\{1,\cdots,l\}$，定义$\alpha_j=(\boldsymbol{A}\|\boldsymbol{G}_{\text{id}'})\boldsymbol{w}_j'$，其中$\boldsymbol{G}_{\text{id}'}=\boldsymbol{U}'+H(\text{id}')\boldsymbol{V}$。最终，公开公钥$\{\text{pk}_j',\boldsymbol{A},\boldsymbol{U}',\boldsymbol{V},\boldsymbol{B}_j,\alpha_j\}_{j=1}^{l}$。

3)签名询问阶段：对于待签名消息向量$\{\boldsymbol{v}_{i1},\cdots,\boldsymbol{v}_{il}\}\in V_i$，如果$\text{id}_i\neq\text{id}'$，$\mathcal{C}$计算$\boldsymbol{G}_{\text{id}_i}=\boldsymbol{U}_i+H(\text{id}_i)\boldsymbol{V}=\boldsymbol{A}\boldsymbol{R}_{\boldsymbol{U}_i}+\boldsymbol{\Delta}_i\boldsymbol{B}$，其中$\boldsymbol{\Delta}_i=H(\text{id}_i)-H(\text{id}')$为满秩矩阵，然后计算$\sigma_{\text{id}_{ij}}\leftarrow\text{sign}(\text{sk}_j',\text{id}_i)$，运行引理6中的算法$\boldsymbol{T}_{\boldsymbol{M}_i}\leftarrow\text{RightExt}(\boldsymbol{T}_{\boldsymbol{B}},\boldsymbol{M}_i=\boldsymbol{A}\|(\boldsymbol{A}\boldsymbol{R}_{\boldsymbol{U}_i}+\boldsymbol{\Delta}_i\boldsymbol{B}),\boldsymbol{R}_{\boldsymbol{U}_i},\boldsymbol{\Delta}_i,\boldsymbol{B})$以获得$\Lambda_q^{\perp}(\boldsymbol{M}_i)$的对应基$\boldsymbol{T}_{\boldsymbol{M}_i}$，定义$\Lambda_2=\Lambda_q^{\perp}(\boldsymbol{M}_i)$，则$\boldsymbol{T}_i=p\boldsymbol{T}_{\boldsymbol{M}_{ij}}$是$\Lambda_1\cap\Lambda_2=p\Lambda_2$的一个基。对于所有$j\in\{1,\cdots,l\}$，计算$\boldsymbol{y}_{ij}\in Z^{(l+1)m}$，使$\boldsymbol{y}_{ij}\bmod p=\boldsymbol{v}_{ij}$且$\boldsymbol{M}_i\boldsymbol{y}_{ij}=\alpha_j\bmod q$。最后，计算$\sigma_{\boldsymbol{v}_{ij}}\leftarrow\text{SamplePre}(\Lambda_1\cap\Lambda_2,\boldsymbol{T}_i,\boldsymbol{y}_{ij},s)$并返回$\{\boldsymbol{v}_{i1},\cdots,\boldsymbol{v}_{il}\}\in V_i$对应的签名$\{\sigma_{\text{id}_{ij}},\sigma_{\boldsymbol{v}_{ij}}\}_{j=1}^{l}$。

如果$\text{id}_i=\text{id}'$，此时$\boldsymbol{G}_{\text{id}'}=\boldsymbol{U}'+H(\text{id}')\boldsymbol{V}=\boldsymbol{A}\boldsymbol{R}_{\boldsymbol{U}'}$。$\mathcal{C}$计算$\boldsymbol{M}'=\boldsymbol{A}\|\boldsymbol{G}_{\text{id}'}$，并定义$\Lambda_2=\Lambda_q^{\perp}(\boldsymbol{M}')$。对于所有$j\in\{1,\cdots,l\}$，计算$\sigma_{\text{id}_j'}\leftarrow\text{AS.Sign}(\text{sk}_j',\text{id}')$，并设$\sigma_{\boldsymbol{v}_j'}=\boldsymbol{w}_j'$，最终返回$\{\boldsymbol{v}_1',\cdots,\boldsymbol{v}_l'\}\in V'$对应的签名$\{\sigma_{\text{id}_j'},\sigma_{\boldsymbol{v}_j'}\}_{j=1}^{l}$。

