计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(10):301−307 [doi: 10.15888/j.cnki.csa.009243]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

格上基于身份的代理签名方案①

姬蔚萍, 范士喜, 李子臣

(北京印刷学院 信息工程学院, 北京 102600)
通信作者: 李子臣, E-mail: lizc2020@163.com

摘　要: 为抵抗量子计算攻击, 降低代理签名中用户私钥泄露的风险, 构造了一个格上基于身份的代理签名方案. 方案的设计基于安全高效的 GPV 签名框架, 结合用户身份信息生成验证公钥, 使用格基委派技术生成用户签名私钥, 并使用盆景树代理委托算法提升签名效率. 方案的安全性可规约至格上最小整数解问题, 满足基于身份代理签名的安全属性, 且在随机谕言和量子随机谕言下均具有存在性不可伪造性.

关键词: 基于身份的代理签名; GPV 签名框架; 后量子密码; 格上最小整数解问题; 格基委派算法

引用格式: 姬蔚萍,范士喜,李子臣.格上基于身份的代理签名方案.计算机系统应用,2023,32(10):301–307. http://www.c-s-a.org.cn/1003-3254/9243.html

Identity-based Proxy Signature on Lattices

JI Wei-Ping, FAN Shi-Xi, LI Zi-Chen

(School of Information Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China)

Abstract: To resist quantum computing attacks and reduce the risk of private key leakage of users in proxy signatures, this study proposes an identity-based proxy signature scheme on lattices. This scheme is designed based on the secure and efficient GPV signature framework. The verification public key is generated by combining the user identity information. The lattice basis delegation technology is used to generate the private key for the user signature, and the bonsai tree delegation algorithm is adopted to improve signing efficiency. The security of the scheme is based on the shortest integer solution (SIS) assumption. It satisfies the security properties of identity-based proxy signatures and has existential unforgeability under random oracles and quantum random oracles.

Key words: identity-based proxy signature; GPV signature framework; post-quantum cryptography; shortest integer solution (SIS) assumption; basis delegation algorithm

数字签名是指只有信息发送者才能生成且其他任何人无法伪造的一段字符串, 这段字符串同时也是对信息的发送者所发送的信息是否真实有效的证明. 一个完备的数字签名通常需要定义两个互补运算, 一个用于签名, 另一个用于验证. 代理签名的特点在于可以在原始签名者无法签名的情况下进行签名权力的委托, 并完成安全的数字签名过程. 比如, 某单位负责人由于某些原因无法返回公司, 将公司相关事务委托给他的助理, 为赋予事务的办理权力, 负责人需要给予助理自己的公章, 让其能够代表公司在文件上盖章, 以上所述即为“代理”的过程. 因此可以看出, 代理签名具有不可替代的研究意义和应用前景.

1996 年, 代理签名的概念被 Mambo 等人[1] 提出, 该方案具有两个角色: 原始签名者 O (original signer)

① 基金项目: 国家自然科学基金 (61370188); 北京市教委科研计划 (KM202010015009, KM202310015002); 北京市教委科研计划 (KM202110015004); 北京市高等教育学会 2022 年立项面上攻关课题 (MS2022093); 北京印刷学院博士启动金 (27170120003/020, 27170122006); 北京印刷学院科研创新团队项目 (Eb202101); 北京印刷学院校内学科建设项目 (21090121021); 北京印刷学院重点教改项目 (22150121033/009); 北京印刷学院科研基础研究一般项目 (Ec202201)
收稿时间: 2023-02-22; 修改时间: 2023-04-07; 采用时间: 2023-04-23; csa 在线出版时间: 2023-07-21
CNKI 网络首发时间: 2023-07-21

和代理签名者 P (proxy signer) . 签名者 O 赋予代理签名者 P 签名的权力, P 在获得签名权力之后, 可以代替原始签名者 O 进行有效签名, 产生合法签名信息. 在此概念提出之后, 代理签名方案的研究如火如荼地进行, 基于离散对数的代理签名方案、基于大整数分解的代理签名以及基于双线性对映射上的代理签名方案等不断被提出[2−5]. 1984 年, Shamir[6] 首次提出了基于身份的签名方案, 身份的特殊属性可以使密钥管理过程更加简洁高效, 用户的身份信息即为用户公钥, 用户私钥通过主密钥以及用户身份 id 构造. 2005 年, Xu 等人[4] 基于椭圆曲线上的双线性对困难问题构建了第 1 个基于身份的代理签名方案, 但该方案缺少对于自适应选择身份攻击和选择消息攻击的安全性证明. 2006 年, Shim[7] 指出基于身份的代理签名所需的安全属性应包含不可伪造性、可验证性、强的身份可识别性、阻止误用性以及不可抵赖性. 2007 年, Wu 等人[8] 优化了基于身份地代理签名的安全概念, 并基于双线性对构造了一个高效的签名方案. 该方案可抵抗自适应选择明文攻击和选择身份伪造攻击. 2015 年, Gu 等人[9] 提出了一个标准模型下的签名框架, 并基于 CDH (computational Diffie-Hellman problem) 问题提出了一个可证安全的基于身份的代理签名方案.

