软件学报 ISSN 1000-9825, CODEN RUXUEW
2025,36(10):4444−4460 [doi: 10.13328/j.cnki.jos.007390] [CSTR: 32375.14.jos.007390]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

具有用户自主链接及验证者条件撤销的格基群签名*

陈 颖, 何德彪, 彭 聪, 罗 敏

(空天信息安全与可信计算教育部重点实验室 (武汉大学), 湖北 武汉 430072)

通信作者: 何德彪, E-mail: hedebiao@163.com

摘 要: 群签名作为一种隐私保护的重要技术, 为用户匿名性提供良好的保障. 然而, 普通群签名方案存在可追溯签名者身份的群管理员, 与区块链去中心化的特性相悖, 难以满足对于隐私性要求更严格的应用场景. 结合防双重认证签名技术, 提出一种具有用户自主链接及验证者条件撤销的群签名, 较好地实现了用户隐私与平台管理之间的平衡, 并给出了格上实例化方案. 通过随机谕言机模型下的安全性分析, 方案满足无私匿名性、可追溯性和不可诽谤性. 通过性能分析, 方案的时间开销和通信开销均在可接受范围内. 最后, 设计了一种基于区块链的后量子安全医疗数据共享条件隐私保护系统, 给出方案的具体应用实例.

关键词: 群签名; 后量子密码; 区块链; 条件隐私保护; 格密码

中图法分类号: TP309

中文引用格式: 陈颖, 何德彪, 彭聪, 罗敏. 具有用户自主链接及验证者条件撤销的格基群签名. 软件学报, 2025, 36(10): 4444–4460. http://www.jos.org.cn/1000-9825/7390.htm

英文引用格式: Chen Y, He DB, Peng C, Luo M. Lattice-based Group Signatures with User-controlled Linkability and Verifier Conditional Revocation. Ruan Jian Xue Bao/Journal of Software, 2025, 36(10): 4444–4460 (in Chinese). http://www.jos.org.cn/1000-9825/7390.htm

Lattice-based Group Signatures with User-controlled Linkability and Verifier Conditional Revocation

CHEN Ying, HE De-Biao, PENG Cong, LUO Min

(Key Laboratory of Aerospace Information Security and Trusted Computing (Wuhan University), Wuhan 430072, China)

Abstract: Recognized as a crucial privacy-protecting technology, group signatures provide robust anonymity assurances for users. However, conventional group signature schemes often rely on group managers capable of revealing the identities of signers, a feature that contradicts the decentralized nature of blockchain and fails to meet stricter privacy demands in certain applications. To address these limitations, this study introduces a group signature scheme with user-controlled linkability and verifier conditional revocation, inspired by double-authentication-preventing signatures and existing linkable and revocable group signatures. The proposed scheme achieves an optimal balance between user privacy and platform oversight, with a concrete instantiation constructed on lattices. Under the random oracle model, the scheme is demonstrated to satisfy the properties of selfless anonymity, traceability, and non-frameability. Performance evaluations indicate that both time and communication costs remain within acceptable limits, ensuring feasibility for practical deployment. In addition, a post-quantum secure medical data sharing system has been designed, integrating the proposed group signature scheme with blockchain technology.

Key words: group signature; post-quantum cryptography; blockchain; conditional privacy protection; lattices

---

* 基金项目: 国家重点研发计划 (2022YFB4400700); 国家自然科学基金 (62325209, 62172307, U23A20302); 中央高校基本科研业务费专项资金 (2042023KF0203, 2042024kf1013, 2042024kf0002)
本文由“抗量子密码与区块链应用”专题特约编辑翁健教授、祝烈煌教授、赵运磊教授推荐.
收稿时间: 2024-06-30; 修改时间: 2024-09-05; 采用时间: 2024-12-30; jos 在线出版时间: 2025-01-20
CNKI 网络首发时间: 2025-00-00

1 引 言

在现代数字化社会中, 以区块链[1]为代表的分布式计算架构为数字资产的确权、交易、流通和计算等提供了可靠、安全、公平的解决方案. 具备隐私保护功能的密码技术成为其底层支撑, 以防止因类架构具备的透明性造成用户数据、行为记录等隐私泄露问题. 特别地, 群签名、环签名、盲签名等密码原语的引入, 允许用户以匿名的方式进行可信数据交换, 为用户隐私提供了有效保护, 推动其在金融、医疗、物联网等敏感领域广泛应用. 然而, 这种强匿名性也为恶意用户滥用提供了可能. 因此, 如何较好地平衡用户隐私与平台管理, 对匿名签署机制提出了新的挑战和要求.

群签名 (group signature, GS) 技术在隐私保护领域具有重要意义, 最早由 Chaum 等人[2]提出. 群签名允许群成员代表整个群组签署任意消息, 验证者可以确认该签名来自群组中的某个群成员, 但无法确切地知晓签名者的身份. 根据群成员是否可以在系统生成后动态地入群或退出, 群签名又可以被分为静态群签名和动态群签名两大类[3]. 当前, 量子计算机的威胁严重冲击了以大整数分解、离散对数问题等为基础的传统公钥密码体制, 因此, 建立在经典困难问题假设上的群签名方案[2,4]已然不能满足抗量子需求. Gordon 等人[5]于 2010 年提出了首个基于格的群签名方案, 奠定了后量子群签名研究的基础. 以高效率、更安全、多功能为目标, 基于格的群签名研究在近年来得到了飞速发展. 在效率方面, 以 Libert 等人[6]提出基于默克尔树累加器构造格上群签名为代表的方案, 将群签名尺寸从线性级别降低为对数级别; Esgin 等人[7]基于 one-out-of-many 技术并解决了多轮重复才可忽略可靠性误差的问题, 实现了群 (环) 签名效率的进一步优化; Lyubashevsky 等人[8]在 LANES 框架的基础上应用 BDLOP 承诺和 Regev 加密形式上的相似性, 使得其中“先加密, 后证明”的代价更小. 在安全方面, Piekert 等人[9]基于带错误学习问题构造了相关性难处理 (correlation intractability, CI) 性质的哈希函数以替代随机谕言机, 得到公共字符串模型下的非交互式零知识证明系统, 进而可转换为群签名方案.

然而, 普通群签名中的群管理员可以对签名进行打开, 从而追溯用户身份, 这与区块链去中心化的特性相悖, 同时, 撤销用户操作将导致其他未撤销用户更新密钥, 造成额外开销, 不便于大规模用户平台采用; 另一方面, 匿名方式也使得用户难以在日后有需要时对自己的历史签名进行链接. 验证者本地撤销的群签名 (group signature with verifier local revocation, GS-VLR)[10]很大程度上削弱了群管理员的权利, 同时撤销用户操作对其他未撤销用户不产生任何影响. 其中, 群管理员仅参与群组的维护, 无法对签名进行打开追溯签名者具体身份; 验签算法需额外输入一个公开的撤销列表, 用于存放撤销用户的撤销令牌, 当某个用户被撤销时, 其产生的签名无法通过签名验证, 并且, 被撤销用户产生的签名可以被链接. 支持用户自主链接的群签名 (group sigantures with user-controlled linkability, GS-UCL)[11]允许用户根据实际需求自主选择自己的历史签名并链接, 证明这些签名都是由自己生成的, 这样的链接方式称为隐式链接; 而与此相对, 用户对于同一个事件主题下产生的签名可以自动被链接, 这样的链接方式称为显式链接. 近年来, 对于验证者本地撤销的群签名有了后量子方案的迁移, Langlois 等人[12]首次提出了基于格的方案, 但这一方案仅支持固定群成员数. 此后, Huang 等人[12]提出了支持群成员动态加入的验证者本地撤销群签名. 而对于支持用户自主链接的群签名[13], Fiore 等人[13]将自主链接的性质扩展到环签名并给出了基于匿名密钥随机化签名转换的格上版本, 但后量子安全的支持用户自主链接群签名尚未有人提出. 同时, 现有验证者本地撤销群签名缺乏撤销条件, 且撤销过程较为模糊, 难以避免验证者恶意撤销用户等行为, 极大地限制了其在实际应用中的落地. 防双重认证签名 (double-authentication-preventing signature, DAPS)[14]旨在对于两个具有相同第 1 部分 (地址) 和不同第 2 部分 (荷载) 的消息生成签名的用户进行私钥提取, 以此作为惩罚, 可视为一种“自发的”条件撤销机制, 在防止双花攻击、一票多投等场景中有着重要应用.

针对现有验证者本地撤销群签名中可能存在的恶意撤销行为, 本文结合防双重认证签名技术的自发条件撤销机制, 提出了具有用户自主链接及验证者条件撤销的群签名 (group signature with user-controlled linkability and verifier conditional revocation, GS-UCL-VCR) 的形式化定义和安全模型, 并以带错误学习问题和带舍入学习问题为底层困难问题构造了格上实例化方案. 对于动态加入群组的成员, 限定其在同一个事件主题下仅可以对一个消息签名, 否则触发撤销条件, 使得验证者可以很容易地提取其撤销令牌并加入到撤销列表, 强迫用户下线, 该过程

不可逆, 即已撤销的用户只能再次申请注册加入群组而无法恢复原有群成员身份. 同时, 诚实签名者可以自主选择其历史签名进行链接并输出链接证明. 与完全匿名且不可追溯的环签名方案相比, 本文方案能更好地实现可控匿名, 在最大程度保护诚实用户隐私的前提下有效遏制潜在恶意行为, 同时赋予诚实用户选择链接历史签名的权力. 在本文方案构造中, 为保证群成员身份匿名性并降低群签名尺寸, 基于 Stern 类协议并借助可更新默克尔树累加器[15]实现了签名大小与群规模成对数关系的动态群签名方案; 为实现上述条件撤销, 借助对偶 Regev 加密方案及逆用同态陷门函数进行违规群成员的撤销令牌提取; 为满足用户自主链接需求, 本文基于格上可验证随机函数 LaV[16]及 LEANES[6–8,17,18]、LEANES+[16]高效格上零知识证明架构并设计了批量链接证明方法实现链接证明与验证. 本文首先给出了基于格的具有用户自主链接及验证者条件撤销的群签名具体构造并进一步证明了该方案在随机谕言机模型下的安全性. 同时, 通过时间、通信开销分析与测试验证了方案的可用性. 最后, 与区块链技术相结合设计了一种基于区块链的后量子安全医疗数据共享条件隐私保护系统, 实现对患者敏感信息的保护, 并保证关键数据的真实性、有效性和准确性.

本文第 2 节回顾格、零知识证明、可更新默克尔树累加器、可验证随机函数相关基础知识. 第 3 节定义具有用户自主链接及验证者条件撤销的群签名的语法与安全模型. 第 4 节给出基于格的具有用户自主链接及验证者条件撤销的群签名具体构造, 并进行了进一步正确性、安全性分析. 第 5 节对所设计的方案进行性能分析、测试与评估. 第 6 节提出一种基于区块链的后量子安全医疗数据共享条件隐私保护系统, 将方案应用落地. 第 7 节总结本文工作.

2 基础知识

2.1 格相关知识

定义 1 (格). 格 $\mathcal{L}$ 是 m 维空间中的 n 个线性无关的向量 $\{\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n\}\in\mathbb{R}^{m\times n}$ 的所有整线性组合构成的向量集合, 表达式如下:

$$\mathcal{L}(\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n)=\left\{\sum_{i=1}^{n}x_i\boldsymbol{b}_i : x_i\in\mathbb{Z}\right\}.$$

其中, 向量组 $\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n$ 称为格 $\mathcal{L}$ 的基, 其中, m 称为格的维数, 基中向量的个数 n 称为格的秩. 当 $m=n$ 时, 格 $\mathcal{L}$ 为满秩格. 同一个格的格基不唯一.

LWE 问题由 Regev 在文献 [19] 提出, 并证明其在量子归约下至少与最坏情况下的近似最短向量问题 (shortest verctor problem, SVP) 困难度一致. 此外, LWE 问题也有其环上版本 RLWE、模格版本 MSIS.

定义 2 (带错误学习问题 (learning with errors, LWE)). 给定 $n,m\geqslant 1,q\geqslant 2$, χ 是 $\mathbb{Z}$ 上的概率分布. 对于 $\boldsymbol{s}\in\mathbb{Z}_q^n$, 给定 $\mathcal{D}_{s,\chi}$ 是由 $\boldsymbol{a}\leftarrow\mathbb{Z}_q^n$, $\boldsymbol{e}\leftarrow\chi$ 定义的分布, 输出 $(\boldsymbol{a},\boldsymbol{s}^{\mathrm{T}}\cdot\boldsymbol{a}+\boldsymbol{e})\in\mathbb{Z}_q^n\times\mathbb{Z}_q$. $\mathrm{LWE}_{n,q,\chi}$ 问题要求区分根据 $\mathcal{D}_{s,\chi}$ 选择的 m 个实例以及从均匀分布 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上选取的 m 个实例.

LWE 中的误差项是随机选取的, 因此不固定. LWE 问题的变体舍入学习问题 (learning with rounding, LWR) 其误差为确定性误差, 由 Banerjee 等人[20]于 2012 年在欧密会上提出, 并证明其困难程度与 LWE 问题等价. 相较于 LWE, LWR 中确定性误差的引入更适宜伪随机函数、可验证随机函数等密码原语的构造.