4)伪造阶段：$\mathcal{A}$输出一个有效伪造$(\{c_j\}_{j=1}^{l},\text{id}^*,\boldsymbol{v}^*,\sigma^*)$，满足$1\leftarrow\text{LHAS.Verify}(\{c_j\}_{j=1}^{l},\text{id}^*,\boldsymbol{v}^*,\sigma^*)$。

当$\mathcal{A}$以概率ε_1输出第一类伪造时，对于任意

$i \in \{1,\cdots,Q\}$，均有 $\mathrm{id}^* \neq \mathrm{id}_i$，且 $\boldsymbol{v}^* \neq \boldsymbol{0}$。此时，$\sigma_{\mathrm{id}^*}$ 从未被 $\mathcal{A}$ 查询过。因此，$\mathcal{C}$ 直接返回 σ^* 中的 σ_{id^*} 作为底层聚合签名方案 AS 中的关于 id^* 的聚合签名伪造，这意味着 $\mathcal{C}$ 能够以概率 ε_1 破坏聚合签名方案 AS 的不可伪造性。

当 $\mathcal{A}$ 以概率 ε_2 输出第二类伪造时，存在 $i \in \{1,\cdots,Q\}$，使 $\mathrm{id}^* = \mathrm{id}_i$，且 $\boldsymbol{v}^* \neq \mathrm{LHAS.Combine}(\mathrm{id}_i, \{\boldsymbol{v}_{ij},\sigma_{ij},c_{ij}\}_{j=1}^{l})$。此时，$P(\mathrm{id}^* = \mathrm{id}_i) = \dfrac{1}{Q}$。根据 LHAS.Combine 算法的正确性，有

$$\sum_{j=1}^{l} c_j'\boldsymbol{M}'\sigma_{\boldsymbol{v}_j'} = \sum_{j=1}^{l} c_j'\alpha_j = \boldsymbol{M}'\sigma_{\boldsymbol{v}^*} \tag{7}$$

这表明

$$(\boldsymbol{A}\|\boldsymbol{A}\boldsymbol{R}_{U'})\left(\sum_{j=1}^{l} c_j'\sigma_{\boldsymbol{v}_j'} - \sigma_{\boldsymbol{v}^*}\right) = \boldsymbol{0} \tag{8}$$

由于 $\boldsymbol{v}^* \neq \mathrm{LHAS.Combine}(\mathrm{id}', \{\boldsymbol{v}_j',\sigma_j',c_j'\}_{j=1}^{l})$，则 $\boldsymbol{v}^* \neq \sum_{j=1}^{l} c_j'\boldsymbol{v}_j'$。验证条件③（$\sigma_{\mathrm{agg}} \bmod p = \boldsymbol{v}_{\mathrm{agg}} \bmod p$）意味着 $\sum_{j=1}^{l} c_j'\sigma_{\boldsymbol{v}_j'} - \sigma_{\boldsymbol{v}^*} \bmod p = \sum_{j=1}^{l} c_j'\boldsymbol{v}_j' - \boldsymbol{v}^* \neq \boldsymbol{0}$，因此 $\sum_{j=1}^{l} c_j'\sigma_{\boldsymbol{v}_j'} - \sigma_{\boldsymbol{v}^*} \neq \boldsymbol{0}$。设定 $\sum_{j=1}^{l} c_j'\sigma_{\boldsymbol{v}_j'} - \sigma_{\boldsymbol{v}^*} = (\hat{\boldsymbol{\sigma}}_1^{\mathrm{T}},\hat{\boldsymbol{\sigma}}_2^{\mathrm{T}})^{\mathrm{T}} \in Z_q^{(l+1)m}$，其中 $\hat{\boldsymbol{\sigma}}_1^{T} \in Z_q^{m}$、$\hat{\boldsymbol{\sigma}}_2^{T} \in Z_q^{lm}$。则：

$$(\boldsymbol{A}\|\boldsymbol{A}\boldsymbol{R}_{U'})\left(\sum_{j=1}^{l} c_j'\sigma_{\boldsymbol{v}_j'} - \sigma_{\boldsymbol{v}^*}\right) = \boldsymbol{A}(\hat{\boldsymbol{\sigma}}_1 + \boldsymbol{R}_{U'}\hat{\boldsymbol{\sigma}}_2) = \boldsymbol{0} \tag{9}$$