随着后量子时代的到来, 传统公钥密码系统岌岌可危[10,11], 量子安全代理签名方案的研究已经成为当务之急. 2008 年, Gentry 等人[12] 创造性地提出了以困难格陷门为基础的 hash-and-sign 签名范式, 该签名范式是第 1 个公认安全高效的格上陷门方案, 此框架提出后, 格上数字签名得到快速发展. Cash 等人[13] 利用原像抽样函数构造了著名的格基委派算法, 并提出了第 1 个标准模型下可证安全的格签名方案. 文献 [14] 利用 Gentry 所提出的陷门构造方法提出了一种标准模型下基于格的代理签名方案. 之后, 文献 [15] 结合身份信息构造了一个基于身份的格代理签名方案, 但此方案只满足存在不可伪造性, 并未分析其他安全属性. 文献 [16] 基于格上短整数解和非均匀小整数解难题提出了第 1 种标准模型下基于身份的代理盲签名方案, 并分析了其不可伪造性. 文献 [17] 基于最小整数解问题在理想格上构造了一个基于身份的代理签名方案, 并证明了方案在选择身份和固定选择消息攻击下仍具有强不可伪造性, 但方案签名复杂度较高. 文献 [18] 构造了一种 NTRU 格上基于身份的代理签名方案, 由于 NTRU 的特性, 该方案在公钥和签名尺寸较短. 文献 [19] 提出了一种前向安全的格基代理签名, 但方案是以牺牲效率为代价来提升安全性.

本文基于 GPV 签名框架构建了一个基于身份的代理签名方案, 使用盆景树生长算法[13] 合成原始签名者 O 和代理签名者 P 各自的公钥矩阵, 利用格基委派算法提取身份 id 对应的用户私钥, 利用原像取样算法完成签名及验证过程. 经分析, 该方案安全性依赖于格上 SIS 困难问题, 且满足随机谕言机模型下选择身份和选择消息的存在不可伪造性、强的身份可识别性以及不可抵赖性.

1 相关知识

1.1 格上定义

定义 1. 最小整数解困难问题 (shortest integer solution, SIS). 给定正整数 q, m, n, 实数 $\beta > 0$, 选取随机均匀矩阵 $A \in \mathbb{Z}_q^{n\times m}$, 寻找一个非零向量 e, 使其满足 $Ae = 0 \pmod q$, 且 $\|e\| \leqslant \beta$ 是困难的.

定义 2. 原像取样函数 (preimage sampleable function, PSF). 即给定一个函数值, 求解其对应的原像. 算法输入矩阵 $A \in \mathbb{Z}_q^{n\times m}$, 及其格基 $T \in \mathbb{Z}_q^{m\times m}$, 向量 $u \in \mathbb{Z}_q^n$, 参数 $\sigma \geqslant \|\widetilde{T}_A\| \cdot \omega(\sqrt{\log n})$, 运行原像取样函数 $SamplePre(A, T, u, \sigma)$, 在多项式时间内输出满足 $Av = u \pmod q$ 的采样点 v.

定义 3. 格基委派算法 (lattice basis delegation). 给定整数 $m \geqslant 2n\log q$, 素数 $q \geqslant 2$, m, n 均为整数, 存在一个概率多项式时间算法 $SampleBasis(A, T_i)$, 其中 $i \in [k] = \{1, 2, \cdots, k\}$, $A = [A_1|\cdots|A_k] \in \mathbb{Z}_q^{n\times km}$ 为联合矩阵, T_i 是 A_i 的优质基. 运行算法输出为格 $\Lambda_q^{\perp}(A)$ 的随机优质基 $T \in \mathbb{Z}_q^{km\times km}$.

1.2 GPV 签名框架

2008 年, Gentry 等人[12] 设计了一个安全的基于格的数字签名框架. 该框架的安全性可归约于最小整数解问题, 在 SIS 困难问题的假设下, GPV 框架已被证明在 ROM (random oracle model) 和 QROM (quantum random oracle model) 下均有着的 EUF-CMA 安全性, 即适应性选择消息攻击下的存在不可伪造性. GPV 签名框架是格基签名方案的认证性理论基础, 具有安全简洁的特性, 其主要内容如下.

参数生成过程: 给定安全参数 n, 整数 (t_0, q, m), 常

数$\delta_1 \in (0,1)$, 高斯参数$\sigma \geqslant m^{1+\delta_1}\omega(\sqrt{\log m})$. 假设$H$: $\{0,1\}^* \to \mathbb{Z}_q^n$为抗碰撞哈希函数. 方案使用陷门生成算法$TrapGen(n,q,m)$获得矩阵$A \in Z_q^{n\times m}$以及陷门$T \in \mathbb{Z}_q^{m\times m}$, 并将他们作为公私钥$(pk,sk)$, 这里$AT = 0 \pmod q$, 且$\|\widetilde{T}\| \leqslant m^{1+\delta_1}$.

签名和验证过程: 对于消息M, 选取随机字符串$r \leftarrow \{0,1\}^{t_0}$, 计算$s \leftarrow SamplePre(A,T,H(M\|r),\sigma)$, 输出$(r,s)$即为消息$M$的签名. 验证时, 若有$r \leftarrow \{0,1\}^{t_0}$和等式$As = H(M\|r)$同时成立, 且满足$s \leqslant \sigma\sqrt{m}$, 则认为此签名合法; 否则, 拒绝签名.