定义 3 (带舍入学习问题 (learning with rounding, LWR)). 给定参数 $n,m,q,p,\mathcal{B}$, 满足 $q>p,\mathbb{Z}_q$ 表示模 q 剩余类群, 随机选择矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{m\times n}$ 和向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$, 计算 $\boldsymbol{v}=\lfloor\boldsymbol{A}\boldsymbol{s}\rceil_p$. 要求区分 LWR 实例中计算出的 $\boldsymbol{v}\in\mathbb{Z}_p^m$ 和在均匀分布 $\mathbb{Z}_p^m$ 中均匀选取的向量 $\boldsymbol{v}'$.

由此, 容易得到以下引理.

引理 1[18]. 令 $\boldsymbol{u}\in\mathbb{Z}_q^n$, $\boldsymbol{v}\in\mathbb{Z}_q^n$, 对于 $q>p$, p 整除 q, 则 $\boldsymbol{v}=\lfloor\boldsymbol{u}\rceil_p$ 当且仅当存在向量 $\boldsymbol{e}\in\mathbb{Z}^n$ 满足 $\boldsymbol{e}\in\left[\frac{q}{p}\right]^n$ 且 $\boldsymbol{e}=\boldsymbol{u}-\frac{q}{p}\cdot\boldsymbol{v}\bmod q$.

定义 4 (离散高斯分布 (discrete Gaussian distribution)). Λ 上以 $\boldsymbol{c}$ 为中心, σ 为参数的离散高斯分布定义为:

$$\forall \boldsymbol{y} \in \Lambda,\ \mathcal{D}_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{y}) = \frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})}{\rho_{\sigma,\boldsymbol{c}}(\lambda)}.$$

其中, $\rho_{\sigma,\boldsymbol{c}}$ 是以 $\boldsymbol{c}$ 为中心, σ 为参数的高斯函数, 这里, 以 $\boldsymbol{c}$ 为中心, σ 为参数的高斯函数. 当 $\boldsymbol{c}=0$ 时, 可以省略不写.

定理 1 (陷门生成 (trapdoor generation, TrapGen)[21]). 令 $q \geqslant 3$ 为一个奇数, 整数 $l = \lceil \log q \rceil$. 当 $m \geqslant \mathrm{O}(n \log q)$ 时, 存在一个多项式时间算法 $\mathrm{TrapGen}(1^n, 1^m, q)$ 可输出一个矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ 及其陷门, 即 $\Lambda^{\perp}(\boldsymbol{A})$ 的基 $\boldsymbol{B} \in \mathbb{Z}_q^{m \times nl}$. 这里, 矩阵 $\boldsymbol{A}$ 与从 $\mathbb{Z}_q^{n \times m}$ 上均匀选择的矩阵 $\boldsymbol{A}'$ 不可区分, 且 $\|\boldsymbol{B}\|_2 = \mathrm{O}\left(\sqrt{m}\right)$, 以压倒性概率成立.

由于本方案设计的需要, 这里描述陷门生成算法的一个特殊形式 $\mathrm{GenTrap}(1^n, 1^m, q)$ [22]. 令环 $\mathcal{R} = \mathbb{Z}[X]/(X^n+1)$, 给定 $\zeta \in \mathbb{N}, m = \mathrm{O}(n \log q). g = q^{\frac{1}{\zeta}} \in \mathcal{R}_q, \boldsymbol{g}^t = [1 | g | \ldots | g^{\zeta-1}]$, 存在一个多项式时间算法 $\mathrm{GenTrap}(1^n, 1^m, q)$ 可输出一个矩阵 $\boldsymbol{a}^t \in \mathcal{R}_q^{1 \times m}$ 及其陷门 $\boldsymbol{T}_{\boldsymbol{a}} \in \mathcal{R}^{m \times \zeta}$ 满足 $\boldsymbol{a}^t \boldsymbol{T}_{\boldsymbol{a}} = \boldsymbol{g}^t$. 这里, 矩阵 $\boldsymbol{a}^t$ 与从 $\mathbb{Z}_q^{1 \times m}$ 上均匀选择的矩阵 $\boldsymbol{a}^{t\prime}$ 不可区分.

给定 $\Lambda^{\perp}(\boldsymbol{A})$ 的基, 存在一个多项式时间算法可以解决 (I)SIS 问题, 有以下定理.

定理 2 (原像采样 (SamPre)[21]). 令 $q \geqslant 3$ 为一个素数, 整数 $m \geqslant n, k \geqslant 1$. 高斯参数 $\sigma \geqslant \left\|\tilde{\boldsymbol{B}}\right\| \cdot \omega\left(\sqrt{\log n}\right)$, 矩阵 $\boldsymbol{U} \in \mathbb{Z}_q^{n \times k}$, 存在多项式时间算法 $\mathrm{SamPre}(\boldsymbol{A}, \boldsymbol{B}, \sigma, \boldsymbol{U})$ 输出 $\boldsymbol{S} \in \mathbb{Z}_q^{m \times k}$ 满足 $\boldsymbol{AS} = \boldsymbol{U} \bmod q$. 这里, $\boldsymbol{A}, \boldsymbol{B}$ 是 TrapGen 的输出, $\boldsymbol{S}$ 统计上接近分布 $G_{\Lambda^{u_1}(A),\sigma} \times \ldots \times G_{\Lambda^{u_k}(A),\sigma}$ 且 $\|\boldsymbol{S}\| \leqslant \sigma\sqrt{m}$ 以压倒性概率成立.

类似于陷门生成, 这里描述原像采样算法的一个特殊形式 $\mathrm{PreSample}(\boldsymbol{a}^t, \boldsymbol{T}_{\boldsymbol{a}}, \sigma, u)$ [22] 输入矩阵 $\boldsymbol{a}^t \in \mathcal{R}_q^{1 \times m}$ 及其陷门 $\boldsymbol{T}_{\boldsymbol{a}} \in \mathcal{R}^{m \times \zeta}$, $u \in \mathcal{R}_q$, 高斯参数 $s \geqslant \eta_{\epsilon}(\mathbb{Z}) \sqrt{g^2+1} \sqrt{\|\boldsymbol{R}\|^2}$, 输出 $\boldsymbol{v}$ 在统计上接近分布 $G_{\mathcal{R}_q^m,\sigma}$ 满足 $\boldsymbol{a}^t \boldsymbol{v} = u \bmod q$.

定义 5 (同态陷门函数 (homomorphic trapdoor functions, HTDF)[23]). 定义索引空间 $\mathcal{X}$, 输入空间 $\mathcal{U}$, 输出空间 $\mathcal{V}$, 一个 HTDF 由以下 4 个多项式时间算法构成.

(1) $(pk, sk) \leftarrow \mathrm{HTDF.KeyGen}(1^{\lambda})$: 一个密钥生成过程. 输入安全参数 λ, 输出密钥对 (pk, sk).

(2) $f_{pk,x} : \mathcal{U} \to \mathcal{V}$: 一个确定性函数由 $x \in \mathcal{X}, pk$ 索引.

(3) $Inv_{sk,x} : \mathcal{V} \to \mathcal{U}$: 一个概率性逆向函数由 $x \in \mathcal{X}, sk$ 索引.

(4) $u^* = \mathrm{HTDF.Eval}^{\mathrm{in}}(g, (x_1, u_1), \ldots, (x_l, u_l)), v^* = \mathrm{HTDF.Eval}^{\mathrm{Out}}(g, v_1, \ldots, v_l)$: 确定性的输入/输出同态评估算法. 皆以函数 $g : \mathcal{X}^l \to \mathcal{X}$ 及数值 $x_i \in \mathcal{X}, u_i \in \mathcal{U}, v_i \in \mathcal{V}$ 作为输入, 分别以 $u^* \in \mathcal{U}, v^* \in \mathcal{V}$ 作为输出.

一个 HTDF 需要满足与无爪性相似的性质, 即找到两个 $u, u' \in \mathcal{U}$ 且 $x \neq x' \in \mathcal{X}$, 满足 $f_{pk,x}(u) = f_{pk,x'}(u')$ 是困难的. 正式地, 我们要求对于任意多项式时间内的敌手 $\mathcal{A}$ 需满足:

$$\Pr\left[\begin{array}{ll} f_{pk,x}(u) = f_{pk,x'}(u') & (pk, sk) \leftarrow \mathrm{HTDF.KeyGen}(1^{\lambda}) \\ u, u' \in \mathcal{U}, x, x' \in \mathcal{X}, x \neq x' & : \quad (u, u', x, x') \leftarrow \mathcal{A}(1^{\lambda}, pk) \end{array}\right] \leqslant negl(\lambda).$$

2.2 零知识证明

零知识证明系统包括两个参与方: 证明者 P 和验证者 V. P 需要在不透露某个陈述 $x \in \mathcal{L}_{\mathcal{R}}$ 为真之外任何信息的前提下说服 V 相信 x, 在此过程中, V 不知道除了 x 之外的任何信息. 零知识证明最早由 Goldwasser 等人[24]提出, 对于各类密码方案的构建有着重要作用. 本节对非交互式零知识证明系统 (non-interactive zero knowledge system, NIZK) 进行回顾, 其包含 3 个多项式时间算法.

定义 6 (非交互式零知识证明系统 (non-interactive zero knowledge system, NIZK)). 一个 NIZK 系统包含以下 3 个多项式时间算法.

(1) $crs \leftarrow \mathrm{Setup}(1^{\lambda})$: 输入安全参数 λ, 输出公共参考串 crs.

(2) $\pi \leftarrow P(crs, w, x)$: 输入公共参考串 crs, 陈述 x 和证据 w, 生成证明 π.

(3) $1/0 \leftarrow V(crs, x, \pi)$: 输入公共参考串 crs, 陈述 x 和证明 x, 验证证明是否合法.若合法则返回 1; 否则, 返回 0.

通常, NIZK 系统需要满足完备性, 可靠性以及诚实验证者零知识性. 具体定义如下.

- 完备性 (completeness). 对于正确陈述 $x \in \mathcal{L}_{\mathcal{R}}$ 及所有满足 $\mathcal{R}(x, w) = 1$ 的证据 w, 我们有:

$$\Pr\left[(x, \pi) \leftarrow P(crs, w, x) = 1 \ : \ V\left(crs \leftarrow \mathrm{Setup}\left(1^{\lambda}\right)\right)\right] = 1.$$

- 可靠性 (soundness). 对于任意多项式时间内的敌手 $\mathcal{A}$, 我们有:

$$\Pr\left[\begin{array}{ll} V(crs,x,\pi)=1 & crs\leftarrow \mathrm{Setup}(1^{\lambda}) \\ \exists x\notin\mathcal{L}_{\mathcal{R}} & : \\ & (x,\pi)\leftarrow\mathcal{A}(crs)\end{array}\right]=1.$$

● 零知识性 (honest-verifier zero-knowledge). 对于任意陈述 $x\in\mathcal{L}_{\mathcal{R}}$ 及所有满足 $\mathcal{R}(x,w)=1$ 的证据 w, 存在一个模拟器 S 使得其输出与诚实验证者 V 的视图 $V(crs,x,\pi)$ 满足计算不可区分性.

2.3 基于陷门的对偶 Regev (dual-Regev) 加密方案[21]

本文方案中用到了对偶 Regev 加密方案, 这里对其进行描述. 令安全参数为 λ, m,q 为陷门参数, χ 为上界为 $\mathcal{B}$ 的噪声分布, $\mathcal{B}=\mathrm{O}(q/m)$, Π_{PKE} (PKE.keyGen, PKE, Enc, PKE.Dec) 描述如下.

(1) PKE.keyGen(1^{λ}): 输入安全参数 λ, 输出陷门 $(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}})\leftarrow\mathrm{TrapGen}(1^{n},1^{m},q)$, $\boldsymbol{A}\in\mathbb{Z}_{q}^{n\times m}$. 输出密钥对 $(sk,pk)=(\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{A})$.

(2) PKE, Enc(pk,m): 输入公钥 pk, 以及一个消息 $m\in\{0,1\}$, 随机选取向量 $\boldsymbol{d},\boldsymbol{s}\leftarrow\mathbb{Z}_{q}^{n}$, 噪声向量 $\boldsymbol{e}\leftarrow\chi^{m+1}$. 计算 $\boldsymbol{b}=[\boldsymbol{A}|\boldsymbol{d}]^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e}+\left[0\left|\left|\left\lfloor\frac{q}{2}\right\rfloor\cdot m\right|\right.\right]$. 输出密文 $ct=(\boldsymbol{d},\boldsymbol{b})$.

(3) PKE.Dec(sk,ct): 输入私钥 sk 以及密文 ct, 解析 $\boldsymbol{b}=(\boldsymbol{b}_{0},b_{1})$, 计算 $\boldsymbol{s}\leftarrow Inv(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{b})$, $m'=b_{1}-\boldsymbol{d}^{\mathrm{T}}\boldsymbol{s}$.

本节所描述的 dual-Regev 方案满足正确性及选择明文安全下的不可区分性 (indistinguishability against chosen-plaintext attacks, IND-CPA). 详细证明过程可参考文献 [21].