验证条件②（$\|\sigma_{\mathrm{agg}}\| \leqslant l \cdot \dfrac{p}{2} s\sqrt{(L+1)m}$）表明 $\sum_{j=1}^{l} c_j'\sigma_{\boldsymbol{v}_j'}$ 和 $\sigma_{\boldsymbol{v}}^*$ 的长度都小于 $l \cdot \dfrac{p}{2} \cdot s\sqrt{(l+1)m}$，因此 $\|\hat{\sigma}_1\| \leqslant \left\| \sum_{j=1}^{l} c_j'\sigma_{\boldsymbol{v}_j'} - \sigma_{\boldsymbol{v}^*} \right\| \leqslant l \cdot p \cdot s\sqrt{(l+1)m}$。类似地，$\|\hat{\sigma}_2\| \leqslant l \cdot p \cdot s\sqrt{(l+1)m}$。根据文献[30]，由于 $\boldsymbol{R}_{U'} \in Z_{\{-1,1\}}^{m \times lm}$，因此 $\|\boldsymbol{R}_{U'}\| \leqslant 12\sqrt{(l+1)m}$，则

$$\|\hat{\sigma}_1 + \boldsymbol{R}_{U'}\hat{\sigma}_2\| \leqslant \|\hat{\sigma}_1\| + \|\boldsymbol{R}_{U'}\hat{\sigma}_2\| \leqslant 13 \cdot m \cdot l \cdot p \cdot s \cdot (l+1) \leqslant \beta \tag{10}$$

因此，$\mathcal{C}$ 可以以概率 $\dfrac{\varepsilon_2}{Q}$ 提取出 $\mathrm{SIS}_{n,q,m,\beta}$ 的有效解 $(\hat{\sigma}_1 + \boldsymbol{R}_{U'}\hat{\sigma}_2)$。由于 $\mathrm{SIS}_{n,q,m,\beta}$ 在参数 n,q,β 满足 $q \geqslant \beta \cdot \omega(\sqrt{n\,\mathrm{lb}(n)})$ 时，其最坏情况下的求解优势 ε_2 为可忽略函数 $\mathrm{negl}(n)$，因此敌手的伪造优势 $\dfrac{\varepsilon_2}{Q}$ 仍为可忽略值。这表明在标准模型下，敌手不存在多项式时间内的有效攻击策略，其成功优势被严格绑定到格上困难问题的固有难度。证毕。

3.4 参数选取与可行性分析

在实际部署中，方案的参数需在理论安全归约与工程效率之间取得平衡。本节基于典型安全需求分析参数选取的合理性，并量化评估公钥尺寸、签名长度与计算效率，以证明方案在实际应用中的可行性。方案的安全性规约于 n 维格上 $\mathrm{SIS}_{n,m,q,\beta}$ 问题的困难性。为实现 128 bit 经典安全级别，设置基础安全参数 $n = 512$，设定系统最大支持用户数 $L = 10$，设定素数 $q \approx 2^{23}$，满足 $q = \mathrm{poly}(n)$ 且 $q \geqslant \beta \cdot \omega(\sqrt{n\,\mathrm{lb}(n)})$ 的理论要求，此模数量级与许多已标准化的格密码方案相当，在现有硬件平台上具备计算可行性。取消息模数 $p = 2$，以支持二进制域上的线性运算，适用于多数网络编码与分布式计算场景，根据引理 2，设定 $m = 6n\,\mathrm{lb}(q) \approx 70\,656$。高斯参数 s 需满足 $s \geqslant \|\boldsymbol{T}_{\boldsymbol{A}_i}\| \cdot \omega(\sqrt{\mathrm{lb}(m)})$ 从而确保 SamplePre 算法的统计安全性。基于引理 2 及引理 5，$\|\boldsymbol{T}_{\boldsymbol{A}_i}\|$ 的 Gram-Schmidt 范数上界为 $O(\sqrt{n\,\mathrm{lb}(q)})$，综合考量可取 $s = p \cdot \sqrt{m\,\mathrm{lb}(q)} \cdot \mathrm{lb}(m) \approx 41\,900$。