2 格上基于身份的代理签名方案

本文在 GPV 签名框架基础上, 使用格基委派技术来产生代理签名密钥, 构建了一个基于身份的格上代理签名方案. 该方案共分为 5 个阶段, 分别为系统建立、密钥提取、代理授权委托、代理签名生成和签名验证. 方案流程图如图 1 所示, 方案使用符号及符号说明如表 1.

2.1 系统建立

$Setup(1^n)$: 输入整数$m \geqslant 5n\log q$, 实数$\beta = poly(n)$, $q > \beta\cdot\omega(\log n)$, 整数$l > 0$, 两个原像取样函数$SamplePre$的高斯参数$s_1, s_2$和两个格基派生函数$SampleBasis$的安全高斯参数$s_3$和$L$; 3 个安全的哈希函数, 分别记作:

$$\begin{cases} h_1 : \{0,1\}^* \times \{0,1\}^l \to \mathbb{Z}_q^n \\ h_2 : \{0,1\}^* \to \mathbb{Z}_q^n \\ h_3 : \{0,1\}^* \to \mathbb{Z}_q^{n\times 2m} \end{cases} \tag{1}$$

其中, h_1表示任意长度的随机字符串和长度为l的$\{0,1\}$字符串可转换为$\mathbb{Z}_q$上的多项式; h_2表示任意长度的$\{0,1\}$字符串可转换为$\mathbb{Z}_q$上的多项式; h_3表示任意长度的$\{0,1\}$字符串可转换为$\mathbb{Z}_q$上一个$n\times 2m$大小的矩阵.

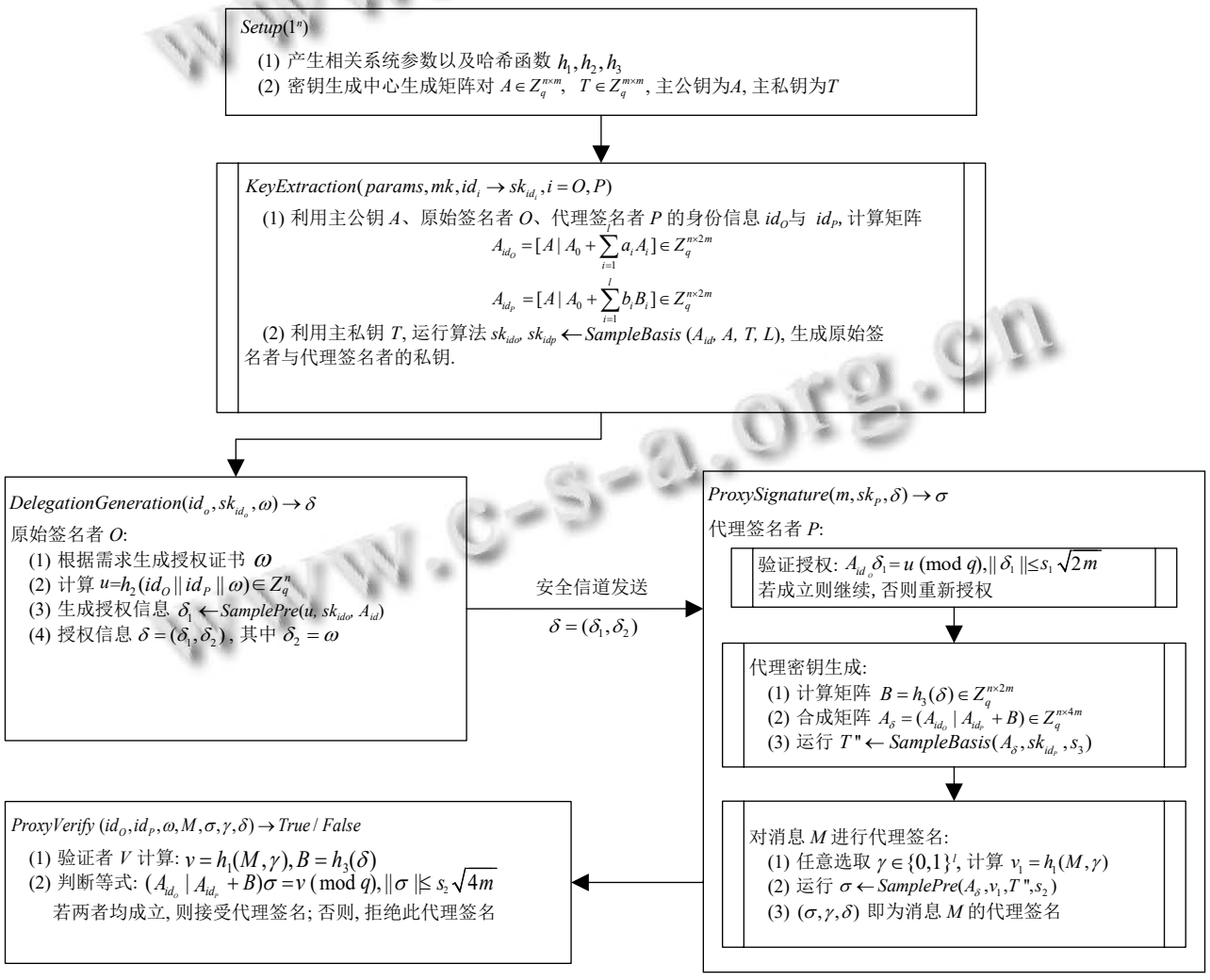

图 1 签名算法流程图

表 1 符号及符号说明

符号	符号说明
O	原始签名者
P	代理签名者
ω	授权证书
V	验证者
n	系统安全参数
$Poly(n)$	n的多项式函数
id_O	原始签名者的身份标识
id_P	代理签名者的身份标识