2.4 可更新默克尔树累加器

可更新默克尔树累加器[15]可看作 Libert 等人[6]所提出的格上默克尔树累加器的扩展, 为构建格上动态群签名提供了高效的密码学组件. 与文献 [6] 中提出的原始累加器适用于静态群 (环) 签名不同, 可更新默克尔树累加器方案给出了一个高效的更新算法, 使得对于给定的待修订叶子结点, 可以简单地对该结点所涉及的路径进行修改, 从而更新累加值. 如图 1 所示, 对于一个叶子结点树为 $2^{3}=8$ 的默克尔树, 将 $R=\{\boldsymbol{d}_{0},\ldots,\boldsymbol{d}_{7}\}$ 累加到根结点 $\boldsymbol{u}$ 中. 图中 $j=011$ 以及黄色部分结点 (路径) 作为 $\boldsymbol{d}_{3}$ 累加到 $\boldsymbol{u}$ 中的证据 w. 若需要更新 $\boldsymbol{d}_{3}$ 为 $\boldsymbol{d}_{3}^{*}$, 则需要更新其中绿色的结点.

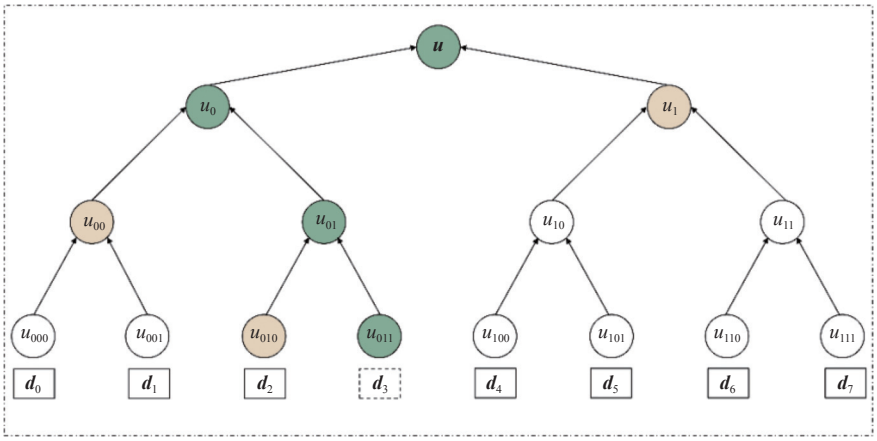

图 1 可更新默克尔树累加器

定义 7 (可更新默克尔树累加器 (updatable Merkle-tree accumulator)). 一个可更新默克尔树累加器由以下 5 个多项式时间算法构成.

(1) $pp\leftarrow\mathrm{TSetup}(\lambda)$: 输入安全参数 λ, 输出公共参数 pp.

(2) $\boldsymbol{u}\leftarrow\mathrm{TAcc}_{pp}(R)$: 输入一个包含 N 个数据的集合 $R=\{\boldsymbol{d}_{0},\ldots,\boldsymbol{d}_{N-1}\}$, 输出累加值 u.

(3) $w/\perp\leftarrow\mathrm{TWitness}_{pp}(R,\boldsymbol{d})$: 输入集合 R 及一个数据 $\boldsymbol{d}$, 若 $\boldsymbol{d}\notin R$ 则输出 $\perp$, 否则, 输出一个证据 w 说明数据 d

确实在 $\mathrm{Tacc}_{pp}(R)$ 的累加中.

(4) $1/0 \leftarrow \mathrm{TVerify}_{pp}(\boldsymbol{u},\boldsymbol{d},w)$: 输入累加值 $\boldsymbol{u}$, 数据 $\boldsymbol{d}$ 以及对应的证据 w, 输出 1 说明 $(\boldsymbol{d},w)$ 对于累加值 $\boldsymbol{u}$ 合法, 否则, 输出 0.

(5) $\boldsymbol{u}' \leftarrow \mathrm{TUpdate}_{pp}(j,\boldsymbol{d}')$: 输入待修订叶子结点索引 j 以及更新后的值, 输出更新后累加值 $\boldsymbol{u}'$.

基于格的 (可更新) 默克尔树累加器依赖于格上抗碰撞哈希函数族, 这里给出定义.

定义 8 (格上抗碰撞哈希函数族 (family of lattice-based collision-resistant hash functions)). 哈希函数族 $\mathcal{H}:\{0,1\}^{nk}\times\{0,1\}^{nk}\rightarrow\{0,1\}^{nk}$ 可以被定义为 $\mathcal{H}=\left\{h_{\boldsymbol{A}}|\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}\right\}$, 其中, $\boldsymbol{A}=[\boldsymbol{A}_0|\boldsymbol{A}_1],\boldsymbol{A}_0,\boldsymbol{A}_1\in\mathbb{Z}_q^{n\times nk}$, 对于任意 $(\boldsymbol{u}_0,\boldsymbol{u}_1)\in\{0,1\}^{nk}\times\{0,1\}$. 我们有: $h_{\boldsymbol{A}}(\boldsymbol{u}_0,\boldsymbol{u}_1)=bin(\boldsymbol{A}_0\boldsymbol{u}_0+\boldsymbol{A}_1\boldsymbol{u}_1 \bmod q)\in\{0,1\}^{nk}$. 这里, $h_{\boldsymbol{A}}(\boldsymbol{u}_0,\boldsymbol{u}_1)=\boldsymbol{u}\Leftrightarrow\boldsymbol{A}_0\boldsymbol{u}_0+\boldsymbol{A}_1\boldsymbol{u}_1=\boldsymbol{G}\boldsymbol{u} \bmod q$. $\boldsymbol{G}\in\mathbb{Z}_q^{n\times nk}$ 为"2 的幂次"工具矩阵:

$$\boldsymbol{G}=\begin{bmatrix}1,2,4,\ldots,2^{k-1} & & \\ & \ddots & \\ & & 1,2,4,\ldots,2^{k-1}\end{bmatrix}.$$

2.5 可验证随机函数

定义 9 (可验证随机函数 (verifiable random function, VRF)[16]). 定义一个 VRF 函数输入长度为 $n(\lambda)$, 输出长度为 $m(\lambda)$. 一个 VRF 函数由以下 3 个多项式时间算法构成.

(1) $(sk,vk)\leftarrow\mathrm{Gen}(\lambda)$: 输入安全参数 λ, 输出公私钥对 (sk,vk).

(2) $(y,\pi)\leftarrow\mathrm{Eval}(sk,x)$: 输入私钥 sk 以及数值 $x\in\{0,1\}^{n(\lambda)}$, 返回输出值 $y\in\{0,1\}^{m(\lambda)}$, 以及证明 π 说明该输出值 y 确实是在 pk 下以输入 x 生成的.

(3) $1/0\leftarrow\mathrm{Verify}(vk,\pi,x,y)$: 输入公钥 vk, 证明 π, 以及输入输出 (x,y), 判断评估算法 Eval 的输出是否合法. 若合法则返回 1, 否则返回 0.

VRF 函数需要满足可证明性、唯一性、自适应不可区分性. 具体定义如下.

● 可证明性 (provability). 对于任意的安全参数 λ 以及输入 $x\in\{0,1\}^{n(\lambda)}$, 我们有:

$$\Pr\left[\begin{array}{l}(sk,vk)\leftarrow\mathrm{Gen}(\lambda)\\(y,\pi)\leftarrow\mathrm{Eval}(sk,x)\end{array}:\mathrm{Verify}(pk,\pi,x,y)=1\right]=1.$$

● 唯一性 (uniqueness). 对于任意的安全参数 λ 以及输入 $x\in\{0,1\}^{n(\lambda)}$, 任意公钥 pk, 存在至多一个单一的输出 $y\in\{0,1\}^{m(\lambda)}$ 对于存在一个可被接受的证明 π.若 $\mathrm{Verify}(pk,\pi,x,y)=\mathrm{Verify}(pk,\pi',x,y')=1$, $y=y'$ 一定成立.

● 自适应不可区分性 (adaptive indistinguishability). 对于任意多项式时间内的敌手 $\mathcal{A}$, 至多以不可忽略的概率 $negl(\lambda)$ 赢得下面的游戏.

$\mathrm{Game}_{\mathcal{A},\mathrm{VRF}}(\lambda)$
$Q:=\varnothing$
$b\leftarrow\{0,1\}$
$(sk,vk)\leftarrow\mathrm{Gen}(\lambda)$
$(st,x^*)\leftarrow\mathcal{A}^{\mathcal{O}_1(sk,\cdot)}(pk)$
$(y_0,\pi)\leftarrow\mathrm{Eval}(sk,x^*)$
$y_1\leftarrow\{0,1\}^{m(\lambda)}$
$b'\leftarrow\mathcal{A}^{\mathcal{O}_1(sk,\cdot)}(st,y_b)$
return $b=b'\wedge x^*\notin Q$

$\mathcal{O}_1(sk,x)$
$(y,\pi)\leftarrow\mathrm{Eval}(sk,x)$
$Q:=Q\cup\{x\}$
return (y,π)

3 具有用户自主链接及验证者条件撤销的群签名的语法及安全模型

本节介绍具有用户自主链接及验证者条件撤销的群签名的语法定义及安全模型.

3.1 具有用户自主链接及验证者条件撤销的群签名语法定义

定义 10 (具有用户自主链接及验证者条件撤销的群签名 (GS-UCL-VCR)). 一个 GS-UCL-VCR 方案包含. 系统初始化 Setup, 群密钥生成 GKeyGen, 用户密钥生成 UKeyGen, 入群 Join, 群更新 GUpdate, 签名 Sign, 验签

Verify, 提取撤销令牌 Extract, 用户自主链接 UCLink, 链接验证 VLink 共 10 个多项式时间算法, 描述如下.

(1) $pp \leftarrow \mathrm{Setup}(1^{\lambda})$: 输入安全参数 λ, 输出系统公共参数 pp. 群管理员 $\mathcal{GM}$ 初始化 Merkle 树 $\mathrm{TSetup}(pp, gpk) \rightarrow T_{crt}$, 将所有叶子结点置为 $\mathbf{0}$, 初始化用户计数器 $c = 0$, 初始化撤销列表 $RL = \varnothing$, 初始化用户注册列表 reg.

(2) $(gsk, gpk) \leftarrow \mathrm{GKeyGen}(pp)$: 输入公共参数 pp, 输出群密钥对 (gsk, gpk). 由群管理员 $\mathcal{GM}$ 执行.

(3) $(usk, upk) \leftarrow \mathrm{UKeyGen}(pp, gpk)$: 输入公共参数 pp, 群公钥 gpk, 输出用户密钥对 (usk, upk). 由用户本地执行.

(4) $\langle(\mathrm{ID}, grt), \perp\rangle \leftarrow \mathrm{Join}\langle user(upk), \mathcal{GM}(gsk)\rangle$: 该算法由 $\mathcal{GM}$ 与用户交互式进行. 用户提交自己的公钥 upk 申请入群, 若 $\mathcal{GM}$ 同意该入群请求, 用户将得到自己的群成员 ID 和撤销令牌 grt. $\mathcal{GM}$ 更新树, 更新用户计数器 c+ = 1, 更新用户注册列表 reg, 无输出.

(5) $info_{\mathrm{new}} \leftarrow \mathrm{GUpdate}(gpk, gsk, info, RL, reg)$: 输入群密钥对 (gsk, gpk), 当前群消息 $info$, 撤销列表 RL, 用户注册列表 reg, 输出最新群消息 $info_{\mathrm{new}}$. 由群管理员 $\mathcal{GM}$ 执行.

(6) $\Sigma \leftarrow \mathrm{Sign}(gpk, pp, usk[\pi], M \in \{0,1\}^{*}, scp, upk[\pi], grt[\pi])$: 输入群公钥 gpk, 系统公共参数 pp, 用户公私钥对 $(usk[\pi], upk[\pi])$, 消息 M, 事件主题 scp, 撤销令牌 $grt[\pi]$, 输出消息-签名对 Σ. 由群成员 ID 为 π 的用户执行.

(7) $1/0 \leftarrow \mathrm{Verify}(gpk, pp, info_{\mathrm{new}}, \Sigma, RL)$: 输入群公钥 gpk, 系统公共参数 pp, 最新群消息 $info_{\mathrm{new}}$, 消息-签名对 Σ, 撤销列表 RL. 输出 1 表示签名合法, 否则输出 0. 由验证者执行. 其中输入的撤销列表 RL 由群管理员 $\mathcal{GM}$ 维护.

(8) $grt[\pi^{*}] / \perp \leftarrow \mathrm{Extract}(\Sigma_1, \Sigma_2)$: 输入两个消息-签名对 Σ_1, Σ_2, 若其是同一个事件主题 scp 下的不同签名, 则提取对应签名者的撤销令牌 $grt[\pi^{*}]$ 并输出, 反馈给群管理员 $\mathcal{GM}$ 将其添加在撤销列表 RL 中; 否则返回 $\perp$. 由验证者执行.

(9) $(\Pi_L, \overline{nym}, \boldsymbol{\Sigma}) \leftarrow \mathrm{UCLink}(\boldsymbol{\Sigma}, usk)$: 输入自己的历史消息-签名对集合 $\boldsymbol{\Sigma} = (\Sigma_1, \Sigma_2, \ldots, \Sigma_K)$, 以及用户私钥 usk, 生成链接证明 Π_L 及聚合假名 $\overline{nym}$ 说明集合 $\boldsymbol{\Sigma}$ 中的签名均由自己所签. 由用户执行.