单个用户公钥 $\boldsymbol{A}_i \in \mathbb{Z}_q^{n \times m}$ 存储开销为 $n \cdot m \cdot \mathrm{lb}(q)$bit，代入 $n = 512, m = 70\,656, \mathrm{lb}(q) = 23$，约为 $512 \times 70\,656 \times 23\,\mathrm{bits} \approx 104\,\mathrm{MB}$。公钥尺寸较大，但可使用文献[28]中的种子扩展技术进行优化，通过存储一个短种子，利用可扩展输出函数生成公钥矩阵 $\boldsymbol{A}_i$，可将存储和传输开销从 $O(nm)$ 降至 $O(n)$，代价是增加少量的本地计算开销。用户 u_i 对向量 $\boldsymbol{v}_i$ 的签名 $\sigma_{\boldsymbol{v}_i}$ 是一个高维短向量，采样自复合格交空间，其维度为 $(L+1)m = 11 \times 70\,656 = 777\,216$。根据引理 4，采样所得向量的欧几里得范数以压倒性概率满足 $\|\sigma_{\boldsymbol{v}_i}\| \leqslant s\sqrt{(L+1)m} \approx 3.69 \times 10^6$。因此，单个签名 $\sigma_{\boldsymbol{v}_i}$ 的尺寸约为 $777\,216 \times 26\,\mathrm{bit} \approx 2.47\,\mathrm{MB}$。聚合签名 σ_{agg} 的尺寸与此相同。此签名尺寸适用于对数据完整性要求较高，但带宽非首要瓶颈的场景。

验证阶段的核心计算是校验等式 $\boldsymbol{M}\sigma_{\mathrm{agg}} \equiv \sum_{i=1}^{l} c_i\alpha_i \bmod q$，其中复合矩阵 $\boldsymbol{M} = \boldsymbol{A}_0\|\boldsymbol{G}_{\mathrm{id}} \in Z_q^{n \times (Lm+m)}$。一次完整的矩阵–向量乘法约需 $n \times (L+1)m =$

512 × 777 216 ≈ 398 百万次模 q 运算。此计算虽密集，但具有良好的并行性，可通过 GPU 或现场可编程门阵列（FPGA）进行加速[30]，以满足实际应用中的延迟要求。

本文提出的 LHAS 方案在理论安全归约下，为实现 128 bit 安全级别，其基础参数设定会导致较大的初始存储与计算开销。然而，通过采用种子扩展技术压缩公钥、并利用硬件加速验证过程，该方案在军事通信、金融分布式账本、关键基础设施的远程认证等特定高安全需求场景中具备工程可行性。其核心价值在于实现了标准模型下的多用户线性同态聚合签名，在保证安全性的同时，提供了完整的功能支持。后续工作将聚焦于构造优化以降低参数维度，以及软硬件协同设计以提升实用效率。

4　性能分析

4.1　数值理论分析

本节将从理论层面，对本文方案的相关存储开销和计算复杂度进行数值化分析与对比。首先量化计算本文方案中公钥矩阵、签名向量等核心元素的比特大小，明确其存储需求。随后，将本文方案与文献[8, 13, 17-18, 20-21]等代表性工作进行横向对比，重点聚焦于公钥尺寸、签名长度等关键指标。通过对比，旨在突出说明本文方案在标准模型安全性与多用户支持 2 个核心优势下，所付出的理论开销处于何种量级，以及与随机预言机模型下的方案相比是否存在差距，从而在理论层面确立方案的效率定位。为统一比较基准，设定模数 $p = 2$，对各代表性文献的性能特征分析如下。

