格上基于身份的变色龙签名方案

张彦华*① 陈 岩① 刘西蒙② 尹毅峰① 胡予濮③
①(郑州轻工业大学计算机与通信工程学院 郑州 450001)
②(福州大学数学与计算机科学学院 福州 350108)
③(西安电子科技大学通信工程学院 西安 710071)

摘 要：变色龙签名(CS)是一种比较理想的指定验证者签名，其采用变色龙哈希函数来实现签名的不可传递性，使得任意第三方不信任指定验证者所披露的内容，且避免了不可否认签名必须在线交互验证的缺陷。在满足不可传递性的同时，变色龙签名还要求满足不可伪造性以及签名者可拒绝性和不可抵赖性等。针对基于大整数分解或离散对数等数论难题的变色龙签名无法抵御量子计算机攻击，以及用户对公钥数字证书依赖的问题，该文给出了格上基于身份的变色龙签名(IBCS)，新方案避免了已有方案存在的签名者无法拒绝指定验证者伪造的签名的安全性漏洞，并将最终签名的传输开销由平方级降为线性级；进一步地，针对变色龙签名在仲裁阶段不可传递性失效的问题，给出了格上抗消息暴露的基于身份的变色龙签名，新方案使得签名者能够在不暴露消息内容的条件下拒绝任意敌手伪造的变色龙签名。特别地，基于格上经典的小整数解问题，两个方案在随机预言机模型下是可证明安全的。

关键词：变色龙签名；格；基于身份的密码；不可传递性；抗消息暴露
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2024)02-0757-08
DOI: 10.11999/JEIT230155

Identity-Based Chameleon Signature Schemes over Lattices

ZHANG Yanhua① CHEN Yan① LIU Ximeng② YIN Yifeng① HU Yupu③
①(*College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450001, *China*)
②(*College of Mathematics and Computer Science, Fuzhou University, Fuzhou* 350108, *China*)
③(*School of Telecommunications Engineering, Xidian University, Xi'an* 710071, *China*)

Abstract: Chameleon Signature (CS) is an ideal designated verifier signature, it realizes non-transferability by using chameleon hash function, makes any third party distrust the content disclosed by a designated verifier, and avoids the shortcoming of online interactive verification of undeniable signature. In addition to non-transferability, CS also should satisfy unforgeability, deniability, non-repudiation for the signer, and so on. To solve the problems that cryptosystems based on the number theory problems such as integer factorization or discrete logarithm cannot resist quantum computing attacks and users rely on digital certificates, an Identity-Based Chameleon Signature (IBCS) over lattices is proposed, the new scheme avoids the security vulnerability that the signer cannot reject the forged signature of the designated verifier in the existing schemes, and reduces the transmission cost of the final signature from square to linear; Furthermore, to solve the failure problem of non-transferability in the arbitration phase, an IBCS scheme with exposure-freeness over lattices is proposed, the new scheme enables the signer to reject a forged signature of any adversary without exposing the real message. Particularly, based on the hardness of the small integer solution problem, both schemes can be proved secure in the random oracle model.

收稿日期：2023-03-14；改回日期：2023-07-12；网络出版：2023-07-21
*通信作者： 张彦华 yhzhang@email.zzuli.edu.cn
基金项目：国家自然科学基金(61802075)，河南省自然科学基金(222300420371，202300410508)，河南省网络密码技术重点实验室开放课题(LNCT2022-A09)，河南省高等学校重点科研项目(22A520047)
Foundation Items: The National Natural Science Foundation of China (61802075), The Natural Science Foundation of Henan Province (222300420371, 202300410508), The Open Subjects of Henan Provincial Key Laboratory of Network Cryptography (LNCT2022-A09), The Key Scientific Research Project of Higher Education of Henan Province (22A520047)

Key words: Chameleon Signature (CS); Lattice; Identity-based cryptography; Non-transferability; Exposure-freeness

1 引言

一个传统的数字签名应该是公开可验证、可传递且不可伪造的，即任意用户都能够验证并相信(或拒绝)某文件的真实性及其签名者的身份信息。然而，这些性质无法满足某些旨在防止验证者对文件内容传播的特殊场景。1989年，Chaum和Van Antwerpen[1]提出的不可否认签名(Undeniable Signature, US)要求验证者在尝试验证前必须向签名者发出在线请求，且不可避免地涉及繁重的零知识证明系统，致使签名效率普遍不高。1996年，Jakobsson等人[2]提出了指定验证者签名(Designated Verifier Signature, DVS)，签名者和指定验证者拥有同等级的签名权限，除二者之外的任意第三方均无法确认签名的真实生成者，因此，当双方对签名的真伪产生争议时无法提供任何仲裁手段。1998年，Krawczyk和Rabin[3]提出的变色龙签名(Chameleon Signature, CS)更巧妙地解决了指定验证者对被签名的文件二次传递的问题。

相较于US和DVS, CS同样能够实现不可传递性，且不使用复杂的交互协议，避免了US中为设计零知识证明系统而产生的复杂性。特别地，CS通过在签名算法中嵌入变色龙哈希函数，使得持有该函数陷门的验证者获得伪造签名的能力，进而使得验证者二次传递的签名在第三方面前“失信”。此外，对于指定验证者伪造的签名，签名者有能力说服仲裁者予以拒绝，即满足签名者可拒绝性；而对于签名者真实生成的签名，签名者无法否认，即满足不可抵赖性。1984年，Shamir[4]提出基于身份的密码体制，用户的公钥可根据身份标识公开计算，相应的私钥由私钥生成器(Private Key Generator, PKG)根据身份为其派发，因此不再依赖传统公钥密码系统的数字证书。结合基于身份的密码体制的优点和变色龙签名的安全特性，基于身份的变色龙签名在云医疗系统、版权保护、电子竞拍及在线/离线签名等应用场景中尤为适用[5-8]。