(10) $1/0 \leftarrow \mathrm{VLink}(\boldsymbol{\Sigma}, \overline{nym}, \Pi_L)$: 输入某一用户的历史消息-签名对集合 $\boldsymbol{\Sigma}$, 聚合假名 $\overline{nym}$, 以及对应的链接证明 Π_L, 输出 1 表示证明合法, 否则输出 0. 任何人可以执行.

GS-UCL-VCR 方案满足正确性, 其同时满足签名验证正确性、链接验证正确性及条件可提取性.

● 签名验证正确性 (verification correctness). 一个 GS-UCL-VCR 方案满足签名验证正确性, 当且仅当对于所有由系统初始化 Setup 产生的 pp, 群密钥生成算法 GKeyGen 产生的 gpk, 群更新算法 GUpdate 所产生的最新群消息 $info_{\mathrm{new}}$ 及通过加入算法 Join 认证的持有密钥 $(usk[i], upk[i])$ 和撤销令牌 $grt[i]$ 的群成员 (ID = i) 所产生的签名均合法, 除非该成员已被撤销. 正式地:

$$\mathrm{Verify}(gpk, pp, \mathrm{GUpdate}(gpk, gsk), \mathrm{Sign}(gpk, pp, usk[i], M \in \{0,1\}^{*}, scp, upk[i], grt[i]), RL) = 1 \Leftrightarrow grt[i] \notin RL.$$

● 链接正确性 (link correctness). 一个 GS-UCL-VCR 方案满足链接正确性, 当且仅当对于通过加入算法 Join 认证的持有密钥 $(usk[i], upk[i])$ 和撤销令牌 $grt[i]$ 的群成员 (ID = i) 所产生合法消息-签名对集合 $\boldsymbol{\Sigma} = (\Sigma_1, \Sigma_2, \ldots, \Sigma_K)$, 利用用户自主链接算法 UCLink 为其生成的链接证明 Π_L 及聚合假名 $\overline{nym}$, 一定可以通过链接验证算法的验证. 正式地,

$$\Pr\left[\begin{array}{ll} \Sigma_j \leftarrow \mathrm{Sign}(gpk, pp, usk[i], M \in \{0,1\}^{*}, scp, upk[i], grt[i]) & \\ j = \{1, 2, \ldots, K\} & : \mathrm{VLink}(\boldsymbol{\Sigma}, \overline{nym}, \Pi_L) = 1 \\ \boldsymbol{\Sigma} = (\Sigma_1, \Sigma_2, \ldots, \Sigma_K) & \end{array}\right] = 1.$$

● 条件可提取性 (conditional extractability). 一个 GS-UCL-VCR 方案满足条件可提取性, 当且仅当对于所有由系统初始化 Setup 产生的 pp, 群密钥生成算法 GKeyGen 产生的 gpk, 群更新算法 GUpdate 所产生的最新群消息 $info_{\mathrm{new}}$ 及通过加入算法 Join 认证的持有密钥 $(usk[i], upk[i])$ 和撤销令牌 $grt[i]$ 的群成员 (ID = i) 所产生的任意两个消息-签名对 $\Sigma_1 \leftarrow \mathrm{Sign}(gpk, pp, usk[i], M_1, scp_1, upk[i], grt[i])$, $\Sigma_2 \leftarrow \mathrm{Sign}(gpk, pp, usk[i], M_2, scp_2, upk[i], grt[i])$, 始终满足:

$$\mathrm{Extract}(\Sigma_1, \Sigma_2) = \begin{cases} grt[i], & \text{if } nym_1 = nym_2 \wedge M_1 \neq M_2 \\ \perp, & \text{otherwise} \end{cases}.$$

其中, $\Sigma_1=(sig_1,M_1,nym_1,\tau_1,scp_1),\Sigma_2=(sig_2,M_2,nym_2,\tau_2,scp_2)$.

3.2 安全模型

具有用户自主链接及验证者条件撤销的群签名方案应满足无私匿名性、可追溯性、不可诽谤性. 这里, 相较于普通完全匿名的群签名方案, 无私匿名性是指不依赖公钥加密可实现的最优匿名性[3], 即敌手不可以获得用于挑战的两个用户对应的私钥.

定义 11 (无私匿名性 (selfless-anonymity)). 定义无私匿名性游戏 $\text{Game}_{\text{selfano}}$, 敌手 $\mathcal{A}$ 的目标是判断一个给定签名是由两个用户中的哪一个产生的. 游戏定义如下.

(1) Setup. 挑战者 $\mathcal{C}$ 依次运行系统初始化算法 Setup, 群密钥生成算法 GKeyGen, 用户密钥生成算法 UKeyGen, 入群算法 Join 得到公共参数 pp, 群密钥对 (gsk,gpk), 用户 $(\text{ID}=i)$ 密钥对及撤销令牌 $(usk[i],upk[i],grt[i])$. 将 pp,gpk 发送给 $\mathcal{A}$.

(2) Queries. $\mathcal{A}$ 做如下询问.

a) $\mathcal{SO}$: $\mathcal{A}$ 自适应选择消息 μ 和主题事件 scp 在 $\text{ID}=i,i\in[c]$ 用户私钥下的签名. $\mathcal{C}$ 运行签名算法返回 $\Sigma\leftarrow\text{Sign}(gpk,pp,usk[\pi],\mu\in\{0,1\}^*,scp,upk[\pi],grt[\pi])$ 给 $\mathcal{A}$. 为避免平凡攻击, 对于同一个 ID 下的同一个主题事件 scp 仅可询问 1 次.

b) $\mathcal{CO}$: $\mathcal{A}$ 询问 $\text{ID}=i,i\in[c]$ 用户的私钥. $\mathcal{C}$ 返回对应 $usk[i]$. 此时, 对应用户被腐化.

c) $\mathcal{RO}$: $\mathcal{A}$ 询问 $\text{ID}=i,i\in[c]$ 用户的撤销令牌. $\mathcal{C}$ 返回对应的 $grt[i]$. 此时, 对应用户被腐化.

d) $\mathcal{LO}$: $\mathcal{A}$ 选取 $\text{ID}=i$ 所对应的私钥 $usk[i]$ 所生成的历史消息-签名集合 $\boldsymbol{\Sigma}$, 询问其链接证明. $\mathcal{C}$ 返回对应的 Π_L.

(3) Chal. $\mathcal{A}$ 输出挑战消息 μ^*, 主题事件 scp^* 及两个群成员 ID 索引 i_0,i_1, 这里索引对应的用户不可以是已被撤销的或已在 $\mathcal{CO},\mathcal{RO}$ 询问中出现过的同时, 为避免平凡攻击, 若 i_0,i_1 在 $\mathcal{SO}$ 询问中出现过, 则 scp^* 不可以与对应历史 $\mathcal{SO}$ 中询问 i_0,i_1 时的 scp 相同 $\mathcal{C}$ 随机选取一个比特 $b\leftarrow\{0,1\}$, 计算由 $usk[i_b]$ 产生的签名 $\Sigma^*\leftarrow\text{Sign}(gpk,pp,usk[i_b],M^*,scp,upk[i_b],grt[i_b])$ 并发送给 $\mathcal{A}$.

(4) Restricted Queries. $\mathcal{A}$ 可做与 Queries 阶段中相同的询问, 但在 $\mathcal{CO},\mathcal{RO}$ 询问时, 不可以对索引 i_0,i_1 进行询问. 在对索引 i_0,i_1 进行 $\mathcal{SO}$ 询问时, 主题事件 $scp\neq scp^*$ 且不可与 Queries 阶段对 i_0,i_1的$\mathcal{SO}$ 询问输入的 scp 相同.对于索引 i_0,i_1, 在 Queries 和 Restricted Queries 阶段, 分别定义 $\mathcal{SO}$ 询问得到返回值 Σ 的集合分别为 $SIG,CSIG$, $\mathcal{LO}$ 询问得到的返回值集合分别为 LP,CLP, 在对索引 i_0,i_1 进行 $\mathcal{LO}$ 询问时, 若选择的 $\boldsymbol{\Sigma}$ 满足 $(\boldsymbol{\Sigma}\wedge SIG\neq\varnothing\wedge(*,\boldsymbol{\Sigma})\in LP)\wedge(\boldsymbol{\Sigma}\cap\wedge CSIG\neq\varnothing\wedge(*,\boldsymbol{\Sigma})\in CLP)$, 则中止游戏.

(5) Output. $\mathcal{A}$ 输出一个比特 b', 若 $b'=b$ 则赢得游戏.

若 $\mathcal{A}$ 赢得游戏 $\text{Game}_{\text{selfano}}$ 的优势 $\text{Adv}_{\text{Game}_{\text{selfano}}}=\left|\Pr[b'=b]-\frac{1}{2}\right|\leqslant negl(\lambda)$, 则 GS-UCL-VCR 满足无私匿名性.

定义 12 (可追溯性 (traceability)). 定义可追溯性游戏 $\text{Game}_{\text{trace}}$, 敌手 $\mathcal{A}$ 的目标是伪造一个合法签名 (或链接证明) 使其不可以被追溯到一个合法群成员. 这里首先定义一个辅助函数 Identity 用于判断一个给定的签名是否由群成员生成, $\text{Identity}(gpk,usk,\Sigma)\rightarrow 1/0$, 若 Σ 确实是由 usk 生成则返回 1, 否则返回 0. 其次, 定义询问 $\mathcal{LO}$, $\mathcal{A}$ 选取 $\text{ID}=i$ 所对应的私钥 $usk[i]$ 所生成的历史签名集合 $\boldsymbol{\Sigma}$, $\mathcal{C}$ 运行用户自主链接算法 UCLink 返回对应的 Π_L; 若 $\exists\Sigma\in\boldsymbol{\Sigma},\text{Identity}(gpk,usk,\Sigma)=0\wedge\text{Verify}(gpk,pp,info_{\text{new}},\Sigma,RL)=0$, 游戏中止并返回 $\perp$.

可追溯性覆盖了以往群签名中不可伪造的性质, 保证了只有合法有效的群成员才可以代表群签名. 假设 $\mathcal{A}$ 伪造了 n 个签名 ($n\geqslant 1$), $\mathcal{A}$ 赢得签名可追溯 (signature traceability, $\text{Game}^1_{\text{trace}}$) 和链接证明可追溯 (link traceability, $\text{Game}^2_{\text{trace}}$) 两个游戏的概率:

$$Adv_{\text{Game}^1_{\text{trace}}}=\Pr\left[\begin{array}{l}pp,gsk,gpk,info_{\text{new}}\leftarrow\text{Setup},\text{GKeyGen},\text{GUpdate}\\(\Sigma_1,\ldots,\Sigma_n)\leftarrow\mathcal{A}^{so,co}(gpk)\\\text{for } i=1,\ldots,n,\text{Verify}(gpk,pp,info_{\text{new}},\Sigma_i,RL)=1\wedge\Sigma_i=(sig_i,M_i,nym_i,T_i,scp_i)\\\exists\Sigma_i\text{ s.t. }\forall\text{ ID}\in reg\cup RL:\ \text{Identity}(gpk,\text{ID},\Sigma_i)=0\end{array}\right]\leqslant negl(\lambda),$$

$$Adv_{\mathrm{Game}^2_{\mathrm{trace}}}=\Pr\left[\begin{array}{l} pp,gsk,gpk,info_{\mathrm{new}}\leftarrow \mathrm{Setup,\ GKeyGen,GUpdate}\\ (\Pi_L,\overline{nym},\boldsymbol{\Sigma})\leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{LO}}(gpk)\\ \mathrm{VLink}(\boldsymbol{\Sigma},\overline{nym},\Pi_L)=1\\ \exists\Sigma\in\boldsymbol{\Sigma}\ \text{s.t.}\ \forall\ \mathrm{ID}\in reg\vee RL:\mathrm{Identity}(gpk,\mathrm{ID},\Sigma_i)=0 \end{array}\right]\leqslant negl(\lambda).$$

定义 13 (不可诽谤性 (non-frameability)). 定义不可诽谤性游戏 $\mathrm{Game}_{\mathrm{noframe}}$, 敌手 $\mathcal{A}$ 的目标是使得诚实用户的签名与其从未产生过的签名相链接. 由于在本签名语法设定中, 由同一个 usk 在同一个 scp 下对不同消息产生的两个签名可导致条件撤销, 故这里我们仅考虑 $\mathcal{A}$ 以不同的事件主题企图与诚实用户链接的情况. $\mathcal{A}$ 诽谤诚实用户可以通过以下两种途径: (1) 伪造签名使其与诚实用户产生的签名相链接 (签名诽谤); (2) 为诚实用户产生一个链接证明, 所涉及的签名均由该用户生成, 但该用户没有产生过该证明, 即证明本身是伪造的 (链接诽谤). 假设 $\mathrm{ID}=i$ 的诚实用户所产生的历史签名集合为 $\boldsymbol{\Sigma}_i$, $\mathcal{A}$ 赢得不可诽谤 $\mathrm{Game}_{\mathrm{noframe}}$ 游戏的概率:

$$Adv_{\mathrm{Game}_{\mathrm{noframe}}}=\Pr\left[\begin{array}{l} pp,gsk,gpk,info_{\mathrm{new}}\leftarrow \mathrm{Setup,GKeyGen,GUpdate}\\ (\Pi_L,\overline{nym},\boldsymbol{\Sigma})\leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{LO}}(gsk,gpk)\\ (1)\ \mathrm{VLink}(\boldsymbol{\Sigma},\overline{nym},\Pi_L)=1\ \text{s.t.}\ \exists\Sigma,\Sigma'\in\boldsymbol{\Sigma}:\Sigma\in\boldsymbol{\Sigma}_i\wedge\Sigma'\in\boldsymbol{\Sigma}_i\\ (2)\ \mathrm{VLink}(\boldsymbol{\Sigma},\overline{nym},\Pi_L)=1\ \text{s.t.}\ \forall\Sigma\in\boldsymbol{\Sigma},\Sigma\in\boldsymbol{\Sigma}_i\wedge(\overline{nym},\Pi_L)\notin LO\ (\mathrm{ID}=i) \end{array}\right]\leqslant negl(\lambda).$$

4 基于格的具有用户自主链接及验证者条件撤销的群签名设计

本节描述基于格的具有用户自主链接及验证者条件撤销的群签名的具体构造. 在群签名的构造上, 借助格上可更新的默克尔树累加器[15]及基于 SIS 和 LWE 的 Stern 类协议[25]实现对数级群签名尺寸同时保证匿名性. 在条件撤销环节, 逆用同态陷门函数使其在既定条件下输出碰撞得到替代陷门求解撤销令牌. 在用户自主链接环节, 受到 LaV 格上可验证随机函数的启发设计批量链接证明方法[16]. 同时, 我们将第 2.3 节中所描述的对偶 Regev 公钥加密方案 $\Pi_{\mathrm{PKE}}(\mathrm{PKE.keyGen},\mathrm{PKE},\mathrm{Enc},\mathrm{PKE.Dec})$ 作为黑盒使用. 具体方案描述如下.