文献[8]借助中国剩余定理构建复合格 $\Lambda_{2q}^{q\cdot\nu}(\boldsymbol{A})$，并通过模 2 分量实现消息绑定，在随机预言模型下实现了高效的单用户签名。然而，该方案公钥尺寸为 $nm + nm\,\mathrm{lb}\,(q)$，签名尺寸为 $2m + 2m\,\mathrm{lb}\,(q)$，在同类方案中显著偏大，且缺乏多用户扩展机制，难以适用于分布式场景。文献[13]利用矩阵向量乘法的同态特性优化了签名长度，将公钥尺寸降低至 $nm\,\mathrm{lb}\,(q)$，签名尺寸缩减为 $m\,\mathrm{lb}\,(q)$，但仍未突破单用户场景的限制，其安全性证明依赖于随机预言机假设，在实际部署中面临理想化模型带来的安全风险。文献[17-18]虽在标准模型下实现了单用户线性同态签名，摆脱了对随机预言机的依赖，但其格基结构固定，缺乏灵活的多用户聚合能力，难以适应多节点协同的网络环境。

在支持多用户聚合的方案中，文献[20]采用共享公钥机制，公钥尺寸为 $2nm\,\mathrm{lb}\,(q)$，签名尺寸为 $2m\,\mathrm{lb}\,(q)$。然而，该设计存在合谋攻击风险，且安全性仍建立在随机预言模型之上，未能实现安全性与多功能性之间的有效平衡。文献[21]通过独立公钥级联策略支持多用户场景，公钥尺寸为 $nm\,\mathrm{lb}\,(q)$，签名尺寸为 $m\,\mathrm{lb}\,(q)$，验证开销与文献[13]相当，但其安全证明同样局限于随机预言框架，在安全要求严格的场景中适用性不足。

如表 2 所示，上述方案在安全模型与功能支持方面各有取舍，尚无法同时满足标准模型下的安全性要求与多用户动态聚合需求。本文方案在公钥尺寸（$nm\,\mathrm{lb}\,(q)$）与签名尺寸（$m\,\mathrm{lb}\,(q)$）方面与文献[13,21]保持同一量级，但在实现标准模型下安全性证明的同时，具备多用户线性同态聚合能力。相较于文献[8,13]等随机预言模型下的单用户方案，本文方案通过构建全局公钥矩阵 $\boldsymbol{A}_0 = \boldsymbol{A}_1\|\cdots\|\boldsymbol{A}_L$ 与复合格交空间 $\Lambda_1 \cap \Lambda_2$，在摒弃理想哈希假设的前提下实现了多用户签名的有效组合；与文献[17]等标准模型下单用户方案相比，引入格基扩展与独立陷门生成机制，突破了固定矩阵结构对多用户扩展的限制；相较于文献[20-21]等多用户随机预言模型方案，采用满秩差分哈希函数将文件标识符嵌入验证矩阵 $\boldsymbol{G}_{\mathrm{id}} = \boldsymbol{U} + H(\mathrm{id})\boldsymbol{V}$，既规避了合谋风险，又不依赖随机预言假设，从而在安全性上更具优势。

4.2　方案实验分析

本节将聚焦于方案的实践性能，通过具体的实验数据展示各核心算法的运行效率。通过与理论分析的相互印证，旨在论证方案在实际计算平台上的可行性，并为后续的优化工作提供数据支撑。实验平台选用 Intel Corei7-12800HX 处理器（基频 3.4 GHz，睿频至 4.8 GHz）和 32 GB RAM，运行 Ubuntu 20.04 LTS 操作系统。所有代码均使用 C 语言实现，并通过 GCC 9.4.0 编译器启用 O2 优化级别进行编译。基于实现复杂性与实验成本的综合考量，选取 96 bit 经典安全级别，在保障方案安全性的同时，能够控制密钥与签名的存储开销，降低原型系统实现的工程门槛，从而更清晰地展示方案核心机制的性能特征。具体参数配置如表 3 所示。为了全面评估方案的可扩展性，测试了不同用户规模下的性能表现。实验记录了方