基于经典数论难题的密码体制无法抵御量子计算机的攻击，这意味着后量子时代大多数现有密码方案将在多项式时间内被攻破[9,10]。具备抗量子计算攻击特性的格密码体制之所以脱颖而出，得益于格上轻量级的代数运算，且格上一些困难问题的难度存在平均情况到最坏情况的安全规约。2010年，Cash等人[11]设计出格上变色龙哈希函数。2013年，谢璇等人[12]宣称构造了格上首个CS方案，但是不满足签名者可拒绝性，且签名中必须携带的大尺寸矩阵严重影响了传输效率。2016年，Noh等人[13]构造了格上强指定验证者签名方案，缺陷是无法解决签名者和指定验证者的争议问题。2017年，Xie等人[14]提出了同态变色龙哈希函数的概念，并宣称构造了一个格上有限级数全同态签名方案，缺陷是同态变色龙哈希函数的设计存在天然的计算错误。2021年，Thanalakshmi等人[15]构造了基于哈希的CS方案，缺陷是签名者和指定验证者必须各自存储一个复杂的有向无环图，且签名的生成过程比较繁琐。

进一步地，现有的大多数CS方案在解决签名争议时，往往要求签名者向仲裁者(一个可信的第三方)出示真实的消息和签名，进而与指定验证者的伪造产生变色龙哈希函数的碰撞。由于除指定验证者外任何用户都不具备伪造的能力，这足以证明签名者未对假消息进行过签名。然而，一旦签名者发起对某个伪造的“打假”，也意味着其本欲保护的签名失去了不可传递性。

该文提出了格上基于身份的变色龙签名(Identity-Based CS, IBCS)方案，避免了文献[12]中存在的任意第三方可伪造签名和签名者无法拒绝指定验证者伪造的签名的安全性漏洞，并将最终签名的传输开销由平方级降为线性级。在此基础上，给出的变色龙签名方案2能够在签名者不暴露消息内容的条件下辅助仲裁者拒绝任意敌手伪造的签名。假设平均情况下的小整数解(Small Integer Solution, SIS)问题是困难的，在随机预言机模型下严格证明了两个方案满足抗选择身份和自适应性选择消息攻击下强不可伪造性、签名不可传递性、签名者可拒绝性和不可抵赖性，以及方案2的抗消息暴露性。

2 预备知识

2.1 格理论

定义1[16] 设q, n和m为正整数，给定矩阵$\boldsymbol{A}\in Z_q^{n\times m}$和向量$\boldsymbol{u}\in Z_q^n$，有以下定义：

$$\begin{aligned}&\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in Z^m:\boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q\},\\&\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})=\{\boldsymbol{e}\in Z^m:\boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{u}\bmod q\}\end{aligned}\tag{1}$$

定义2[16] 设m为正整数，给定$\boldsymbol{c}\in R^m$和$\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2\Big/s^2\right)$，有以下定义：

$\mathcal{D}_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\rho_{s,\boldsymbol{c}}(\boldsymbol{x})\Big/\sum_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$：一个$m$维格$\Lambda$上以$\boldsymbol{c}$为中心，$s\in R^+$为高斯参数的离散高斯分布。

定义3[16,17] 给定素数q，矩阵$\boldsymbol{A}\in Z_q^{n\times m}$和实

数$\beta>0$，小整数解问题$\mathrm{SIS}_{q,m,\beta}$定义为：求解齐次线性方程组$\boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q$的非零小尺寸整数解$\boldsymbol{e}\in Z^m$，满足$0<\|\boldsymbol{e}\|\le\beta$。

引理1[16,17]　设整数m，实数$\beta=\mathrm{poly}(n)$，素数$q\ge\beta\cdot\omega\left(\sqrt{n\log_2 n}\right)$和渐进因子$\gamma\ge\beta\cdot\tilde{\mathcal{O}}(\sqrt{n})$，则平均情况下的$\mathrm{SIS}_{q,m,\beta}$问题与最坏情况下的最短独立向量组问题$\mathrm{SIVP}_\gamma$的困难性是等价的。

引理2[17-19]　设素数$q\ge 2$，存在概率多项式时间(Probabilistic Polynomial Time, PPT)算法TrapGen，输入q，n和$m\ge 2n\log_2 q$，输出$\boldsymbol{A}\in Z_q^{n\times m}$和$\Lambda_q^{\perp}(\boldsymbol{A})$的一组陷门$\boldsymbol{T_A}$，其中$\boldsymbol{A}$统计接近$Z_q^{n\times m}$上的均匀分布$\mathcal{U}$。

引理3[16]　设素数$q\ge 2$，整数$m\ge 2n\log_2 q$，参数$s\ge\omega\left(\sqrt{\log_2 m}\right)$，若$\boldsymbol{A}\in Z_q^{n\times m}$的列向量可生成$Z_q^n$，则对于任意的$\boldsymbol{e}\in\mathcal{D}_{Z^m,s}$，$\boldsymbol{A}\cdot\boldsymbol{e}\bmod q$统计接近$Z_q^n$上的均匀分布$\mathcal{U}$。

引理4[20]　设素数$q>2$，整数$m>2n\log_2 q$，存在PPT算法BasisDel，输入$\boldsymbol{A}\in Z_q^{n\times m}$，$R\in\mathcal{D}m\times m$，$\Lambda_q^{\perp}(\boldsymbol{A})$的陷门$\boldsymbol{T_A}$和参数$s>\left\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\right\|\cdot s_{\boldsymbol{R}}\sqrt{m}\cdot\omega\left(\log_2^{3/2} m\right)$，输出$\Lambda_q^{\perp}\left(\boldsymbol{B}=\boldsymbol{A}\cdot\boldsymbol{R}^{-1}\right)$的陷门$\boldsymbol{T_B}\in Z^{m\times m}$，其中$\mathcal{D}m\times m$是$Z^{m\times m}$上$\bmod q$可逆且列向量服从$\mathcal{D}_{Z^m,s_{\boldsymbol{R}}}$的分布，$s_{\boldsymbol{R}}=\sqrt{n\log_2 q}\cdot\omega\left(\sqrt{\log_2 m}\right)$。