(1) $\mathrm{Setup}(1^\lambda)$: 输入安全参数 λ, 正整数 $n,m,q,p,\sigma,k,\iota,\kappa,\omega,\zeta$, 其中, $k=\lceil\log_2 q\rceil, m=2nk$, 设定群成员数量上限为 $N=2^\iota=poly(\lambda), scp\in\{0,1\}^*$ 数量上限为 Q, 满足 $Q\ll p$; 选取哈希函数 $H_1:\{0,1\}^*\to\mathcal{R}_q^{n\times m}, H_2:\{0,1\}^*\to\mathcal{R}_q^{m\times n}$, $H_3:\{0,1\}^*\to\{1,2,3\}^\kappa, \kappa=\omega(\log\lambda)$, 形如定义 8 中的工具矩阵 $\boldsymbol{G}_1,\boldsymbol{G}_2$, 定义二进制转换函数 $bin:\mathcal{R}^n\to\{0,1\}^{nk}$, 定义 VRF 函数 LaV: $f_x(\boldsymbol{B})=\boldsymbol{B}\boldsymbol{x}_p \bmod p$. 群管理员 $\mathcal{GM}$ 初始化默克尔树 $\mathrm{TSetup}(pp,gpk)\to T_{crt}$, 将所有叶子结点置为 $\mathbf{0}$, 初始化用户计数器 $c=0$, 初始化撤销列表 $RL=\varnothing$, 初始化用户注册列表为 $reg\left(\{[i][grt[i]][upk[i]]\}_{i\in[N]}\right)=\{[i][0^m][0^{nk}]\}$. 输出系统公共参数集合 $pp=\{\lambda,n,m,q,p,\kappa,\omega,\zeta,\sigma,k,N,Q,H_1,H_2,f,\boldsymbol{G}_1,\boldsymbol{G}_2,\iota\}$.

(2) $\mathrm{GKeyGen}(pp,gpk)$: 由群管理员 $\mathcal{GM}$ 执行. 运行 $(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}})\leftarrow\mathrm{TrapGen}(1^n,1^m,q)$, 输出群密钥对 $(gsk,gpk)=(\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{A}), \boldsymbol{A}=(\boldsymbol{A}_0\|\boldsymbol{A}_1)\in\mathcal{R}^{n\times m}, \boldsymbol{A}_0,\boldsymbol{A}_1\in\mathcal{R}^{n\times nk}$ 以适配于格上哈希函数族.

(3) $\mathrm{UKeyGen}(pp,gpk)$: 由用户本地执行. 运行 $(\boldsymbol{b},\boldsymbol{T}_{\boldsymbol{b}})\leftarrow\mathrm{GenTrap}(1^n,1^m,q)$, 选择 $\boldsymbol{x}\leftarrow\{0,1\}^m(\boldsymbol{x}\neq 0)$, 计算 $\boldsymbol{d}=bin(\boldsymbol{A}\boldsymbol{x}_p)$, 输出自己的密钥对 $(usk,upk)=((\boldsymbol{T}_{\boldsymbol{b}},\boldsymbol{x}),(\boldsymbol{b},\boldsymbol{d}))$.

(4) $\langle(\mathrm{ID},grt),\perp\rangle\leftarrow\mathrm{Join}\langle user(upk),\mathcal{GM}(gsk)\rangle$: 由用户与群管理员交互式进行.

a) $user$: 发送 $upk=(\boldsymbol{b},\boldsymbol{d})$ 请求加入群.

b) $\mathcal{GM}$: 若同意请求, 则发布用户 ID 为 $j=bin(c)$, 运行 $s\leftarrow\mathrm{SamPre}(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\sigma,\boldsymbol{b}), \boldsymbol{s}\leqslant\sigma\sqrt{m}$, 将 $usk[j]=(\boldsymbol{T}_{\boldsymbol{b}},\boldsymbol{x},\boldsymbol{s},j)$, $grt[i]=\boldsymbol{s}$ 发送给用户; 更新树 T_{crt} 计算新累加值 $\mathrm{TUpdate}_A(j,\boldsymbol{d})\to\boldsymbol{z}_{\mathrm{new}}$; 更新用户计数器 $c+=1$; 更新用户注册列表 $reg=(\{[j][\boldsymbol{s}][\boldsymbol{d}]\})$.

(5) $\mathrm{GUpdate}(gpk,gsk,info,RL,reg)$: 由群管理员 $\mathcal{GM}$ 执行.

a) 若 $RL=\varnothing$, 则跳转到步骤 b). 否则, 解析 $RL=\{\boldsymbol{s}_1,\ldots,\boldsymbol{s}^*,\ldots\}$, 对于撤销令牌为 $\boldsymbol{s}^*$ 作为本次撤销对象, 以 $\boldsymbol{s}^*$ 为索引在注册列表 reg 中找到 $grt[I]=\boldsymbol{s}^*$ 的用户元组 $\{[I][\boldsymbol{s}][upk[I]]\}$, 将对应的 $upk[I]=\mathbf{0}$ 置零. 更新用户计数器 $c-=1$.

b) 运行 $\mathrm{TUpdate}_A(j,\boldsymbol{d})\to\boldsymbol{z}_{\mathrm{new}}$, 更新树 T_{crt}. 对于每一个 j, 令 $w_j\in\{0,1\}^l\times\left(\{0,1\}^{nk}\right)^l_{j\in[c]}$ 作为证据说明 $\boldsymbol{d}_i$ 已累加到 $\boldsymbol{z}_{\mathrm{new}}$ 中, 发布群消息 $info_{\mathrm{new}}=\left(\boldsymbol{z}_{\mathrm{new}},\{w_j\}_{j\in[c]}\right)$ 经被撤销的用户其对应叶子结点值不累加在 $\boldsymbol{z}_{\mathrm{new}}$ 中.

(6) $\mathrm{Sign}\left(gpk,pp,usk[\pi],\mu\in\{0,1\}^*,scp,upk[\pi],grt[\pi]\right)$: 由用户 π 执行.

a) 运行 $\mathrm{PKE.Enc}(\boldsymbol{b},\boldsymbol{s}')$, 加密 $grt[\pi]$: 随机选择 $\boldsymbol{r}\leftarrow\{0,1\}^{mk}, f\leftarrow\mathcal{R}_q, bin(s)\to\boldsymbol{s}'$; 计算 $\boldsymbol{C}_1=\boldsymbol{b}\boldsymbol{r}^{\mathrm{T}},\boldsymbol{c}_2=f\cdot\boldsymbol{r}+\dfrac{q}{2}\cdot\boldsymbol{s}', ct=(\boldsymbol{C}_1,\boldsymbol{c}_2,f)$.

b) 计算 $\boldsymbol{V}=H_1(scp),\boldsymbol{H}=H_2(scp\|\mu)$, 运行 $\boldsymbol{u}\leftarrow\mathrm{SamPre}(\boldsymbol{b},\boldsymbol{T}_b,\sigma,\boldsymbol{V}+\boldsymbol{H}\boldsymbol{G}_1)$.

c) 计算假名 $nym=\boldsymbol{V}\cdot\boldsymbol{x}_p,\tau=\boldsymbol{H}\cdot\boldsymbol{s}_p$.

d) 生成非交互式零知识证明协议 Φ 说明: (1) 持有具有合法的 $\boldsymbol{x},\boldsymbol{s}$, 且累加器验证通过; (2) b) 中生成的 $\boldsymbol{u}$ 是合法的; (3) 加密 $grt[\pi]$ 的过程是正确的; (4) nym,τ 是正确计算的. 生成的证明描述如下.

$$\Pi_1:\left\{(\boldsymbol{s},\boldsymbol{b})\,|\,\boldsymbol{A}\boldsymbol{s}=\boldsymbol{b}\bmod q,\|\boldsymbol{s}\|\leqslant\sigma\sqrt{m}\wedge\boldsymbol{b}\boldsymbol{u}=\boldsymbol{V}+\boldsymbol{H}\boldsymbol{G}_1\right\},$$

$$\Pi_2:\{(\boldsymbol{x},\boldsymbol{s})\,|\,nym=\boldsymbol{V}\cdot\boldsymbol{x}_p,\tau=\boldsymbol{H}\cdot\boldsymbol{s}_p\},$$

$$\Pi_3:\left\{\left(\boldsymbol{x},\boldsymbol{b},\boldsymbol{d},(j,w_j),\boldsymbol{r},\boldsymbol{s}\cdot\boldsymbol{r}^{\mathrm{T}}\right)|\boldsymbol{A}\boldsymbol{x}_p=\boldsymbol{G}_2\cdot\boldsymbol{d}\bmod p\wedge\mathrm{TVerify}_A(\boldsymbol{z}_{\mathrm{new}},\boldsymbol{d},(j,w_l,\ldots,w_1))=1\right.$$
$$\left.\wedge\boldsymbol{C}_1=\boldsymbol{b}\boldsymbol{r}^{\mathrm{T}},c_2=f\cdot\boldsymbol{r}+\frac{q}{2}\cdot\boldsymbol{s}'\wedge\boldsymbol{d}\neq\boldsymbol{0}^{nk}\right\}.$$

重复 $\kappa=\omega(\log\lambda)\Phi$ 以达到可忽略的完备性错误 (soundness error). 最终生成的证明 $P^{H_3}(X,Z)\to\Pi=\{\Pi_1,\Pi_2,\Pi_3\}$. 这里, 公开输入 $X=(\boldsymbol{A},\boldsymbol{u},scp,\boldsymbol{G}_1,\boldsymbol{G}_2,nym,\tau,ct,\boldsymbol{z}_{\mathrm{new}},\boldsymbol{H},\boldsymbol{V})$, 秘密输入 $(\boldsymbol{s},\boldsymbol{x},\boldsymbol{b},\boldsymbol{d},(j,w_j),\boldsymbol{r},\boldsymbol{s}\cdot\boldsymbol{r}^{\mathrm{T}})$. 通过 Fait-Shamir 转换为非交互式协议 $\Pi=(\{CMT_i\}_{i=1}^{\kappa},CH,\{RSP\}_{i=1}^{\kappa})$, 其中,

$$CH=H_3(\mu,\{CMT_i\}_{i=1}^{\kappa},\boldsymbol{A},\boldsymbol{u},scp,\boldsymbol{G}_1,\boldsymbol{G}_2,nym,\tau,ct,\boldsymbol{z}_{\mathrm{new}},\boldsymbol{H},\boldsymbol{V})\to\{1,2,3\}^{\kappa},$$

其中, $\boldsymbol{d}\neq\boldsymbol{0}^{nk}$ 这一不等关系证明参考文献 [15] 中的不等关系证明.

e) 签名 $sig=(\Pi,ct,\boldsymbol{u})$, 输出消息-签名对为 $\Sigma=(sig,\mu,nym,\tau,scp)$.

(7) $\mathrm{Verify}(gpk,pp,info_{\mathrm{new}},\Sigma,RL)\to1/0$.

a) 下载 $\boldsymbol{z}_{\mathrm{new}}$, 解析 Σ, 计算 $\boldsymbol{V}'=H_1(scp),\boldsymbol{H}'=H_2(scp\|\mu)$.

b) 运行 $\mathrm{V}^{H_3}(X',\Pi)$ 验证证明 Π, 若合法则进行步骤 c), 否则输出 0 返回.

c) 对于 RL 中的每一个 $grt[i]\to\boldsymbol{s}'_j$, 检查是否存在 $\tau=\boldsymbol{H}\cdot\boldsymbol{s}_p$, 若存在则返回 0.