表2 各方案性能对比

方案	公钥尺寸	签名尺寸	安全模型	支持多用户	验证开销
文献[8]	$nm + nm\,\mathrm{lb}(q)$	$2m + 2m\,\mathrm{lb}(q)$	随机预言模型	否	$nm^2 + 2nm^2\,\mathrm{lb}(q)^2 + nm^2\,\mathrm{lb}(q)^2$
文献[13]	$nm\,\mathrm{lb}(q)$	$m\,\mathrm{lb}(q)$	随机预言模型	否	$nm^2\,\mathrm{lb}(q)^2$
文献[17]	$2nm\,\mathrm{lb}(q)$	$2m\,\mathrm{lb}(q)$	标准模型	否	$4nm^2\,\mathrm{lb}(q)^2$
文献[18]	$5nm\,\mathrm{lb}(q)$	$2m\,\mathrm{lb}(q)$	标准模型	否	$10nm^2\,\mathrm{lb}(q)^2$
文献[20]	$2nm\,\mathrm{lb}(q)$	$2m\,\mathrm{lb}(q)$	随机预言模型	是	$4nm^2\,\mathrm{lb}(q)^2$
文献[21]	$nm\,\mathrm{lb}(q)$	$m\,\mathrm{lb}(q)$	随机预言模型	是	$nm^2\,\mathrm{lb}(q)^2$
本文方案	$nm\,\mathrm{lb}(q)$	$m\,\mathrm{lb}(q)$	标准模型	是	$nm^2\,\mathrm{lb}(q)^2$

案在不同用户规模下，其初始化（Setup）、签名（Sign）、组合（Combine）和验证（Verify）4个核心阶段的时间开销。Setup阶段作为计算最密集的部分，其时间开销的线性增长趋势主要源于需要为每个用户独立执行陷门生成算法生成校验矩阵$\boldsymbol{A}_i$和对应的格基陷门$\boldsymbol{T}_{\boldsymbol{A}_i}$。在具体实现过程中，采用了Alwen等[26]提出的高效陷门生成技术，利用优化的高斯采样器快速构造具有良好几何性质的短基，确保在用户数增加时仍能维持可接受的初始化时间。

表3 实验参数设置

参数	符号	取值	参数意义
安全参数	n	384	公钥矩阵行数
模数	q	8 388 593	23 bit素数模数
消息模数	p	2	二进制域运算支持
格维数	m	5 3000	公钥矩阵列数
高斯参数	s	31 400	$D_{\Lambda,s,\boldsymbol{y}}$的标准差
预采样参数	ζ	83 290	原像采样目标分布的标准差
最大用户数	L	10	多用户支持上限

Sign阶段的效率是整个方案的关键瓶颈。对于每个用户的签名操作，算法首先通过满秩差分哈希函数H计算$\boldsymbol{G}_{\mathrm{id}} = \boldsymbol{U} + H(\mathrm{id})\boldsymbol{V}$，建立文件标识符与验证矩阵的绑定关系。随后利用格基扩展算法，以用户陷门$\boldsymbol{T}_{\boldsymbol{A}_i}$为输入，扩展生成复合格$\Lambda_2 = \Lambda_q^{\perp}(\boldsymbol{M})$的基$\boldsymbol{T}_{\boldsymbol{M}}$，其中复合矩阵$\boldsymbol{M} = \boldsymbol{A}_0 \| \boldsymbol{G}_{\mathrm{id}}$。此步骤通过一系列矩阵操作和基扩展完成，确保输出的基质量与输入陷门相当，最后在$\Lambda_1 \cap \Lambda_2$中执行原像采样算法。实验过程中使用了基于克莱因（Klein）原像采样算法[31]的改进版高斯采样器，其内部使用第三代安全散列算法（SHA-3）扩展输出作为随机源，并通过逆变换法生成满足离散高斯分布的整数值，这一设计保证了采样过程的安全性和效率。

Combine阶段时间开销，整体维持在较低水平。聚合操作本质上是多个签名向量在模p下的带权线性组合，即$\sigma_{\mathrm{agg}} = \sum_{i=1}^{l} c_i \sigma_{\boldsymbol{v}_i}$。由于$p = 2$的特殊性质，该操作可进一步优化为按位的异或与条件加法，计算开销极低，这使得方案特别适合需要频繁进行签名聚合的大规模分布式应用场景。