引理5[20]　设素数$q>2$，整数$m>2n\log_2 q$，存在PPT算法SampleRwithBasis，输入$\boldsymbol{A}\in Z_q^{n\times m}$，输出可逆矩阵$R\in\mathcal{D}m\times m$和$\Lambda_q^{\perp}(\boldsymbol{B})$的陷门$\boldsymbol{T_B}$，其中$\boldsymbol{B}=\boldsymbol{A}\cdot\boldsymbol{R}^{-1}$统计接近$Z_q^{n\times m}$上的均匀分布。

引理6[16]　设素数$q\ge 2$，整数$m\ge 2n\log_2 q$，存在PPT算法SamplePre，输入$\boldsymbol{A}\in Z_q^{n\times m}$，$\Lambda_q^{\perp}(\boldsymbol{A})$的陷门$\boldsymbol{T_A}$，参数$s>\left\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\right\|\cdot\omega\left(\sqrt{\log_2 m}\right)$和$\boldsymbol{u}\in Z_q^n$，输出统计接近$\mathcal{D}_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}),s}$的短向量$\boldsymbol{e}\in Z^m$，满足$\boldsymbol{u}=\boldsymbol{A}\cdot\boldsymbol{e}\bmod q$。

2.2 基于身份的变色龙签名

令消息空间为$\mathcal{M}$，身份空间为$\mathcal{ID}$，随机数空间为$\mathcal{R}$以及签名空间为$\mathcal{S}$。基于身份的变色龙签名[5]由以下5个多项式时间算法构成：

Setup：由PKG运行的概率性算法。输入安全参数λ，输出公共参数pp和系统主私钥msk。特别地，pp是以下算法的一个公共输入。

KeyGen：由PKG运行的概率性算法。输入主私钥msk以及身份$\mathrm{id}\in\mathcal{ID}$，输出与id相关联的私钥$\mathrm{sk}_{\mathrm{id}}$。

Sign：由身份为id_S的用户运行的概率性算法。输入签名者身份$\mathrm{id}_S\in\mathcal{ID}$，指定验证者身份$\mathrm{id}_V\in\mathcal{ID}$，签名者私钥$\mathrm{sk}_{\mathrm{id}_S}$以及消息$\mu\in\mathcal{M}$，输出随机数$r\in\mathcal{R}$和签名值$\sigma\in\mathcal{S}$。

Verify：由身份为id_V的用户运行的确定性算法。输入签名者身份$\mathrm{id}_S\in\mathcal{ID}$，指定验证者身份$\mathrm{id}_V\in\mathcal{ID}$，消息$\mu\in\mathcal{M}$，随机数$r\in\mathcal{R}$以及签名值$\sigma\in\mathcal{S}$，输出1或0。

Forge：由身份为id_V的用户运行的概率性算法。输入指定验证者身份$\mathrm{id}_V\in\mathcal{ID}$，私钥$\mathrm{sk}_{\mathrm{id}_V}$，消息$\mu\in\mathcal{M}$以及由签名者$\mathrm{id}_S\in\mathcal{ID}$运行算法Sign生成的随机数$r\in\mathcal{R}$和签名值$\sigma\in\mathcal{S}$，输出新消息$\mu'\in\mathcal{M}$和随机数$r'\in\mathcal{R}$，满足$\mathrm{Verify}(\mathrm{pp},\mathrm{id}_S,\mathrm{id}_V,\mu',r',\sigma)\to 1$。

一个安全的IBCS方案需满足以下性质：

定义4[5]　若对于任意的PPT敌手$\mathcal{A}$在以下游戏中的优势$\mathrm{Adv}_{\mathrm{IBCS},\mathcal{A}}^{\mathrm{unforgeability}}$是可忽略的，则称IBCS是抗选择身份和自适应性选择消息攻击下强不可伪造的。挑战者$\mathcal{C}$与敌手$\mathcal{A}$之间的交互游戏如下：

Initial: $\mathcal{A}$宣布其攻击的目标身份$\mathrm{id}_{S^*}\in\mathcal{ID}$和$\mathrm{id}_{V^*}\in\mathcal{ID}$。

Setup: $\mathcal{C}$运行算法Setup生成公共参数pp和主私钥msk。$\mathcal{C}$秘密持有msk，并将pp发送给$\mathcal{A}$。

Queries: $\mathcal{A}$向$\mathcal{C}$发出多项式有界次的以下询问：

(1) Key query: $\mathcal{A}$适应性地询问任意身份$\mathrm{id}\in\mathcal{ID}$(除$\mathrm{id}_{S^*}$和$\mathrm{id}_{V^*}$外)的私钥，$\mathcal{C}$返回$\mathrm{sk}_{\mathrm{id}}$；

(2) Sign query: $\mathcal{A}$适应性地询问任意身份$\mathrm{id}_i\in\mathcal{ID}$为身份$\mathrm{id}_j\in\mathcal{ID}$生成的关于任意消息$\mu\in\mathcal{M}$的签名，$\mathcal{C}$返回$(\mu,r,\sigma)$，其中$\mathrm{id}_i$和$\mathrm{id}_j$分别为签名者和指定验证者的身份。

Outputs: $\mathcal{A}$输出一个伪造$(\mu^*,r^*,\sigma^*)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$。$\mathcal{A}$赢得游戏的前提是以下条件成立：

(1) $\mathrm{Verify}(\mathrm{pp},\mathrm{id}_{S^*},\mathrm{id}_{V^*},\mu^*,r^*,\sigma^*)\to 1$；

(2) $\mathcal{A}$未曾对id_{S^*}和id_{V^*}进行过Key query，且(μ^*,r^*,σ^*)不是Sign query的返回。

定义5[5]　若对于任意的PPT敌手$\mathcal{A}$在以下游戏中的优势$\mathrm{Adv}_{\mathrm{IBCS},\mathcal{A}}^{\mathrm{non-transferability}}$是可忽略的，则称IBCS是不可传递的。挑战者$\mathcal{C}$与敌手$\mathcal{A}$之间的交互游戏如下：