(8) $\mathrm{Extract}(\Sigma_1,\Sigma_2)\to grt[\pi^*]/\perp$.

a) 运行验证算法 Verify 验证 Σ_1,Σ_2 合法性.

b) 解析 Σ_1,Σ_2, 若 $nym_1=nym_2\wedge\mu_1\neq\mu_2$ 则进行步骤 c), 否则输出 $\perp$.

c) 运行解密算法 $\mathrm{PKE.Dec}(\boldsymbol{u}_1-\boldsymbol{u}_2,ct)\to grt'[\pi^*]$, 并将其反馈给群管理员 $\mathcal{GM}$ 加入 RL 中以撤销该违规群成员.

(9) $\mathrm{UCLink}(\boldsymbol{\Sigma},usk)\to\Pi_L$: 由持有私钥 $\boldsymbol{x}$ 的诚实用户执行.

a) 解析 $\boldsymbol{\Sigma}\to\{(nym_1,scp_1),\ldots,(nym_i,scp_i)\}_{i\in K},K\leqslant Q$.

b) 计算 $\overline{hscp}=\sum_{i=1}^{K}H_1(scp_i),\overline{nym}=\overline{hscp}\cdot\boldsymbol{x}_p$.

c) 生成 NIZK $\Pi_L:\left\{(\boldsymbol{x})\left(\overline{hscp},\overline{nym}\right)|\overline{nym}=\overline{hscp}\cdot\boldsymbol{x}_p\right\}$

(10) $\mathrm{VLink}(\boldsymbol{\Sigma},\overline{nym},\Pi_L)\to1/0$.

a) 解析 $\boldsymbol{\Sigma}\to\{(nym_1,scp_1),\ldots,(nym_i,scp_i)\}_{i\in K},K\leqslant Q$.

b) 运行验签算法 Verify 逐一检验每个 Σ_i 的合法性, 若存在 $\Sigma\in\boldsymbol{\Sigma},\mathrm{Verify}(gpk,pp,info_{\mathrm{new}},\Sigma,RL)=0$, 返回 0.

c) 若对于 $\exists i\neq j\in[K]$, 存在 $scp_i=scp_j$ 返回 0.

d) 计算 $snym=\sum_{i=1}^{K}nym_i,\Delta=snym-\overline{nym}$, 验证 $\|\Delta\|_\infty\leqslant K+1$ 是否成立. 若成立则输出 1 表示 Π_L 合法, 否则输出 0.

4.1 正确性分析

定理 3. GS-UCL-VCR 符合正确性, 其同时满足验证正确性, 链接验证正确性及条件可提取性.

证明: 下面分别证明验证正确性, 链接验证正确性及条件可提取性.

● 验证正确性: 非交互式零知识证明协议 Φ 的完备性及哈希函数 H_1, H_2 的抗碰撞性保证了我们方案的验证正确性. 根据接收到的信息, 验证者总能正确地通过事件主题 scp 及消息 μ 重新计算 $\boldsymbol{V}' = H_1(scp), \boldsymbol{H}' = H_2(scp\|\mu)$. 根据非交互式零知识证明协议 Φ 的完备性, 输入 $X' = (\boldsymbol{A}, \boldsymbol{u}, scp, \boldsymbol{G}_1, \boldsymbol{G}_2, nym, \tau, ct, \boldsymbol{z}_{\text{new}}, \boldsymbol{H}', \boldsymbol{V}')$ 总能使得验证算法输出 1.

● 链接验证正确性: 根据引理 1, 可验证随机函数构造 LaV 的正确性, 以及参数设置条件 $Q \ll p$, GS-UCL-VCR 满足链接验证正确性. 对于某用户 $(usk = x)$ 在一个 scp 下的部分签名 (假名 nym): $nym = \boldsymbol{V} \cdot \boldsymbol{x}_p$, 故存在误差向量 $\boldsymbol{e} = \boldsymbol{V}\boldsymbol{x} - \dfrac{q}{p} \cdot nym, \|\boldsymbol{e}\| \leqslant \dfrac{q}{p}$ 成立, 对于 $\boldsymbol{e}_i = \boldsymbol{V}_i \cdot \boldsymbol{x} - \dfrac{q}{p} \cdot nym_i, i \in [K]$, 存在误差向量 $\|\boldsymbol{e}_i\| \leqslant \dfrac{q}{p}$, 将上述 K 个等式累加可得 $\boldsymbol{E} = \overline{hscp} \cdot \boldsymbol{x} - \dfrac{q}{p} \cdot snym, \|\boldsymbol{E}\| \leqslant \dfrac{q}{p} \cdot K$. 故根据方案中相关参数的设定, 考虑四舍五入带来的误差, 容易得到:

$$snym = \overline{hscp} \cdot \boldsymbol{x} \cdot \frac{p}{q} - \boldsymbol{E} \cdot \frac{p}{q} \approx \overline{nym} - \boldsymbol{E}_p \mp 1 \Rightarrow |snym - \overline{nym}| \leqslant |K| + 1.$$

即对于诚实用户的 K 个历史签名, $\Delta = |snym - \overline{nym}|$, $\|\Delta\|_\infty \leqslant K + 1$ 显然成立.

与此同时, 若用户企图在其中链接一个其他用户 $(usk = x')$ 在 scp_t 下的签名, 类似于上述分析方法, 对于等式 $\boldsymbol{e}_i = \boldsymbol{V}_i \cdot \boldsymbol{x} - \dfrac{q}{p} \cdot nym_i,\ i \in [t-1]$, $\boldsymbol{e}_t = \boldsymbol{V}_t \cdot \boldsymbol{x}' - \dfrac{q}{p} \cdot nym_t$, $\boldsymbol{e}_i = \boldsymbol{V}_i \cdot \boldsymbol{x} - \dfrac{q}{p} \cdot nym_i,\ i \in [t+1, K]$, 进行累加可得 $\|\boldsymbol{E}\| \leqslant \dfrac{q}{p} \cdot K$. 根据方案中相关参数设定, 容易得到 $\Delta = snym - \overline{nym} = \left| \dfrac{p}{q} \cdot \boldsymbol{V}_t(\boldsymbol{x}' - \boldsymbol{x}) - \dfrac{p}{q} \cdot \boldsymbol{E}' \right|$, 又因为 $K \leqslant Q \ll p$, 故 $\|\boldsymbol{V}_t(\boldsymbol{x}' - \boldsymbol{x})\| > \|\boldsymbol{E}'\|$, $\|\Delta\|_\infty > K + 1$. 因此无法通过链接验证.

● 条件可提取性: 利用 HTDF 的“碰撞”, 得到陷门 $\boldsymbol{s}$ 的替代 $\boldsymbol{u}_1 - \boldsymbol{u}_2$, 作为私钥运行解密算法得到该用户的撤销令牌 $grt'[\pi^*]$, 将其反馈给群管理员 $\mathcal{GM}$ 将其加入撤销列表 RL.

综上所述, GS-UCL-VCR 同时满足验证正确性, 链接验证正确性及条件可提取性, 因此满足正确性. 证毕.

4.2 安全性分析

定理 4. 在随机谕言机模型下, GS-UCL-VCR 满足无私匿名性, 当以下条件同时成立: (1) 基于格的非交互式零知识证明协议 Φ, Π_L 满足零知识性; (2) LWE 问题是困难的; (3) 对偶 Regev 方案满足 IND-CPA 安全; (4)LWR 问题是困难的; (5) 可验证随机函数 LaV 满足自适应不可区分性.

证明: 在挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$ 之间建立以下几个游戏.

Game_0: 这一游戏过程与 $\text{Game}_{\text{selfano}}$ 一致. $\mathcal{C}$ 真实地运行系统初始化算法 Setup, 群密钥生成算法 GKeyGen, 用户密钥生成算法 UKeyGen, 入群算法 Join 得到公共参数 pp, 群密钥对 (gsk, gpk), 用户 $(\text{ID} = i)$ 密钥对及撤销令牌 $(usk[i], upk[i], grt[i])$. 将 pp, gpk 发送给 $\mathcal{A}$. 在此游戏中, 所选择的挑战比特 $b = 0$.

Game_1: 在这一游戏中, $\mathcal{A}$ 与模拟器 $\mathcal{S}_1$ 交互. 不同于 Game_0, $\mathcal{S}_1$ 运行模拟协议 $\mathcal{S}_p$ 生成非交互式零知识证明协议 Φ 的证明 Π^*. 根据协议 Φ 的零知识性:

$$Adv^{\text{selfano}}_{\text{Game}_0}(\lambda) \approx Adv^{\text{selfano}}_{\text{Game}_1}(\lambda).$$

Game_2: 在这一游戏中, $\mathcal{A}$ 与模拟器 $\mathcal{S}_2$ 交互. $\mathcal{S}_2$ 与 $\mathcal{S}_1$ 几乎一致, 密文 $\boldsymbol{c}_2$ 及 $\boldsymbol{u}$ 的生成方式除外. 不同于 Game_1 中 $\boldsymbol{c}_2 = f \cdot \boldsymbol{r} + \dfrac{q}{2} \cdot \boldsymbol{s}', \boldsymbol{u} \leftarrow \text{SamPre}(\boldsymbol{b}, \boldsymbol{T}_b, \sigma, \boldsymbol{V} + \boldsymbol{H} \cdot \boldsymbol{G}_1)$ 计算得出, 这里 $\mathcal{S}_2$ 直接从均匀分布中选取 $\boldsymbol{c}_2^* \leftarrow \mathbb{Z}^{mk}, \boldsymbol{u}^* \leftarrow \mathbb{Z}^{1 \times n}$, 根据判定性 LWE 的困难性及定理 4:

$$Adv^{\text{selfano}}_{\text{Game}_2}(\lambda) \approx Adv^{\text{selfano}}_{\text{Game}_1}(\lambda).$$

Game_3: 在这一游戏中, $\mathcal{A}$ 与模拟器 $\mathcal{S}_3$ 交互. $\mathcal{S}_3$ 与 $\mathcal{S}_2$ 几乎一致, nym, τ 的生成方式除外. 不同于 Game_2 中 $nym = \boldsymbol{V} \cdot \boldsymbol{x}_p, \tau = \boldsymbol{H} \cdot \boldsymbol{s}_p$ 计算得出, 这里 $\mathcal{S}_3$ 直接从均匀分布中随机选取 $nym^* \leftarrow \mathbb{Z}_p^n, \tau^* \leftarrow \mathbb{Z}_p^m$, 根据 LWR 问题的困难性及可验证随机函数 LaV 的自适应不可区分性:

$$Adv^{\text{selfano}}_{\text{Game}_3}(\lambda) \approx Adv^{\text{selfano}}_{\text{Game}_2}(\lambda).$$

Game_4: 这一游戏与 Game_3 一致, $\mathcal{A}$ 与模拟器 $\mathcal{S}_4$ 交互. $\mathcal{S}_4$ 与 $\mathcal{S}_3$ 几乎一致, Π_L 的生成方式除外. 不同于 Game_3

中 Π_L 由 UCLink 算法计算得出, 这里 $\mathcal{S}_4$ 运行模拟协议 $\mathcal{S}'_p$ 生成 Π^*. 根据 Π_L 的零知识性:

$$Adv^{\text{selfano}}_{\text{Game}_4}(\lambda) \approx Adv^{\text{selfano}}_{\text{Game}_4}(\lambda).$$

Game_5: 这一游戏与 Game_0 一致, 除了所选择的挑战比特 $b=1$. 上述游戏 0–5 等价, $\mathcal{A}$ 以很大概率不可区分其中任意两个. 因此 GS-UCL-VCR 满足无私匿名性. 证毕.

定理 5. 在随机谕言机模型下, GS-UCL-VCR 满足可追溯性, 当以下条件同时成立: (1) LWR 问题是困难的; (2) GS-UCL-VCR 满足签名可追溯性.

证明: 首先证明签名可追溯性. 在挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$ 之间建立以下游戏.

Game_0: 这一游戏与 $\text{Game}^1_{\text{trace}}$ 一致.

Game_1, Game_2, Game_3:与定理 6 证明中的 Game_1, Game_2, Game_3 一致.

我们分析 $\mathcal{A}$ 赢得游戏 $\text{Game}^1_{\text{trace}}$ 的困难性. 假设 $\mathcal{A}$ 可以伪造一个消息-签名对 $\Sigma^* = (\Pi^*, ct^*, \boldsymbol{u}^*, \mu^*, nym^*, \tau^*, scp^*)$ 满足 $\text{Verify}(gpk, pp, info_{\text{new}}, \Sigma^*, RL) = 1$. 根据协议 Φ 的可靠性, 证据 $\left(\boldsymbol{x}^*, \boldsymbol{b}^*, \boldsymbol{d}^*, \left(j^*, w_j^*\right), \boldsymbol{r}^*, \boldsymbol{s}^* \cdot \boldsymbol{r}^{*\mathrm{T}}\right)$ 可以被提取且等式 $\lfloor \boldsymbol{A}\boldsymbol{x} \rceil^*_p = \boldsymbol{G}_2 \cdot \boldsymbol{d}^* \bmod p$ 成立, 同时 $\text{TVerify}_A(\boldsymbol{z}_{\text{new}}, \boldsymbol{d}^*, (j^*, w_l^*, \ldots, w_1^*)) = 1$ s.t. $\forall \text{ID} \in reg \cup RL, \text{Identity}(gpk, \text{ID}, \Sigma^*) = 0$. 这里, 对于当前有效群成员和已被撤销的群成员其公钥均未被腐化, 因此, $\boldsymbol{x}_i \neq \boldsymbol{x}^*$. 考虑以下两种情况.