Verify阶段的时间开销呈现近似线性的增长趋势。验证过程的核心计算负担在于校验等式$\boldsymbol{M}\sigma_{\mathrm{agg}} \equiv \sum c_i \alpha_i \bmod q$是否成立。实验过程针对大矩阵向量乘法进行了专门优化，将高维矩阵$\boldsymbol{M}$按块加载到内存中，并利用单指令多数据流（SIMD, single instruction multiple data）技术对模乘加操作进行并行加速。

实验数据展示了方案的整体性能特征，如图1所示，其中，左纵轴表示Setup与Sign阶段的时间，右纵轴则表示Combine与Verify阶段的时间，以更清晰地展示不同阶段的时间量级差异。系统建立时间与用户数呈线性增长关系，主要耗时在于陷门生成，这在Setup阶段是可以接受的。签名时间对单个用户而言是主要开销，其核心瓶颈在于高维格上的高斯原像采样，这也是未来优化的重点方向。验证时间虽然随着聚合用户数的增加而线性增长，但由于其高度并行化的特性，在实际部署中可通过GPU或专用硬件获得数量级的加速。

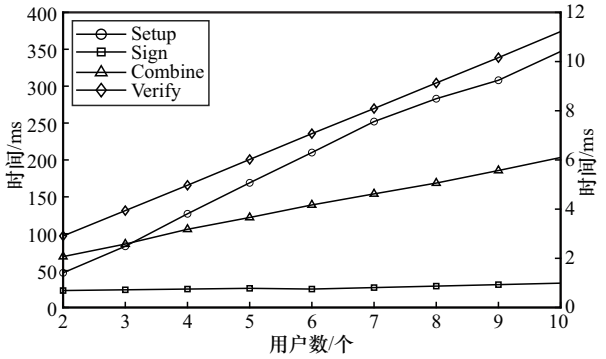

图1　不同用户数下各阶段时间开销对比

综上所述，实验结果表明，尽管LHAS在实现标准模型下多用户线性同态聚合签名的过程中，不可避免地带来了较高的计算开销，但通过设计算法优化和底层实现技巧后，其核心操作在通用计算平台上仍是切实可行的。本文方案在不同用户规模下展现出的性能表现，验证了其在实际应用中的可扩展性。本文方案的价值在于其较强的安全基础与功能的完整性，为安全优先型应用提供了新的技术选择。未来的工作将聚焦于构造更高效的陷门生成与采样算法，并探索硬件加速以进一步提升方案的实用边界。

5　结束语

本文构建了标准模型下支持多用户协同的线性同态聚合签名方案，突破了传统线性同态签名的适用场景局限与计算操作限制。在标准模型下基于SIS问题的困难性证明了方案的不可伪造性，并分析了本文方案在安全性与功能上展现出的优势。未来研究将不局限于线性同态性，而是探索更高阶、复杂的同态运算支持，力求在保持方案安全性的同时，拓展其应用范围与灵活性。

参考文献：

[1] JOHNSON R, MOLNAR D, SONG D, et al. Homomorphic signature schemes[C]//Topics in Cryptology-CT-RSA 2002. Berlin: Springer, 2002: 244-262.

[2] LIN Q, YAN H Y, HUANG Z G, et al. An ID-based linearly homomorphic signature scheme and its application in blockchain[J]. IEEE Access, 2018, 6: 20632-20640.

[3] WU B, WANG C F, YAO H L. A certificateless linearly homomorphic signature scheme for network coding and its application in the IoT[J]. Peer-to-Peer Networking and Applications, 2021, 14(2): 852-872.

[4] WANG H Q. Identity-based distributed provable data possession in multicloud storage[J]. IEEE Transactions on Services Computing, 2015, 8(2): 328-340.

[5] LI Y M, ZHANG F T, SUN Y X. Lightweight certificateless linearly homomorphic network coding signature scheme for electronic health system[J]. IET Information Security, 2021, 15(1): 131-146.

[6] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1994: 124-134.

[7] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303-332.

[8] BONEH D, FREEMAN D M. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures[C]//Public Key Cryptography-PKC 2011. Berlin: Springer, 2011: 1-16.

[9] CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate a lattice basis[J]. Journal of Cryptology, 2012, 25(4): 601-639.