Setup: 与定义4中相同，$\mathcal{C}$生成公共参数pp和主私钥msk，并将pp发送给$\mathcal{A}$。

Challenge: $\mathcal{A}$选择目标身份$\mathrm{id}_{S^*}\in\mathcal{ID}$和$\mathrm{id}_{V^*}\in\mathcal{ID}$。$\mathcal{C}$运行算法KeyGen生成私钥$\mathrm{sk}_{\mathrm{id}_{S^*}}$和$\mathrm{sk}_{\mathrm{id}_{V^*}}$，随机选取消息$\mu_0\in\mathcal{M}$，运行算法$\mathrm{Sign}(\mathrm{pp},\mathrm{id}_{S^*},\mathrm{id}_{V^*},\mathrm{sk}_{\mathrm{id}_{S^*}},\mu_0)$生成随机数$r_0\in\mathcal{R}$和签名值$\sigma\in\mathcal{S}$；运行算法$\mathrm{Forge}(\mathrm{pp},\mathrm{id}_{V^*},\mathrm{sk}_{\mathrm{id}_{V^*}},\mu_0,r_0,\sigma)$生成新消息$\mu_1\in\mathcal{M}$和随机数$r_1\in\mathcal{R}$；随机选取$b\in\{0,1\}$，并返回$(\mu_b,r_b,\sigma)$。

Outputs: $\mathcal{A}$输出$b^*\in\{0,1\}$。若$b^*=b$，则$\mathcal{A}$赢得游戏。

定义6[5]　若签名$(\mu,r,\sigma)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$为指定

验证者$\mathrm{id}_{V^*}\in\mathcal{ID}$伪造，且签名者$\mathrm{id}_{S^*}\in\mathcal{ID}$有能力说服仲裁者拒绝该签名，则称IBCS满足签名者可拒绝性；相反地，若$(\mu,r,\sigma)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$为签名者$\mathrm{id}_{S^*}\in\mathcal{ID}$真实生成，且其无法否认，则称IBCS满足签名者不可抵赖性。上述两个性质可由签名者id_{S^*}与仲裁者之间的一个公开的拒绝协议(Denial Protocol)来保证：

对于id_{V^*}运行算法Forge伪造的$(\mu,r,\sigma)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$，$\mathrm{id}_{S^*}$可向仲裁者提交碰撞$(\mu',r',\sigma)$：

(1) 若$\mu\neq\mu'$，且$\mathrm{Verify}\left(\mathrm{pp},\mathrm{id}_{S^*},\mathrm{id}_{V^*},\mu',r',\sigma\right)\to 1$，则仲裁者断定$(\mu,r,\sigma)$非$\mathrm{id}_{S^*}$生成，而是$\mathrm{id}_{V^*}$伪造；

(2) 否则，仲裁者判定(μ,r,σ)为id_{S^*}生成。

3 格上基于身份的变色龙签名

令消息空间$\mathcal{M}=\{0,1\}^m$(任意消息可采用抗碰撞哈希函数映射到$\mathcal{M}$)，身份空间$\mathcal{ID}=\{0,1\}^*$，随机数空间$\mathcal{R}=\mathcal{D}_{Z^m,s}$以及签名空间$\mathcal{S}=\mathcal{D}_{Z^m,s}$，$\mathrm{id}_S\in\mathcal{ID}$和$\mathrm{id}_V\in\mathcal{ID}$分别对应签名者和指定验证者的身份。

3.1 方案构造

$\mathrm{Setup}\left(1^\lambda\right)\to(\mathrm{pp},\mathrm{msk})$：输入安全参数$\lambda$，令素数$q=\mathrm{poly}\left(\lambda\right)$，整数$m=2n\lceil\log_2 q\rceil$, $n=\mathrm{poly}\left(\lambda\right)$，高斯参数$s=\tilde{\mathcal{O}}\left(n^2\right)$。PKG执行以下操作：

(1) 运行$\mathrm{TrapGen}\left(q,n,m\right)$，生成$\boldsymbol{A}\in Z_q^{n\times m}$和$\Lambda_q^\perp\left(\boldsymbol{A}\right)$的陷门$\boldsymbol{T}_{\boldsymbol{A}}$；

(2) 随机选取$\boldsymbol{B}\in Z_q^{n\times m}$，作为构造变色龙哈希函数$\mathcal{CH}$的公共矩阵；

(3) 选取抗碰撞哈希函数$\mathcal{H}_1:\{0,1\}^*\to\mathcal{D}_{m\times m}$和$\mathcal{H}_2:\{0,1\}^*\to Z_q^n$，其中$\mathcal{D}_{m\times m}$见引理4；

(4) 输出公共参数$\mathrm{pp}=(\boldsymbol{A},\boldsymbol{B},\mathcal{H}_1,\mathcal{H}_2)$和系统主私钥$\mathrm{msk}=\boldsymbol{T}_{\boldsymbol{A}}$。

$\mathrm{KeyGen}\left(\mathrm{pp},\mathrm{msk},\mathrm{id}\right)\to\left(\mathrm{sk}_{\mathrm{id}}\right)$:输入参数pp，主私钥msk以及身份$\mathrm{id}\in\mathcal{ID}$，PKG执行以下操作：

(1)令$\boldsymbol{R}_{\mathrm{id}}=\mathcal{H}_1\left(\mathrm{id}\right)\in\mathcal{D}_{m\times m}$，计算$\boldsymbol{F}_{id}=\boldsymbol{A}\cdot\boldsymbol{R}_{\mathrm{id}}^{-1}\bmod q\in Z_q^{n\times m}$(以下将$\boldsymbol{F}_{\mathrm{id}_S}$和$\boldsymbol{F}_{\mathrm{id}_V}$分别简记为$\boldsymbol{F}_S$和$\boldsymbol{F}_V$)；

(2) 运行$\mathrm{BasisDel}\left(\boldsymbol{A},\boldsymbol{R}_{\mathrm{id}},\boldsymbol{T}_{\boldsymbol{A}},s\right)$，生成$\Lambda_q^\perp\left(\boldsymbol{F}_{\mathrm{id}}\right)$的陷门$\boldsymbol{T}_{\boldsymbol{F}_{\mathrm{id}}}$；