(1) $\boldsymbol{d}^* \notin reg^*$: 此时, 说明 $\boldsymbol{d}^*$ 不在 $\boldsymbol{z}_{\text{new}}$ 的累加中而累加器验证算法仍返回 1, 等价于打破了累加器的安全性, 与前提假设相悖.

(2) $\boldsymbol{d}^* \in reg^*$: 此时, $\boldsymbol{d}^* = \boldsymbol{d}_i, i \in reg^*$. 根据协议 Φ 的可靠性且 $\boldsymbol{x}_i \neq \boldsymbol{x}^*, i \in reg^*$, 必定存在:

$$\boldsymbol{A}\boldsymbol{x}_{ip} = \boldsymbol{G}_2 \cdot \boldsymbol{d}_i \wedge \boldsymbol{A}\boldsymbol{x}^*{}_p = \boldsymbol{G}_2 \cdot \boldsymbol{d}^*.$$

由此可以推导出 $\boldsymbol{A} \cdot (\boldsymbol{x}_i - \boldsymbol{x}^*)_p = \boldsymbol{0}$, 相当于得到了一个 LWR 问题的解. 然而, 对于任意多项式时间内的敌手 $\mathcal{A}$, LWR 问题是困难的. 因此 GS-UCL-VCR 满足签名可追溯性.

接下来证明链接可追溯性. 若方案满足签名可追溯性, 则等价于不存在 $\text{Verify}(gpk, pp, info_{\text{new}}, \Sigma^*, RL) \wedge \forall \text{ID} \in \text{ID} \in reg \cup RL, \text{Identity}(gpk, \text{ID}, \Sigma^*) = 0$, 因此由非合法群成员生成的签名不可能通过验签算法 Verify. 而链接验证算法 VLink 包含了 Verify 的过程. 由此 GS-UCL-VCR 亦满足链接可追溯性.

综上所述, GS-UCL-VCR 满足可追溯性. 证毕.

定理 6. 在随机谕言机模型下, GS-UCL-VCR 满足不可诽谤性, 当以下条件同时成立: (1) 可验证随机函数 LaV 满足唯一性; (2) GS-UCL-VCR 满足可追溯性.

证明: 我们分别从定义 12 中敌手企图赢得不可诽谤性游戏可以采取的两种途径出发进行分析.

情形 1: 伪造签名使其与诚实用户产生的签名相链接 (签名诽谤). 若 GS-UCL-VCR 满足链接可追溯性, 则不存在 $\text{VLink}(\boldsymbol{\Sigma}, \overline{nym}, \Pi_L) = 1$ s.t. $\exists \Sigma, \Sigma^* \in \boldsymbol{\Sigma} : \Sigma \in \boldsymbol{\Sigma}_i \wedge \Sigma^* \notin \boldsymbol{\Sigma}_i$, 其中, $\boldsymbol{\Sigma}$ 为诚实用户的历史消息-签名集合, Σ^* 为敌手 $\mathcal{A}$ 伪造的消息-签名对.

情形 2. 为诚实用户产生一个链接证明, 所涉及的签名均由该用户生成, 但该用户没有产生过该证明, 即证明本身是伪造的 (链接诽谤). 假设诚实用户所产生的历史消息-签名集合为 $\boldsymbol{\Sigma}$, 其私钥 $usk = \boldsymbol{x}$, 原本该用户可以利用自己的私钥 $\boldsymbol{x}$ 运行用户自主链接算法 $\Pi_L = \left\{(\boldsymbol{x})\left(\overline{hscp}, \overline{nym}\right) | \overline{nym} = \overline{hscp} \cdot \boldsymbol{x}_p\right\}$ 对 $\boldsymbol{\Sigma}$ 产生链接证明 $\text{UCLink}(\boldsymbol{\Sigma}, usk) \to \Pi_L$, 这里, 其本质是一个可验证随机函数. 若敌手 $\mathcal{A}$ 企图为该诚实用户的这一历史消息-签名集合为 $\boldsymbol{\Sigma}$ 生成一个链接证明 Π_L^*, $\overline{hscp}$ 容易通过已有信息计算, 由于私钥 $\boldsymbol{x}$ 未被腐化, 则 $\mathcal{A}$ 用于伪造证明和伪造聚合假名 $\overline{nym}^*$ 的私钥 $\boldsymbol{x}^* \neq \boldsymbol{x}$, 若 Π_L^* 可以满足 $\text{VLink}(\boldsymbol{\Sigma}, \overline{nym}^*, \Pi_L^*) = 1$, 存在以下两种情况.

(1) $\overline{nym}^* = \overline{nym}$: 此时, 容易推导出 $\overline{hscp} \cdot (\boldsymbol{x} - \boldsymbol{x}^*)_p = 0$, 即找到了一个 LWR 问题实例的解. 然而, 对于任意多项式时间内的敌手 $\mathcal{A}$, LWR 问题是困难的.

(2) $\overline{nym}^* \neq \overline{nym}$: 此时, 由于输入 $\overline{hscp}$ 相同, 对于能够通过链接验证 VLink 的证明 Π_L, 其输出是唯一的. 这与可验证随机函数的唯一性相悖.

因此, GS-UCL-VCR 满足不可诽谤性. 证毕.

5 性能分析

本节从时间开销分析及通信开销分析对本文所提出的基于格的具有用户自主链接及验证者条件撤销的群签名进行性能分析, 并与已有相近方案进行对比.

本文在环 $\mathcal{R}=\mathbb{Z}[X]/(X^d+1)$ 上对本方案进行实例化. 参考文献 [26,27] 设置相关参数: $d=256$, $q=8380417$, $n=2048$, $m=2048$, $\sigma=7112$, $k=\log q=23$, $N=2^{16}$, $Q=100$. 根据文献 [28] 中安全评估工具, 本方案在此参数设定下可达到约 254 比特经典安全强度及 248 比特量子安全强度.

5.1 时间开销分析

本文基于文献 [16,29] 中源码及 Miracl 大整数库, 采用 Windows 10 64 位操作系统对本方案及对比方案涉及的基本算子进行测试, 实验环境为 Intel(R) Core(TM) i7-8700 CPU @3.20 GHz, 16.0 GB RAM. 其中涉及到的基本算子符号定义及测试结果如表 1 所示 (假设群组满员, 即 $c=N=2^{16}$).

表 1 基本算子符号定义及时间开销测试结果 (ms)

符号	定义	时间	符号	定义	时间
T_{trapgen}	陷门生成耗时	44.50	$T_{\text{gen-proof}}$	$\mathcal{P}'^{H_3}(X,Z)\to\Pi$耗时	3900
T_{SamPre}	原像采样耗时	2.00	T_{ver}	$\mathcal{V}'^{H_3}(X',\Pi)\to 1/0$耗时	0.69
T_{mul}	多项式乘法耗时	0.06	T_{H_1}	哈希函数 H_1 耗时	0.37
T_{add}	多项式加法耗时	≈ 0	T_{H_2}	哈希函数 H_2 耗时	0.37
$T_{\text{mat-mul}}$	矩阵-向量乘法耗时	0.20	T_h	哈希函数 h 耗时[11]	0.005
$T_{\text{vrf-eval}}$	LaV.Eval评估算法耗时	35.75	T_{pm}	$\mathbb{G}_1$群上点乘[11]	1.74
$T_{\text{vrf-Verify}}$	Lav.Verify验证算法耗时	1.19	T_{pa}	$\mathbb{G}_1$群上点加[11]	0.008

本文考虑与已有文献 [11–13,15,30] 进行对比, 主要关注签名算法 Sign, 验签算法 Verify, 链接算法 UCLink 以及链接验证算法 Vlink, 分析结果如表 2 所示 (假设 $RL=\varnothing$, 用户链接签名个数为 $K=Q=100$).

表 2 文献 [11–13,15,30] 与本文方案时间开销及功能对比

文献	Sign (ms)	Verify (ms)	UCLink (ms)	VLink (ms)	F_1	F_2	F_3	F_4
[11]	$T_{\text{gen-proof}}+T_{H_1}\approx 3900.37$	$T_{\text{ver}}\approx 0.69$	—	—	√	×	×	√
[12]	$T_{\text{gen-proof}}+4T_{\text{mat-mul}}+4T_{\text{add}}\approx 3900.24$	$T_{\text{ver}}+2T_{\text{mat-mul}}\approx 0.81$	—	—	√	×	×	√
[13]	$T_{\text{gen-proof}}+T_{H_1}+2T_{\text{mat-mul}}\approx 3900.77$	$T_{\text{ver}}\approx 0.69$	$2T_{H_1}+3T_{\text{mat-mul}}+T_{H_2}+KT_{\text{add}}\approx 2.71$	$2T_{H_2}+T_{\text{Verify}}+KT_{\text{add}}\approx 2.8$	×	√	×	√
[15]	$2T_{\text{mat-mul}}+T_{\text{mul}}+T_{\text{add}}+T_{\text{gen-proof}}\approx 3900.46$	$T_{\text{ver}}\approx 0.69$	—	—	×	×	×	√
[30]	$4(T_{\text{pa}}+T_{\text{pm}})+2h\approx 1.782$	$4T_{\text{pa}}+9T_{\text{pm}}+2h\approx 17.50$	$(K+1)h+(K+2)T_{\text{pm}}\approx 178.0$	$(K+1)h+2T_{\text{pm}}\approx 4.0$	×	√	×	×
本文	$2T_{\text{mul}}+T_{\text{mat - mul}}+2T_{\text{add}}+2T_{\text{vrf-eval}}+T_{\text{SamPre}}+T_{\text{gen-proof}}\approx 3973.82$	$T_{\text{ver}}+T_{H_1}+T_{H_2}\approx 1.43$	$KH_1+T_{\text{vrf-eval}}\approx 72.75$	$KH_1+KT_{\text{add}}+T_{\text{vrf-Verify}}\approx 38.19$	√	√	√	√

*注: 其中 F_1 代表是否支持验证者本地撤销, F_2 代表是否支持用户自主链接, F_3 代表是否支持条件撤销, F_4 代表是否具有后量子安全性

由于文献 [11–13,15] 及本方案均是基于格构建的群环签名方案, 其基于 Stern 协议的零知识证明部分时间开销参考文献 [29] 做估计, 在同一平台下的时间消耗远大于文献 [30] 一般群上构建的群签名方案, 故签名部分时间开销有较大差异. 根据分析结果, 本文所提出的方案功能最为丰富, 与原始格上动态群签名方案[15]相比, 增加的开销不大, 签名算法、链接验证算法阶段时间开销虽略高于现有文献 [11–13,30], 但均在可接受范围内.

5.2 通信开销分析

对于方案通信开销的评估, 本文关注签名尺寸及链接证明尺寸, 分析结果如表 3 所示. 其中, $|\mathbb{G}_1|$ (32 字节) 是群 $\mathbb{G}_1$ 中元素的长度, $|\mathbb{Z}_p|$ 是有限域 $\mathbb{Z}_p$ 中整数的长度, $hlen$(32 字节) 是哈希函数 h 的输出长度. 根据文献 [16] 中的定义, $|t_L|$ 代表 LEANES 证明[6–8,17,18]的长度, $|\pi_L|$ 代表 LEANES+证明[16]的长度 ($|t_L|+|\pi_L|\approx 7.1$ KB), $|\pi_R|$ 代表其中松弛证明长度 (3.18 KB).

表 3 文献 [11,12,30] 与本文方案通信开销对比

对比项	文献[11]	文献[12]	文献[30]	本文方案
签名尺寸	$O(n\log N)$	$O(n\log N)$	$4\times\|\mathbb{G}_1\|+5\times\|\mathbb{Z}_p\|+hlen$	$O(n\log N+n\times mk\log q+mk\log q+2m\log q+n\log q)$
链接证明尺寸	—	—	$\|\mathbb{Z}_p\|+hlen$	$\|t_L\|+\|\pi_L\|+\|\pi_R\|$

根据相关参数设置, 本方案签名尺寸在群成员数量为 $N=2^{16}$ 时约为 163 KB, 链接证明尺寸约为 10.28 KB, 具有较强的可用性.

6 应 用

医疗数据对于推动医药研究领域前沿技术的发展有着不可替代的作用, 保证其安全共享十分重要. 一方面, 需要保护患者隐私, 其敏感信息如姓名、出生日期等信息一旦被盗用将会造成经济损失和法律问题; 另一方面, 关键数据的真实性、有效性和准确性对于研究过程至关重要. 同时, 设置合理、适当的奖励机制有助于患者乐于贡献自己的病情数据用于医药研究, 有利于维护医患信任, 从而推动医药行业的发展. 因此, 亟需建立新技术为医疗数据共享平台提供安全、可靠的条件隐私保护机制.

针对以上需求, 本文结合具有用户自主链接及验证者撤销的格基群签名方案和区块链技术, 设计了一种基于区块链的后量子安全医疗数据共享条件隐私保护系统, 实现对患者敏感信息的保护, 并保证数据的真实性、有效性和准确性, 大致运行流程如图 2 所示.