2.2 密钥提取

密钥提取阶段$KeyExtraction(params, mk, id)$输入公共参数, 主私钥以及用户身份 id, 生成原始签名者与代理签名者的用户私钥, 具体如下.

(1) 密钥生成中心运行算法$TrapGen$生成矩阵$A \in \mathbb{Z}_q^{n\times m}$以及格$\Lambda_q^{\perp}(A)$的一个陷门基$T \in \mathbb{Z}_q^{m\times m}$, 其中主公钥为$A$, 主私钥为$T$.

(2) 随机为 O 和 P 选取矩阵$A_0, A_1, \cdots, A_l \in \mathbb{Z}_q^{n\times m}$, 和$B_0, B_1, \cdots, B_l \in \mathbb{Z}_q^{n\times m}$, 结合主公钥 A 和 O 与 P 的身份信息id_O与id_P, 计算矩阵:

$$\begin{cases} A_{id_O} = \left[A|A_0 + \sum_{i=1}^{l} a_i A_i\right] \in Z_q^{n\times 2m} \\ A_{id_P} = \left[A|A_0 + \sum_{i=1}^{l} b_i B_i\right] \in Z_q^{n\times 2m} \end{cases} \tag{2}$$

其中, $id_O = (a_1, a_2, \cdots, a_l), id_P = (b_1, b_2, \cdots, b_l) \in \{0,1\}^l$.

(3) 利用主私钥T, 运行格基委派算法$SampleBasis(A_{id}, A, T, L)$, 其中$\|\widetilde{T}\|$与$\|T\|$正交, $L \geqslant \|\widetilde{T}\| \cdot \sqrt{2m} \cdot \omega(\sqrt{\log 2m})$. 输出格$\Lambda_q^{\perp}(A_{id_O})$和格$\Lambda_q^{\perp}(A_{id_P})$的一组短基$R_{id_O} \in \mathbb{Z}^{2m\times 2m}$和$R_{id_P} \in \mathbb{Z}^{2m\times 2m}$, 产生$O$的私钥$sk_{id_O} = R_{id_O}$和$P$的私钥$sk_{id_P} = R_{id_P}$, 且$\|\widetilde{R}_{id_i}\| \leqslant L, i = O, P$.

2.3 代理委托

代理委托算法$DelegationGeneration$用于确认代理签名者身份, 利用委托证书、原始签名者身份信息及其私钥, 生成授权信息, 具体如下.

(1) 原始签名者O根据需求生成授权证书ω, 授权证书中包含O和P的身份信息、代理授权期限以及代理授权范围等内容.

(2) 原始签名者O计算$u = h_2(id_O \| id_P \| \omega) \in Z_q^n$, 运行算法$\delta_1 \leftarrow SamplePre(u, sk_{id_O}, A_{id_O})$, 对$u$进行签名, 生成授权信息$\delta_1$, 同时, 令$\delta_2 = \omega$.

(3) 原始签名者O将$\delta = (\delta_1, \delta_2)$发送给代理签名者.

2.4 代理签名生成

代理签名算法$ProxySignature$输入消息M、代理签名者私钥以及授权信息, 产生对应代理签名, 具体过程如下.

(1) 代理签名者P收到δ后, 首先验证等式$A_{id_O}\delta_1 = u \pmod q$和$\|\delta_1\| \leqslant s_1\sqrt{2m}$是否成立. 若成立, 则接受授权, 否则需重新授权.

(2) 根据授权信息计算矩阵$B = h_3(\delta) \in Z_q^{n\times 2m}$, 再结合$O$和$P$的公钥$A_{id_O}$和$A_{id_P}$以及$P$的私钥$R_{id_P}$, 计算矩阵:

$$A_\delta = (A_{id_O}|A_{id_P} + B) \in Z_q^{n\times 4m} \tag{3}$$

运行$T'' \leftarrow SampleBasis(A_\delta, R_{id_P}, s_3)$生成代理签名密钥$T''$, 高斯参数$s_3$需满足$s_3 \geqslant \|R_{id_P}\| \cdot \sqrt{4m} \cdot \omega\sqrt{\log 4m}$.

(3) 对消息M进行代理签名, 过程如下.

1) 随机选取$\gamma \in \{0,1\}^l$, 计算$v_1 = h_1(M, \gamma)$.

2) 运行$\sigma \leftarrow SamplePre(A_\delta, v_1, T'', s_2)$生成$\sigma$.

3) (σ, γ, δ)即为消息M的代理签名.