(3) 输出私钥$\mathrm{sk}_{\mathrm{id}}=\boldsymbol{T}_{\boldsymbol{F}_{\mathrm{id}}}$。

$\mathrm{Sign}\left(\mathrm{pp},\mathrm{id}_S,\mathrm{id}_V,\mathrm{sk}_{\mathrm{id}_S},\mu\right)\to(\mu,\boldsymbol{r},\boldsymbol{\sigma})$：输入参数pp，签名者身份$\mathrm{id}_S\in\mathcal{ID}$，指定验证者身份$\mathrm{id}_V\in\mathcal{ID}$，签名者私钥$\mathrm{sk}_{\mathrm{id}_S}=\boldsymbol{T}_{\boldsymbol{F}_S}$以及消息$\mu\in\{0,1\}^m$，签名者执行以下操作：

(1) 首先查找本地签名库是否存储$(\mathrm{id}_V,\mu,\boldsymbol{r},\sigma)$，若存在，执行步骤(6)，否则执行步骤(2)；

(2) 令$\boldsymbol{R}_{\mathrm{id}_S}=\mathcal{H}_1\left(\mathrm{id}_S\right)$和$\boldsymbol{R}_{\mathrm{id}_V}=\mathcal{H}_1\left(\mathrm{id}_V\right)$，计算$\boldsymbol{F}_S=\boldsymbol{A}\cdot\boldsymbol{R}_{\mathrm{id}_S}^{-1}\bmod q$和$\boldsymbol{F}_V=\boldsymbol{A}\cdot\boldsymbol{R}_{\mathrm{id}_V}^{-1}\bmod q$；

(3) 随机选取$\boldsymbol{r}\in\mathcal{R}$，计算关于$\boldsymbol{\mu}$的变色龙哈希值$\boldsymbol{y}=\mathcal{CH}\left(\boldsymbol{\mu},\boldsymbol{r}\right)=\boldsymbol{B}\cdot\boldsymbol{\mu}+\boldsymbol{F}_V\cdot\boldsymbol{r}\bmod q$；

(4) 令$\boldsymbol{h}=\mathcal{H}_2\left(\mathrm{id}_S,\mathrm{id}_V,\mathrm{bin}\left(\boldsymbol{y}\right)\right)$，其中$\mathrm{bin}\left(\boldsymbol{y}\right)\in\{0,1\}^{n\lceil\log_2 q\rceil}$为$\boldsymbol{y}\in Z_q^n$的二进制表示；

(5) 运行$\mathrm{SamplePre}\left(\boldsymbol{F}_S,\boldsymbol{T}_{\boldsymbol{F}_S},\boldsymbol{h},s\right)$，生成签名值$\boldsymbol{\sigma}\in Z^m$；

(6) 输出$(\mu,\boldsymbol{r},\boldsymbol{\sigma})$，并存储$(\mathrm{id}_V,\mu,\boldsymbol{r},\boldsymbol{\sigma})$于本地签名库。

$\mathrm{Verify}\left(\mathrm{pp},\mathrm{id}_S,\mathrm{id}_V,\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma}\right)\to(1\text{ or }0)$：输入参数pp，签名者身份$\mathrm{id}_S\in\mathcal{ID}$，指定验证者身份$\mathrm{id}_V\in\mathcal{ID}$，消息$\boldsymbol{\mu}\in\{0,1\}^m$，随机数$\boldsymbol{r}\in\mathcal{R}$以及签名值$\sigma\in\mathcal{S}$，指定验证者执行以下操作：

(1) 验证$0<\|\boldsymbol{r}\|,\|\boldsymbol{\sigma}\|\leq s\sqrt{m}$是否成立；

(2) 令$\boldsymbol{R}_{\mathrm{id}_S}=\mathcal{H}_1\left(\mathrm{id}_S\right)$和$\boldsymbol{R}_{\mathrm{id}_V}=\mathcal{H}_1\left(\mathrm{id}_V\right)$，计算$\boldsymbol{F}_S=\boldsymbol{A}\cdot\boldsymbol{R}_{\mathrm{id}_S}^{-1}\bmod q$和$\boldsymbol{F}_V=\boldsymbol{A}\cdot\boldsymbol{R}_{\mathrm{id}_V}^{-1}\bmod q$；

(3) 计算$\boldsymbol{y}=\mathcal{CH}\left(\boldsymbol{\mu},\boldsymbol{r}\right)=\boldsymbol{B}\cdot\boldsymbol{\mu}+\boldsymbol{F}_V\cdot\boldsymbol{r}\bmod q$；

(4) 验证$\boldsymbol{F}_S\cdot\boldsymbol{\sigma}=\mathcal{H}_2\left(\mathrm{id}_S,\mathrm{id}_V,\mathrm{bin}\left(\boldsymbol{y}\right)\right)\bmod q$是否成立；

(5) 若以上条件全部成立，输出1，否则输出0。

$\mathrm{Forge}\left(\mathrm{pp},\mathrm{id}_V,\mathrm{sk}_{\mathrm{id}_V},\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma}\right)\to\left(\boldsymbol{\mu'},\boldsymbol{r'},\boldsymbol{\sigma}\right)$:输入参数pp，指定验证者身份$\mathrm{id}_V$，私钥$\mathrm{sk}_{\mathrm{id}_V}=\boldsymbol{T}_{\boldsymbol{F}_V}$以及由签名者生成的$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$，指定验证者执行以下操作：

(1)令$\boldsymbol{R}_{\mathrm{id}_V}=\mathcal{H}_1\left(\mathrm{id}_V\right)$，计算$\boldsymbol{F}_V=\boldsymbol{A}\cdot\boldsymbol{R}_{\mathrm{id}_V}^{-1}\bmod q$和$\boldsymbol{y}=\mathcal{CH}\left(\mu,\boldsymbol{r}\right)=\boldsymbol{B}\cdot\boldsymbol{\mu}+\boldsymbol{F}_V\cdot\boldsymbol{r}\bmod q$;