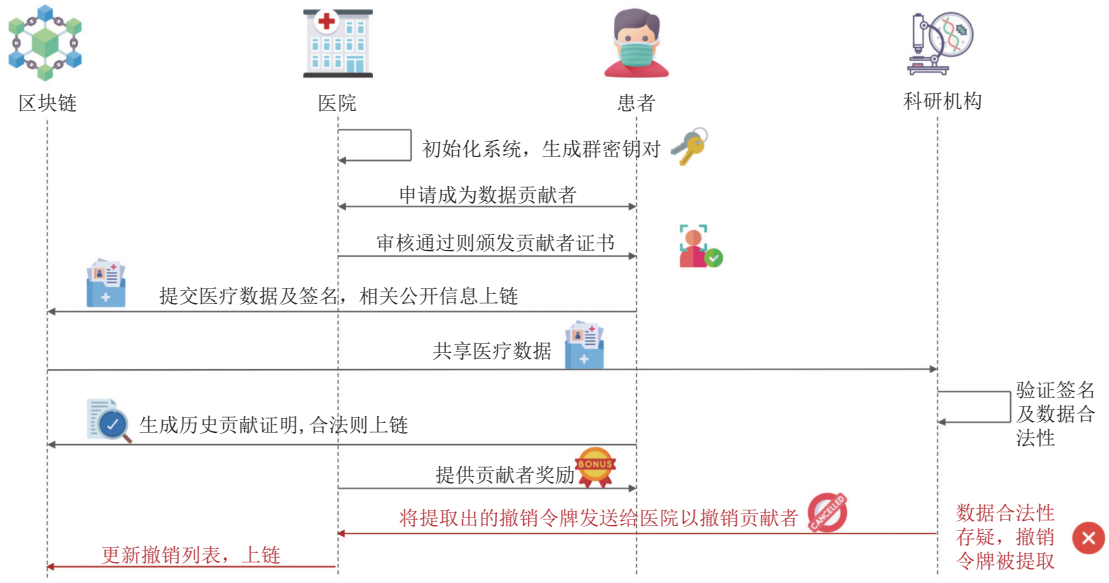

图 2 基于区块链的后量子安全医疗数据共享条件隐私保护系统

该系统主要包含: 患者 *PAT*、医疗数据管理中心 (医院)*HSP*、医药科研机构 *MR*、区块链 *BC* 等模块, 集成了具有用户自主链接及验证者撤销的格基群签名模块和区块链模块. 其中, 数据合法性存疑指对于同一患者登记号

的贡献两份不同病例档案的患者, 视为违规贡献者. 具有用户自主链接及验证者撤销的格基群签名模块提供贡献者证书分发、历史贡献证明生成、违规数据提供者撤销, 同时不会揭露患者身份隐私. 区块链模块用于记录公开数据及贡献者证书等. 根据本文第 4 节描述的基于格的具有用户自主链接及验证者条件撤销群签名, 具体过程如下.

(1) 初始化系统, 生成群密钥对: 由 *HSP* 先后运行 Setup、GKeyGen 算法得到系统参数与群密钥对.

(2) 申请成为数据贡献者: 由 *PAT* 运行 UKeyGen 算法得到自己的原始用户密钥对并运行 Join 算法与 *HSP* 交互成为数据贡献者, *HSP* 向符合条件的 *PAT* 颁发证书 (包含信息 ID, grt).

(3) 贡献医疗数据及签名: *PAT* 运行 Sign 算法对自己所贡献的医疗信息 μ 签名, 其唯一的登记号为 scp. 将以上信息及签名对公开在 *BC* 上.

(4) 共享医疗数据及验证数据合法性: 由 *PAT* 提交的医疗数据通过 *BC* 共享, *MR* 从中获取数据, 运行 Verify 验证数据合法性, 运行 Extract, 若提取出撤销令牌, 则数据合法性存疑, 将所提取的撤销令牌反馈给 *HSP*, 将其加入到公开撤销列表中, 在 *BC* 中上链, 强制违规的 *PAT* 下线.

(5) 诚实数据贡献者可自主选择生成贡献证明以获得奖励: *PAT* 运行 UCLink 算法选择性地生成历史贡献证明, *HSP* 等运行 VLink 算法验证该证明的合法性, 若合法, 则在 *BC* 中上链, 对贡献者进行奖励.

7 总 结

本文探索基于格的具有用户自主链接及验证者条件撤销的群签名. 受到防双重认证签名思想的启发, 实现验证者本地条件撤销, 并基于格上可验证随机函数 LaV 设计了批量链接证明方法. 本文给出具有用户自主链接及验证者条件撤销的群签名的语法及安全模型定义, 同时给出基于格的具有用户自主链接及验证者条件撤销的群签名的具体构造及安全性分析. 最后, 通过时间、通信开销分析验证本文方案的实用性. 同时, 本文给出了一个具体应用场景, 用于构建基于区块链的后量子安全医疗数据共享条件隐私保护系统. 实际应用时, 需综合考虑多种需求, 如何进一步提高基于格的群签名效率、丰富其功能, 需在我们的后续工作中研究探索.

References:

[1] Liu JW, Fan Y, Sun R, Liu L, Wu C, Mumtaz S. Blockchain-aided privacy-preserving medical data sharing scheme for E-healthcare system. IEEE Internet of Things Journal, 2023, 10(24): 21377–21388. [doi: 10.1109/JIOT.2023.3287636]

[2] Chaum D, Van Heyst E. Group signatures. In: Proc. of the 1991 Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Brighton: Springer, 1991. 257–265. [doi: 10.1007/3-540-46416-6_22]

[3] Feng HW, Liu JW, Wu QH. Group signatures and ring signatures with post-quantum security. Journal of Cryptologic Research, 2021, 8(2): 183–201 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000430]

[4] Yang YT, Cai JL, Zhang XW, Yuan Z. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm. Ruan Jian Xue Bao/Journal of Software, 2019, 30(6): 1692–1704 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5745.htm [doi: 10.13328/j.cnki.jos.005745]

[5] Gordon SD, Katz J, Vaikuntanathan V. A group signature scheme from lattice assumptions. In: Proc. of the 2010 Annual Int'l Conf. on the Theory and Application of Cryptology and Information Security. Singapore: Springer, 2010. 395–412. [doi: 10.1007/978-3-642-17373-8_23]

[6] Libert B, Ling S, Nguyen K, Wang HX. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In: Proc. of the 2016 Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Vienna: Springer, 2016. 1–31. [doi: 10.1007/978-3-662-49896-5_1]

[7] Esgin MF, Steinfeld R, Liu JK, Liu DX. Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications. In: Proc. of the 39th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2019. 115–146. [doi: 10.1007/978-3-030-26948-7_5]

[8] Baum C, Damgård I, Lyubashevsky V, Oechsner S, Peikert C. More efficient commitments from structured lattice assumptions. In: Proc. of the 11th Int'l Conf. on Security and Cryptography for Networks. Amalfi: Springer, 2018. 368–385. [doi: 10.1007/978-3-319-98113-0_20]

[9] Peikert C, Shiehian S. Noninteractive zero knowledge for NP from (plain) learning with errors. In: Proc. of the 39th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2019. 89–114. [doi: 10.1007/978-3-030-26948-7_4]

[10] Boneh D, Shacham H. Group signatures with verifier-local revocation. In: Proc. of the 11th ACM Conf. on Computer and Communications Security. Washington: ACM, 2004. 168–177. [doi: 10.1145/1030083.1030106]

[11] Diaz J, Lehmann A. Group signatures with user-controlled and sequential linkability. In: Proc. of the 24th IACR Int'l Conf. on Practice and Theory of Public Key Cryptography. Springer, 2021. 360–388. [doi: 10.1007/978-3-030-75245-3_14]

[12] Langlois A, Ling S, Nguyen K, Wang HX. Lattice-based group signature scheme with verifier-local revocation. In: Proc. of the 17th Int'l Conf. on Public-key Cryptography. Buenos Aires: Springer, 2014. 345–361. [doi: 10.1007/978-3-642-54631-0_20]

[13] Fiore D, Garms L, Kolonelos D, Soriente C, Tucker I. Ring signatures with user-controlled linkability. In: Proc. of the 27th European Symp. on Research in Computer Security. Copenhagen: Springer, 2022. 405–426. [doi: 10.1007/978-3-031-17146-8_20]

[14] Bellare M, Poettering B, Stebila D. Deterring certificate subversion: Efficient double-authentication-preventing signatures. In: Proc. of the 2017 Int'l Conf. on Practice and Theory of Public-key Cryptography. Amsterdam: Springer, 2017. 121–151. [doi: 10.1007/978-3-662-54388-7_5]

[15] Ling S, Nguyen K, Wang HX, Xu YH. Lattice-based group signatures: Achieving full dynamicity with ease. In: Proc. of the 15th Int'l Conf. on Applied Cryptography and Network Security. Kanazawa: Springer, 2017. 293–312. [doi: 10.1007/978-3-319-61204-1_15]

[16] Esgin MF, Steinfeld R, Liu DX, Ruj S. Efficient hybrid exact/relaxed lattice proofs and applications to rounding and VRFs. In: Proc. of the 43rd Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2023. 484–517. [doi: 10.1007/978-3-031-38554-4_16]

[17] Lyubashevsky V, Nguyen NK, Plançon M, Seiler G. Shorter lattice-based group signatures via "almost free" encryption and other optimizations. In: Proc. of the 27th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Singapore: Springer, 2021. 218–248. [doi: 10.1007/978-3-030-92068-5_8]

[18] Libert B, Ling S, Nguyen K, Wang HX. Zero-knowledge arguments for lattice-based PRFs and applications to e-cash. In: Proc. of the 23rd Int'l Conf. on the Theory and Applications of Cryptology and Information Security. Hong Kong: Springer, 2017. 304–335. [doi: 10.1007/978-3-319-70700-6_11]

[19] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 2009, 56(6): 34. [doi: 10.1145/1568318.1568324]

[20] Banerjee A, Peikert C, Rosen A. Pseudorandom functions and lattices. In: Proc. of the 31st Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Cambridge: Springer, 2012. 719–737. [doi: 10.1007/978-3-642-29011-4_42]

[21] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proc. of the 40th Annual ACM Symp. on Theory of Computing. Victoria British: ACM, 2008. 197–206. [doi: 10.1145/1374376.1374407]

[22] Blömer J, Bobolz J, Porzenheim L. A generic construction of an anonymous reputation system and instantiations from lattices. In: Proc. of the 29th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Guangzhou: Springer, 2023. 418–452. [doi: 10.1007/978-981-99-8724-5_13]

[23] Gorbunov S, Vaikuntanathan V, Wichs D. Leveled fully homomorphic signatures from standard lattices. In: Proc. of the 47th Annual ACM Symp. on Theory of Computing. Portland: ACM, 2015. 469–477. [doi: 10.1145/2746539.2746576]

[24] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems. In: Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali. ACM, 2019. 203–225. [doi: 10.1145/3335741.3335750]

[25] Ling S, Nguyen K, Stehlé D, Wang HX. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In: Proc. of the 16th Int'l Conf. on Practice and Theory in Public-key Cryptography. Nara: Springer, 2013. 107–124. [doi: 10.1007/978-3-642-36362-7_8]

[26] Fouque PA, Hoffstein J, Kirchner P, *et al*. Falcon: Fast-Fourier lattice-based compact signatures over NTRU. 2019. https://api.semanticscholar.org/CorpusID:231637439

[27] Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, Stehlé D. CRYSTALS-dilithium: A lattice-based digital signature scheme. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2018, 2018(1): 238–268.

[28] Albrecht MR, Player R, Scott S. On the concrete hardness of learning with errors. Journal of Mathematical Cryptology, 2015, 9(3): 169–203. [doi: 10.1515/jmc-2015-0016]

[29] Ishai Y, Su H, Wu DJ. Shorter and faster post-quantum designated-verifier zkSNARKs from lattices. In: Proc. of the 2021 ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2021. 212–234. [doi: 10.1145/3460120.3484572]

[30] Huang XJ, Song JS, Li ZC. Dynamic group signature scheme on lattice with verifier-local revocation. Cryptology ePrint Archive, 2022/022, 2022.

附中文参考文献:

[3] 冯翰文, 刘建伟, 伍前红. 后量子安全的群签名和环签名. 密码学报, 2021, 8(2): 183–201. [doi: 10.13868/j.cnki.jcr.000430]

[4] 杨亚涛, 蔡居良, 张筱薇, 袁征. 基于 SM9 算法可证明安全的区块链隐私保护方案. 软件学报, 2019, 30(6): 1692–1704. http://www.jos.org.cn/1000-9825/5745.htm [doi: 10.13328/j.cnki.jos.005745]

陈颖(1999－), 女, 博士生, 主要研究领域为隐私保护, 格密码.

彭聪(1989－), 男, 博士, 副教授, 博士生导师, CCF 专业会员, 主要研究领域为抗量子密码, 身份隐私保护.

何德彪(1980－), 男, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为密码学, 信息安全.

罗敏(1974－), 男, 博士, 教授, 博士生导师, CCF 专业会员, 主要研究领域为信息安全, 可信软件, 数据挖掘.