2.5 签名验证

签名验证函数$ProxyVerify$输入对应的验证信息, 输出签名信息的正确性, 具体如下.

(1) 验证者V在已知公钥(id_O, id_P)的情况下, 计算$v = h_1(M, \gamma)$和$B = h_3(\delta)$.

(2) 判断两条件$(A_{id_O}|A_{id_P} + B)\sigma = v \pmod q$和$\|\sigma\| \leqslant s_2\sqrt{4m}$是否成立. 若两者均成立, 则代理签名合法; 否则, 此代理签名为非法签名.

3 安全性分析

3.1 不可伪造性

在分析代理签名的存在性伪造攻击时, 一般分为两类伪造者攻击.

第 1 类攻击中, 代理签名者并未被授权, 即此类伪造者已知代理签名者的公私钥和原始签名者的公钥.

第 2 类为原始签名者攻击, 是指恶意的原始签名者伪装成合法的代理签名者, 此类伪造者已经掌握原始签名者的公私钥和代理签名者的公钥.

定理 1. 如果本文提出的基于身份的代理签名方案被选择身份和固定选择消息攻击成功的概率ε不可忽略, 那么将存在一个算法Θ在多项式时间内可解决 SIS 问题. 因此在 SIS 问题难解的情况下, 该代理签名强不可被伪造.

证明: 假设存在敌手Γ, 通过q_1次h_1询问, q_2次h_2询问, q_3次h_3询问, 以及q_4次授权过程询问, q_5次签名询问, q_6次密钥提取询问, 能够成功地伪造出代理签名,

那么我们就可以利用敌手Γ构造一个多项式时间挑战者 C 解决 SIS 困难问题.

系统建立: 假设挑战者 C 接收到一个 SIS 困难问题的实例$A' \in Z_q^{n\times 4m}$, 希望找到能够满足$v \leqslant 2s\sqrt{4m}$和$A'v = 0 \pmod q$的向量v, 选取相关参数(h_1,h_2,h_3,q,m,n,s)发送给伪造者. 在整个询问过程中, 将产生 6 个对应于 3 个哈希函数、授权过程、代理签名和密钥提取过程的询问列表$\{L_i, i=1, 2, 3, 4, 5, 6\}$, 分别用来存储询问随机谕言机的结果. 挑战者 C 接收敌手Γ发送的(id_i, M), 其中$id_i \in \{0,1\}^l$为目标身份. 交互过程模拟如下.

(1) 密钥提取询问, 对于身份$\{id_i, i = O, P\}$, 敌手Γ会向挑战者发起相应的公私钥提取询问, 所需执行步骤为: 如果列表 L_2 中有记录, C 直接将对应值返回给伪造者; 如果没有, 则分两种情况, 若$id_i' = id_i$, 则终止询问; 若$id_i' \neq id_i$, 则 C 随机选取R'_{id_i}, 伪造者Γ将(id_i', R'_{id_i})返回给挑战者 C, 并将其存储在列表 L_6 中.

(2) 哈希函数h_2询问, 对于身份$\{id_i, i = O, P\}$对应的授权证书ω', 首先计算哈希函数$h_2(id'_O \| id'_P \| \omega')$, 在这个过程中, 挑战者 C 查询列表 L_2, 观察列表数据是否已有记录, 若有查询记录则返回列表中的值, 否则, 随机选择u', 伪造者接收对应的数据, 并保存(id_i', ω', u')在 L_2 中.

(3) 授权委托询问, 挑战者 C 先确定列表 L_4 中是否存在ω'的询问记录, 若不存在, 则进一步查看 L_2, 观察其是否进行过h_2询问, 若存在记录, 则取对应的值(id_i', ω', u'), 这里一般假设在进行授权委托询问之前已经进行过h_2询问, 运行原像采样算法生成对应代理签名授权信息:$\delta_1' \leftarrow SamplePre(u', R_{id_O}, A_{id_O}) \in \mathbb{Z}^{2m}$, 令$\delta_2' = \omega'$, 将授权信息$\delta' = (\delta_1', \delta_2')$秘密地发送给代理签名者, 并将其存入列表 L_4.

(4) 哈希函数h_3询问, h_3主要用于生成B', 在此过程中, 挑战者检查列表 L_3 是否被询问过, 如果 L_3 中有B'的询问记录, 则伪造者Γ直接提取对应数据, 否则挑战者需要从h_3的值域中选取矩阵$B' \in Z_q^{n\times 2m}$, 将(δ', B')保存在列表 L_3 中, 并将B'发送给伪造者Γ. 伪造者通过随机选取id_P的私钥$sk_p' \in \mathbb{Z}_q^{n\times 2m}$来生成代理签名密钥, 过程如下.

1) 计算矩阵$A'_\delta = (A_{id_O} | A_{id_P} + B') \in \mathbb{Z}_q^{n\times 4m}$.

2) 生成代理密钥$T' \leftarrow SampleBasis(A'_\delta, R'_{id_P}, s_3)$, 其中$s_3' \geqslant \|R'_{id_P}\| \cdot \sqrt{4m} \cdot \omega\sqrt{\log 4m}$.

3) 将(A'_δ, T', s_3')存储在列表 L_3 中.