(2) 选取$\boldsymbol{\mu'}\in\{0,1\}^m$且$\boldsymbol{\mu'}\neq\boldsymbol{\mu}$，计算$\boldsymbol{v}=\boldsymbol{y}-\boldsymbol{B}\cdot\boldsymbol{\mu'}\bmod q$；

(3) 运行$\mathrm{SamplePre}\left(\boldsymbol{F}_V,\boldsymbol{T}_{\boldsymbol{F}_V},\boldsymbol{v},s\right)$，生成随机数$\boldsymbol{r'}\in\mathcal{R}$；

(4) 输出$(\boldsymbol{\mu'},\boldsymbol{r'},\boldsymbol{\sigma})$。

3.2 安全性分析

定理1 假设$\mathrm{SIS}_{q,m,2s\sqrt{m}}$是困难的，则本文方案满足抗选择身份和自适应性选择消息攻击下强不可伪造性。

证明 假设$\mathcal{A}$为向本文方案发起攻击的PPT敌手，且能够以不可忽略的优势ε伪造签名，$\mathcal{C}$为试图求解$\mathrm{SIS}_{q,m,2s\sqrt{m}}$难题实例$\boldsymbol{A}^*\cdot\boldsymbol{e}^*=\boldsymbol{0}\bmod q$的挑战者，其中$\boldsymbol{A}^*\in Z_q^{n\times m}$。$\mathcal{C}$与敌手$\mathcal{A}$之间的交互游戏如下：

Initial: $\mathcal{A}$宣布其攻击的目标身份$\mathrm{id}_{S^*}\in\mathcal{ID}$和$\mathrm{id}_{V^*}\in\mathcal{ID}$。

Setup: $\mathcal{C}$随机选取$\boldsymbol{B}\in Z_q^{n\times m}$和可逆矩阵$\boldsymbol{R}^*\in\mathcal{D}_{m\times m}$，令$\boldsymbol{A}=\boldsymbol{A}^*\cdot\boldsymbol{R}^*\bmod q$，并将$(\boldsymbol{A},\boldsymbol{B})$发送给$\mathcal{A}$。

$\mathcal{H}_1$query:$\mathcal{A}$输入$\mathrm{id}_i \in \mathcal{ID}$，若$\mathrm{id}_i \neq \mathrm{id}_{S^*}$，$\mathcal{C}$查找本地密钥库是否存储$(\mathrm{id}_i, R_i, F_i, T_{F_i})$。若存在，则返回$\mathcal{H}_1(\mathrm{id}_i) = \boldsymbol{R}_i$；否则，运行算法SampleRwithBasis$(\boldsymbol{A})$，生成$R_i \in \mathcal{D}m \times m$，$\boldsymbol{F}_i \in Z_q^{n\times m}$和$\Lambda_q^{\perp}(\boldsymbol{F}_i)$的陷门$\boldsymbol{T}_{\boldsymbol{F}_i}$，其中$\boldsymbol{F}_i = \boldsymbol{A}\cdot\boldsymbol{R}_i^{-1}\mathrm{mod}q$，将$(\mathrm{id}_i, \boldsymbol{R}_i, \boldsymbol{F}_i, \boldsymbol{T}_{\boldsymbol{F}_i})$保存至本地密钥库，并返回$\mathcal{H}_1(\mathrm{id}_i) = \boldsymbol{R}_i$。若$\mathrm{id}_i = \mathrm{id}_{S^*}$，则将$(\mathrm{id}_{S^*}, \boldsymbol{R}^*, \boldsymbol{A}^*, \perp)$保存至$\mathcal{C}$的本地密钥库，并返回$\mathcal{H}_1(\mathrm{id}_{S^*}) = \boldsymbol{R}^*$。

$\mathcal{H}_2$ query: $\mathcal{A}$输入$\mathrm{id}_i, \mathrm{id}_j \in \mathcal{ID}$和$\boldsymbol{\mu} \in \mathcal{M}$，$\mathcal{C}$查找本地密钥库是否存储$(\mathrm{id}_i, \boldsymbol{R}_i, \boldsymbol{F}_i, \boldsymbol{T}_{\boldsymbol{F}_i}\mathrm{or}\perp)$和本地签名库是否存储$(\mathrm{id}_i, \mathrm{id}_j, \boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma})$。若存在，则返回$\mathcal{H}_2(\mathrm{id}_i, \mathrm{id}_j, \mathrm{bin}(\boldsymbol{y})) = \boldsymbol{F}_i\cdot\sigma\mathrm{mod}q$；否则，采用$\mathcal{H}_1$query生成$(\mathrm{id}_i \neq \mathrm{id}_{S^*}, \boldsymbol{R}_i, \boldsymbol{F}_i, \boldsymbol{T}_{\boldsymbol{F}_i})$或$(\mathrm{id}_i = \mathrm{id}_{S^*}, \boldsymbol{R}^*, \boldsymbol{A}^*, \perp)$，选取随机数$\boldsymbol{r} \in \mathcal{R}$，计算$\boldsymbol{y} = \mathcal{CH}(\boldsymbol{\mu}, \boldsymbol{r}) = \boldsymbol{B}\cdot\mu + \boldsymbol{F}_j\cdot\boldsymbol{r}\mathrm{mod}q$，随机选取$\boldsymbol{\sigma} \in \mathcal{D}_{Z^m,s}$，将$(\mathrm{id}_i, \mathrm{id}_j, \mu, \boldsymbol{r}, \boldsymbol{\sigma})$保存至本地签名库，并返回$\mathcal{H}_2(\mathrm{id}_i, \mathrm{id}_j, \mathrm{bin}(\boldsymbol{y})) = \boldsymbol{F}_i\cdot\sigma\mathrm{mod}q$。

由引理5知，SampleRwithBasis$(\boldsymbol{A})$的输出$R_i \in \mathcal{D}m \times m$；由引理3知，$\boldsymbol{F}_i\cdot\boldsymbol{\sigma}\mathrm{mod}q$统计接近均匀分布。综上可知，$\mathcal{H}_1$query和$\mathcal{H}_2$ query的返回值与真实方案中$\mathcal{H}_1$和$\mathcal{H}_2$的输出统计不可区分。