[10] DING C, PEI D, SALOMAA A. Chinese remainder theorem: applications in computing, coding, cryptography[M]. Singapore: World Scientific, 1996

[11] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]//Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2008: 197-206.

[12] BONEH D, FREEMAN D M. Homomorphic signatures for polynomial functions[C]//Advances in Cryptology-EUROCRYPT 2011. Berlin: Springer, 2011: 149-168.

[13] WANG F H, HU Y P, WANG B C. Lattice-based linearly homomorphic signature scheme over binary field[J]. Science China Information Sciences, 2013, 56(11): 1-9.

[14] LYUBASHEVSKY V, MICCIANCIO D. Asymptotically efficient lattice-based digital signatures[J]. Journal of Cryptology, 2018, 31(3): 774-797.

[15] CHEN W B, LEI H, QI K. Lattice-based linearly homomorphic signatures in the standard model[J]. Theoretical Computer Science, 2016, 634: 47-54.

[16] RÜCKERT M. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles[C]// Post-Quantum Cryptography. Berlin: Springer, 2010: 182-200.

[17] LIN C J, XUE R, YANG S J, et al. Linearly homomorphic signatures from lattices[J]. The Computer Journal, 2020, 63(12): 1871-1885.

[18] CHEN W B, HUANG Z G. Towards tightly secure short linearly homomorphic signatures[J]. Theoretical Computer Science, 2024, 1014: 114758.

[19] WANG Z D, LAI Q Q, LIU F H. Almost tight security in lattices with polynomial moduli: PRF, IBE, all-but-many LTF, and more[J]. Designs, Codes and Cryptography, 2025, 93(3): 503-551.

[20] ZHANG P, YU J P, WANG T. A homomorphic aggregate signature scheme based on lattice[J]. Chinese Journal of Electronics, 2012, 21(4): 701-704.

[21] JING Z J. An efficient homomorphic aggregate signature scheme based on lattice[J]. Mathematical Problems in Engineering, 2014(1): 536527.

[22] GU Y Y, SHEN L M, ZHANG F T, et al. Provably secure linearly homomorphic aggregate signature scheme for electronic healthcare system[J]. Mathematics, 2022, 10(15): 2588.

[23] ATTRAPADUNG N, LIBERT B. Homomorphic network coding signatures in the standard model[C]//Public Key Cryptography-PKC 2011.

Berlin: Springer, 2011: 17-34.
[24] AJTAI M, Generating hard instances of lattice problems (extendedabstract) [C]//Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1996: 99-108.
[25] AJTAI M. Generating hard instances of the short basis problem[C]// Automata, Languages and Programming. Berlin: Springer, 1999: 1-9.
[26] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48(3): 535-553.
[27] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[C]//Advances in Cryptology-EUROCRYPT 2012. Berlin: Springer, 2012: 700-718.
[28] MICCIANCIO D, GOLDWASSER S. complexity of lattice problems: a cryptographic perspective[M]. Berlin: Springer, 2002.
[29] MICCIANCIO D, REGEV O. Worst-case to average-case reductions based on Gaussian measures[C]//Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 2004: 372-381.
[30] AGRAWAL S, BONEH D, BOYEN X. Efficient lattice (H)IBE in the standard model[C]//Advances in Cryptology-EUROCRYPT 2010. Berlin: Springer, 2010: 553-572.
[31] KIEIN P. Finding the closest lattice vector when it's unusually close[C]// Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms. NewYork: ACM Press, 2000: 937-941.

[作者简介]

韩益亮（1977– ），男，甘肃会宁人，博士，武警工程大学教授，主要研究方向为公钥密码学、隐私计算。

李瑞峰（1998– ），男，满族，吉林省吉林市人，武警工程大学博士生，主要研究方向为同态签名、云计算。

周潭平（1989– ），男，江西鹰潭人，博士，武警工程大学副教授，主要研究方向为全同态加密、智能电网。

汪晶晶（1986– ），女，湖北鄂州人，博士，武警工程大学副教授，主要研究方向为应用密码学、隐私保护。

杨晓元（1959– ），男，湖南湘潭人，武警工程大学教授，主要研究方向为全同态加密、信息隐藏、云计算。