(5) 哈希函数h_1询问, h_1用于产生消息M'的杂凑值, 挑战者需要查询列表 L_1 中是否存在对应记录, 若存在, 则直接将列表对应内容返回给伪造者; 否则, 随机选取$\gamma' \in \{0,1\}^l$和向量$v' \in \mathbb{Z}_q^n$, 通过格基派生算法生成满足$A'_\delta \sigma' = v' \pmod q$的向量$\sigma'$, 最后挑战者将$(M', \sigma', \gamma', v')$存入列表 L_1, 并将(M', v', γ')返回给伪造者.

(6) 代理签名询问, 挑战者首先检查列表 L_5 中对于消息M'的询问记录, 若存在, 则直接返回给伪造者, 若不存在, 则先访问列表 L_1 查找σ'和γ', 再访问列表 L_3 查找向量δ', 然后将$(\sigma', \gamma', \delta')$作为代理签名返回, 同时将$(M', \sigma', \gamma', \delta')$存储到列表 L_5. 若M'在列表 L_1 和 L_2 中没有记录, 则需要进行h_1, h_2, h_3询问, 得到相应的$\sigma', \gamma', \delta'$值.

第 1 类伪造者攻击: 在结束以上 6 组问询以后, 伪造者Γ_1以ε的概率伪造出代理签名$(M^*, \sigma^*, \gamma^*, \delta^*)$. 第 1 类伪造者攻击为未经授权的代理签名者攻击, 此类情况下, 挑战者已知 P 的公私钥和 O 的公钥, 但未知 O 的私钥. 至此, 模拟挑战者可根据其列表中的查询记录和伪造的代理签名$(M^*, \sigma^*, \gamma^*, \delta^*)$成功找到 SIS 问题的实例.

首先, 在授权阶段, 由于未知 O 的私钥而随机产生授权信息δ', 其验证部分分别为:

$$A'_{id_O}\delta_1' = u' \pmod q \tag{4}$$

$$A'_{id_O}\delta_1'^{*} = u'^{*} \pmod q \tag{5}$$

已知$u' = u'^{*} = h_2(id'_O \| id'_P \| \omega')$, 则有:

$$A'_{id_O}(\delta_1' - \delta_1'^{*}) = 0 \pmod q \tag{6}$$

根据格上小整数解问题的困难性可知, 极大概率有$\delta_1' \neq \delta_1'^{*}$, 因此, 此阶段伪造授权信息的概率可忽略, 即授权信息不可伪造. 再对用户 id 的私钥进行提取询问, 由于授权信息不可伪造, 则$B = h_3(\delta') \in Z_q^{n\times 2m}$是正确的, 记为$B'^{*}$. 挑战者再通过查询所有列表的问询记录, 获取对应签名信息$(M'^{*}, \sigma'^{*}, \gamma'^{*}, \delta'^{*})$, 计算可得:

$$(A_{id_O} | A_{id_P} + B'^{*})\sigma' = v'^{*} \pmod q,\ \sigma' \leqslant s\sqrt{4m} \tag{7}$$

$$(A_{id_O} | A_{id_P} + B'^{*})\sigma'^{*} = v'^{*} \pmod q,\ \sigma'^{*} \leqslant s\sqrt{4m} \tag{8}$$

由上可知$\|\sigma' - \sigma'^{*}\| \leqslant 2s\sqrt{4m}$, 若此时有$\sigma' \neq \sigma'^{*}$, 则我们可得出 SIS 问题$(A', q, m, n, s)$的一个实例解. 但由格上问题的困难性可知, Γ_1能够伪造出有效签名的概率极小, 同时根据原像最小熵性质, 熵越大, 概率越小. 在签名未询问时, 挑战者 C 利用$SampleDom$算法选取伪造签名信息的最小熵为$\omega(\log n)$, 因此$\sigma' \neq \sigma'^{*}$的概率为$1 - 2^{-\omega\log n}$. 综上所述, 在第 1 类伪造者攻击下此代理签名不可伪造.

第 2 类伪造者攻击: 在结束以上 6 组问询以后, 伪造者Γ_2能够以ε的概率伪造出代理签名$(M^*,\sigma^*,\gamma^*,\delta^*)$. 第 2 类伪造者攻击为恶意的代理签名者攻击, 此类情况下, 挑战者已知 P 的公钥和 O 的公私钥, 但未知 P 的私钥. 模拟挑战者通过查询所有问询记录, 获取对应签名信息$(M'^*,\sigma'^*,\gamma'^*,\delta'^*)$, 计算可得:

$$(A_{id_O}|A_{id_P}+B'^*)\sigma'^*=v'^*\ (\bmod\ q),\ \sigma'^*\leqslant s\sqrt{4m} \tag{9}$$

$$(A_{id_O}|A_{id_P}+B'^*)\sigma'=v'^*\ (\bmod\ q),\ \sigma'\leqslant s\sqrt{4m} \tag{10}$$