Key query: $\mathcal{A}$输入$\mathrm{id}_i \in \mathcal{ID}$，$\mathrm{id}_i \neq \mathrm{id}_{S^*}$，$\mathrm{id}_i \neq \mathrm{id}_{V^*}$，$\mathcal{C}$查找密钥库$(\mathrm{id}_i, \boldsymbol{R}_i, \boldsymbol{F}_i, \boldsymbol{T}_{\boldsymbol{F}_i})$，返回$\mathrm{sk}_{\mathrm{id}_i} = \boldsymbol{T}_{\boldsymbol{F}_i}$。

Sign query:$\mathcal{A}$输入$\mathrm{id}_i \in \mathcal{ID}$，$\mathrm{id}_j \in \mathcal{ID}$（$\mathrm{id}_i$和$\mathrm{id}_j$分别对应签名者和指定验证者）和$\boldsymbol{\mu} \in \mathcal{M}$，$\mathcal{C}$查找本地签名库$(\mathrm{id}_i, \mathrm{id}_j, \boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma})$，返回$(\boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma}) \in \mathcal{M}\times\mathcal{R}\times\mathcal{S}$。

不失一般性，假设$\mathcal{A}$在输出伪造$(\boldsymbol{\mu}^*, \boldsymbol{r}^*, \boldsymbol{\sigma}^*)$之前向$\mathcal{C}$发起过$(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{\mu}^*)$的$\mathcal{H}_2$ query，则$\mathcal{C}$已在本地存储$(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \mu^*, \boldsymbol{r}_{\boldsymbol{\mu}^*}, \boldsymbol{\sigma}_{\boldsymbol{\mu}^*})$。

Outputs:$\mathcal{A}$输出id_{S^*}为id_{V^*}生成的一个伪造$(\boldsymbol{\mu}^*, \boldsymbol{r}^*, \boldsymbol{\sigma}^*) \in \mathcal{M}\times\mathcal{R}\times\mathcal{S}$，满足：

(1) $\mathrm{Verify}(\mathrm{pp}, \mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{\mu}^*, \boldsymbol{r}^*, \boldsymbol{\sigma}^*) \to 1$；

(2) $\mathcal{A}$未曾对id_{S^*}和id_{V^*}进行过Key query，且$(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{\mu}^*, \boldsymbol{r}^*, \boldsymbol{\sigma}^*)$不是Sign query的返回。

当$\mathcal{A}$输出伪造$(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{\mu}^*, \boldsymbol{r}^*, \boldsymbol{\sigma}^*)$后，$\mathcal{C}$查找本地签名库$(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{\mu}^*, \boldsymbol{r}_{\mu^*}, \boldsymbol{\sigma}_{\mu^*})$，得到$(\boldsymbol{\mu}^*, \boldsymbol{r}_{\mu^*}, \boldsymbol{\sigma}_{\mu^*})$。由于$(\boldsymbol{\mu}^*, \boldsymbol{r}^*, \boldsymbol{\sigma}^*) \in \mathcal{M}\times\mathcal{R}\times\mathcal{S}$是一个成功的伪造，易知$\boldsymbol{F}_{S^*}\cdot\boldsymbol{\sigma}^* = \boldsymbol{F}_{S^*}\cdot\boldsymbol{\sigma}_{\mu^*}$，因此：

$$\begin{aligned}\boldsymbol{A}\cdot(\mathcal{H}_1(\mathrm{id}_{S^*}))^{-1}\cdot\boldsymbol{\sigma}^* &= \boldsymbol{A}^*\cdot\boldsymbol{R}^*\cdot(\boldsymbol{R}^*)^{-1}\cdot\boldsymbol{\sigma}^*\\ &= \boldsymbol{A}^*\cdot\sigma^* = \boldsymbol{A}^*\cdot\boldsymbol{\sigma}_{\mu^*}\mathrm{mod}q\end{aligned} \tag{2}$$

通过以下两种情况来说明$\mathcal{A}$的伪造$(\boldsymbol{\mu}^*, \boldsymbol{r}^*, \boldsymbol{\sigma}^*)$与$\mathcal{C}$的本地签名库中$(\boldsymbol{\mu}^*, \boldsymbol{r}_{\mu^*}, \boldsymbol{\sigma}_{\mu^*})$不同：

(1) 若$\mathcal{A}$曾发起过$(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{\mu}^*)$的Sign query，且$\mathcal{C}$返回$(\boldsymbol{\mu}^*, \boldsymbol{r}_{\mu^*}, \boldsymbol{\sigma}_{\mu^*})$。由于$\mathcal{A}$赢得游戏的条件是输出一个有效的强伪造签名，即$(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{\mu}^*, \boldsymbol{r}^*, \boldsymbol{\sigma}^*)$不是Sign query的返回，因此，$\boldsymbol{\sigma}^* \neq \boldsymbol{\sigma}_{\mu^*}$；

(2) 若$\mathcal{A}$未发起过$(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{\mu}^*)$的Sign query，由于$\mathcal{A}$曾发起过$\mathcal{H}_2$ query，$\mathcal{C}$已存储有$(\boldsymbol{\mu}^*, \boldsymbol{r}_{\mu^*}, \boldsymbol{\sigma}_{\mu^*})$，且返回$\mathcal{H}_2(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \mathrm{bin}(\boldsymbol{y})) = \boldsymbol{A}^*\cdot\boldsymbol{\sigma}_{\mu^*}$。由最小熵性质[14]可知，给定原像采样函数$f_{\boldsymbol{A}^*}(\boldsymbol{e}^*) = \boldsymbol{A}^*\cdot\boldsymbol{e}^*\mathrm{mod}q$，$\boldsymbol{e}^* \in \mathcal{D}_{Z^m,s}$的最小熵为$\omega(\log_2 n)$。因此，$\boldsymbol{\sigma}^* \neq \boldsymbol{\sigma}_{\mu^*}$以压倒性概率$1-2^{-\omega(\log_2 n)}$成立。