故有$\|\sigma'-\sigma'^*\|\leqslant 2s\sqrt{4m}$, 如果$\sigma'\neq\sigma'^*$, 得到一个 SIS 的解, 上述两等式进行变换如下:

$$\begin{aligned}(A_{id_O}|A_{id_P}+B'^*)\sigma'^*&=(A_{id_O}|A_{id_P}+A_{id_O}|B'^*)\sigma'^*\\&=(A_{id_O}|A_{id_P})\sigma'^*+(A_{id_O}|B'^*)\sigma'^*\\&=v'^*\ (\bmod\ q)\end{aligned} \tag{11}$$

$$\begin{aligned}(A_{id_O}|A_{id_P}+B'^*)\sigma'&=(A_{id_O}|A_{id_P}+A_{id_O}|B'^*)\sigma'\\&=(A_{id_O}|A_{id_P})\sigma'+(A_{id_O}|B'^*)\sigma'\\&=v'^*\ (\bmod\ q)\end{aligned} \tag{12}$$

其中, $\sigma'^*=(\sigma_1'^*|\sigma_2'^*),\sigma'=(\sigma_1'|\sigma_2')$, 然后计算$A_{id_P}(\sigma_2'^*-\sigma_2')=0\ (\bmod\ q)$, 且$\sigma_1'^*,\sigma_2'^*,\sigma_1',\sigma_2'\in\mathbb{Z}^{2m}$, 即可得到平均情况下 SIS 困难问题的一个实例解. 由小整数解问题的困难性得, Γ_2能够伪造出有效签名的概率极小, 因此, 在第 2 类伪造者攻击下此基于身份的代理签名不可伪造. 至此, 定理 1 得证.

此外, 在 2011 年, Boneh 等人[20] 考虑到敌手能访问量子叠加态的情况, 提出了 QROM (quantum random oracle model) 安全模型, 并证明 GPV 签名框架在量子随机谕言模型下也是安全的. 之后 Katsumata 等人[21] 对基于身份的 GPV-IBE 方案在 QROM 下进行了更加严密的安全性证明. 由于本文方案是基于身份 ID 以及在 GPV 框架内构造, 因此本文方案亦具有 QROM 下的安全性, 在此不再论证.

3.2 强的身份可确定性

首先, 在一个有效的代理签名中存在一个授权证书ω, 对于原始签名者O和代理签名者P, 该授权证书ω与原始签名者和代理签名者的公钥必须出现在代理签名的验证方程中. 且代理签名者P和原始签名者O的签名私钥不同, 因此他们在同一消息上的签名不同, 验证公钥也不同, 区分代理签名和原始签名是较为容易的.

其次, 由于授权证书ω包含在有效的代理签名中, 因此任何人都可以从授权证书ω确定相应的代理签名者的身份. 当验证者V接收到签名信息元组$(id_O,id_P,A,\omega,M,\sigma,\gamma,\delta)$后, 首先通过授权证书$\omega$确定代理签名者的身份信息$id_P$; 之后通过已公布的验证公钥运行$ProxyVerify$算法验证签名, 如果验证成功, 则说明代理签名者的身份信息为id_P, 保证了该方案强的身份可确定性.

3.3 不可抵赖性

首先, 在本文方案的代理授权过程中, 授权信息是通过原始签名者 O 的私钥R_O运行签名算法产生的, 之后授权信息被发送给代理签名者 P, 因此原始签名者 O 不可否认自己的授权信息.

其次, 已知一个有效的代理签名包含授权证书ω, 且ω必须在验证阶段进行验证, 代理签名人不能修改授权ω. 由于只有代理签名者拥有代理签名密钥, 所以他不能拒绝使用他的代理验证密钥验证的签名. 因此, 一旦代理签名人创建了原始签名人的有效代理签名, 他就不能否认签名的创建. 综上, 本签名方案具有不可抵赖性.

4 性能分析

本文方案基于 GPV 签名框架构造, 在身份授权过程使用格基委派技术, 产生安全的代理签名密钥. 将此方案与其他代理签名方案进行计算复杂度对比, 结果如表 2 所示. 表中所采用的安全参数均为$m\geqslant 5n\log q$, $\beta=poly(n)$, $q>\beta\cdot\omega(\log n)$, $C_{TG/1}$表示调用一次$TrapGen$函数, $C_{SB/1}$表示调用一次$SampleBasis$函数, $C_{SP/1}$表示调用一次$SamplePre$函数, $C_{H/1}$表示一次哈希函数的运算, $C_{V/1}$表示一次矩阵的乘法运算.

表 2 方案计算性能对比

方案	签名过程	验证过程
文献[22]	$C_{TG/2}+C_{SB/1}+C_{SP/2}+C_{H/2}+C_{V/2}$	$C_{H/2}+C_{V/4}$
文献[23]	$C_{TG/2}+C_{SB/1}+C_{SP/2}+C_{H/3}$	$C_{H/3}+C_{V/2}$
本文方案	$C_{TG/1}+C_{SB/2}+C_{SP/2}+C_{H/3}$	$C_{H/2}+C_{V/1}$

由表 2 可知, 本文方案的签名以及验证过程的计算复杂度均优于其他方案, 且增加了身份 id 的可识别性, 具有强的身份可确定性. 但同时方案也存在不足之处, 与其他方案相比较, 虽提升了签名安全性, 但方案通信效率无明显改进, 需进一步研究.

5 总结与展望

随着后量子时代的快速发展, 格上代理签名的研究已经刻不容缓. 本文基于 GPV 签名框架构造了一个格上基于身份的代理签名方案, 使用格基委派技术生成代理签名密钥, 其安全性可归约于格上 SIS 平均困难问题, 且经论证, 方案具有 ROM 和 QROM 下的不可伪造性、强的身份可确定性以及不可抵赖性等安全特

性. 与其他方案相比, 该方案具有计算复杂度低、抗量子攻击的特点.

为提升方案安全性, 方案在代理授权阶段使用了格基派生技术来生成代理签名密钥, 因此如何在保证签名内容和用户信息安全的同时减少通信开销, 将是下一步的研究方向. 在此基础上, 未来将测试方案在软硬件平台上的可行性, 本方案主要涉及模运算以及矩阵乘法, 因此计算复杂度较低, 采样过程采用离散高斯采样器, 或采用快速傅里叶算法来提升运行效率, 以尽量降低算法复杂度为目标来完成软硬件平台上的实现.

参考文献

1 Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation. Proceedings of the 3rd ACM Conference on Computer and Communications Security. New Delhi: ACM Press, 1996. 48–57.

2 Shao ZH. Provably secure proxy-protected signature schemes based on RSA. Computers & Electrical Engineering, 2009, 35(3): 497–505.

3 Zhang FG, Safavi-Naini R, Lin CY. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairing. IACR Cryptology ePrint Archive, 2003. 104.

4 Xu J, Zhang ZF, Feng DG. ID-based proxy signature using bilinear pairings. Proceedings of the 2005 International Symposium on Parallel and Distributed Processing and Applications. Nanjing: Springer, 2005. 359–367.

5 Jiang YL, Kong FY, Ju XL. Lattice-based proxy signature. Proceedings of the 2010 International Conference on Computational Intelligence and Security. Nanning: IEEE Press, 2010. 382–385. [doi: 10.1109/CIS.2010.88]

6 Shamir A. Identity-based cryptosystems and signature schemes. Proceedings of the 1984 Workshop on the Theory and Application of Cryptographic Techniques. Springer, 1984. 47–53. [doi: 10.1007/3-540-39568-7_5.]

7 Shim KA. An identity-based proxy signature scheme from pairings. Proceedings of the 8th International Conference on Information and Communications Security. Raleigh: Springer, 2006. 60–71. [doi: 10.1007/11935308_5]

8 Wu W, Mu Y, Susilo W, *et al*. Identity-based proxy signature from pairings. Proceedings of the 4th International Conference on Autonomic and Trusted Computing. Hong Kong: Springer, 2007. 22–31. [doi: 10.1007/978-3-540-73547-2_5]

9 Gu K, Jia WJ, Jiang CL. Efficient identity-based proxy signature in the standard model. The Computer Journal, 2015, 58(4): 792–807. [doi: 10.1093/comjnl/bxt132]

10 Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe: IEEE Press, 1994. 124–134. [doi: 10.1109/SFCS.1994.365700]

11 Li J, Pan ZS, Zheng J, *et al*. The security analysis of Quantum SAGR04 protocol in collective-rotation noise channel. Chinese Journal of Electronics, 2015, 24(4): 689–693. [doi: 10.1049/cje.2015.10.005]

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

13 Cash D, Hofheinz D, Kiltz E, *et al*. Bonsai trees, or how to delegate a lattice basis. Journal of Cryptology, 2012, 25(4): 601–639. [doi: 10.1007/s00145-011-9105-2]

14 余磊. 一种基于格的代理签名方案. 计算机工程, 2013, 39(10): 123–126, 132.

15 Kim KS, Hong D, Jeong IR. Identity-based proxy signature from lattices. Journal of Communications and Networks, 2013, 15(1): 1–7. [doi: 10.1109/JCN.2013.000003]

16 Zhang LL, Ma YQ. A lattice-based identity-based proxy blind signature scheme in the standard model. Mathematical Problems in Engineering, 2014, 2014(1): 307637. [doi: 10.1155/2014/307637]

17 欧海文, 范祯, 蔡斌思, 等. 理想格上基于身份的代理签名. 计算机应用与软件, 2018, 35(1): 312–317.

18 Zhu HF, Tan YA, Yu X, *et al*. An identity-based proxy signature on NTRU lattice. Chinese Journal of Electronics, 2018, 27(2): 297–303. [doi: 10.1049/cje.2017.09.008]

19 谢佳, 胡予濮, 江明明. 前向安全的格基代理签名. 计算机研究与发展, 2021, 58(3): 583–597.

20 Boneh D, Dagdelen Ö, Fischlin M, *et al*. Random oracles in a quantum world. Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security. Seoul: Springer, 2010. 41–69.

21 Katsumata S, Yamada S, Yamakawa T. Tighter security proofs for GPV-IBE in the quantum random oracle model. Journal of Cryptology, 2021, 34(1): 5. [doi: 10.1007/s00145-020-09371-y]

22 江明明, 胡予濮, 王保仓, 等. 格上的高效代理签名. 北京邮电大学学报, 2014, 37(3): 89–92.

23 乔莉. 基于格的代理签名方案的研究 [硕士学位论文]. 成都: 电子科技大学, 2016.

(校对责编: 孙君艳)