综上可知，若$\boldsymbol{\sigma}^* \neq \boldsymbol{\sigma}_{\mu^*}$，则$\mathcal{C}$可求得原像采样函数$f_{\boldsymbol{A}^*}(\boldsymbol{e}^*) = \boldsymbol{A}^*\cdot\boldsymbol{e}^*\mathrm{mod}q$的一个有效碰撞$(\boldsymbol{\sigma}^*, \boldsymbol{\sigma}_{\mu^*})$，即$\mathcal{C}$能够以优势$\mathrm{Adv}_{\mathrm{IBCS},\mathcal{A}}^{\mathrm{unforgeability}} = \left(1-2^{-\omega(\log_2 n)}\right)\cdot\varepsilon$输出$\mathrm{SIS}_{q,m,2s\sqrt{m}}$难题的一个有效解$\boldsymbol{e}^* = \boldsymbol{\sigma}^* - \boldsymbol{\sigma}_{\mu^*} \in Z^m$，即满足$\boldsymbol{A}^*\cdot\boldsymbol{e}^* = \boldsymbol{0}\mathrm{mod}q$，且$0 < \|\boldsymbol{e}^*\| \leq 2s\sqrt{m}$。证毕

定理2　本文方案满足签名不可传递性。

证明　$\mathcal{A}$选择目标身份$\mathrm{id}_{S^*} \in \mathcal{ID}$和$\mathrm{id}_{V^*} \in \mathcal{ID}$。$\mathcal{C}$运行KeyGen生成$(\boldsymbol{F}_{S^*}, \boldsymbol{T}_{\boldsymbol{F}_{S^*}})$和$(\boldsymbol{F}_{V^*}, \boldsymbol{T}_{\boldsymbol{F}_{V^*}})$；随机选取$\mu_0 \in \mathcal{M}$，运行$\mathrm{Sign}(\mathrm{pp}, \mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \boldsymbol{T}_{\boldsymbol{F}_{S^*}}, \boldsymbol{\mu}_0)$生成$\boldsymbol{r}_0 \in \mathcal{R}$和签名值$\sigma \in \mathcal{S}$；运行$\mathrm{Forge}(\mathrm{pp}, \mathrm{id}_{V^*}, \boldsymbol{T}_{\boldsymbol{F}_{V^*}}, \boldsymbol{\mu}_0, \boldsymbol{r}_0, \boldsymbol{\sigma})$生成新消息$\boldsymbol{\mu}_1 \in \mathcal{M}$和随机数$\boldsymbol{r}_1 \in \mathcal{R}$；随机选取$b \in \{0,1\}$，并最终返回$(\boldsymbol{\mu}_b, \boldsymbol{r}_b, \boldsymbol{\sigma}) \in \mathcal{M}\times\mathcal{R}\times\mathcal{S}$。

在上述过程中，$\boldsymbol{r}_0 \in \mathcal{D}_{Z^m,s}$，$\boldsymbol{r}_1$为运行算法SamplePre生成。由引理6知，短向量$\boldsymbol{r}_0$和$\boldsymbol{r}_1$统计不可区分。对于$(\boldsymbol{\mu}_0, \boldsymbol{r}_0, \boldsymbol{\sigma})$和$(\boldsymbol{\mu}_1, \boldsymbol{r}_1, \boldsymbol{\sigma})$，有$\mathcal{CH}(\boldsymbol{\mu}_0, \boldsymbol{r}_0) = \mathcal{CH}(\boldsymbol{\mu}_1, \boldsymbol{r}_1)$，即$\boldsymbol{B}\cdot\boldsymbol{\mu}_0 + \boldsymbol{F}_{V^*}\cdot\boldsymbol{r}_0 = \boldsymbol{B}\cdot\boldsymbol{\mu}_1 + \boldsymbol{F}_{V^*}\cdot\boldsymbol{r}_1\mathrm{mod}q$；又知当$\mathcal{H}_2$的输入相同时，其输出也一定相同。因此，算法Verify中的条件(4)成立，即

$$\begin{aligned}\boldsymbol{F}_{S^*}\cdot\boldsymbol{\sigma} &= \mathcal{H}_2(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \mathrm{bin}(\boldsymbol{B}\cdot\boldsymbol{\mu}_0 + \boldsymbol{F}_{V^*}\cdot\boldsymbol{r}_0))\\ &= \mathcal{H}_2(\mathrm{id}_{S^*}, \mathrm{id}_{V^*}, \mathrm{bin}(\boldsymbol{B}\cdot\boldsymbol{\mu}_1 + \boldsymbol{F}_{V^*}\cdot\boldsymbol{r}_1))\,\mathrm{mod}\end{aligned} \tag{3}$$

综上可知，对敌手$\mathcal{A}$而言，由挑战者$\mathcal{C}$返回的关于$\boldsymbol{\mu}_0 \in \mathcal{M}$和$\boldsymbol{\mu}_1 \in \mathcal{M}$的变色龙签名是统计不可区分的。因此，任意敌手即使能够运行算法Verify对签名$(\boldsymbol{\mu}_b, \boldsymbol{r}_b, \boldsymbol{\sigma}) \in \mathcal{M}\times\mathcal{R}\times\mathcal{S}$进行验证，仍无法判定出真实生成者为$\mathrm{id}_{S^*} \in \mathcal{ID}$或$\mathrm{id}_{V^*} \in \mathcal{ID}$，敌手$\mathcal{A}$的优势是可忽略的，即$\mathrm{Adv}_{\mathrm{IBCS},\mathcal{A}}^{\mathrm{non\text{-}transferability}} \approx 0$。　证毕

定理3　本文方案满足签名者可拒绝性和不可抵赖性。

证明　对于签名者$\mathrm{id}_{S^*} \in \mathcal{ID}$运行Sign生成，并发送给$\mathrm{id}_{V^*} \in \mathcal{ID}$的签名$(\boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma}) \in \mathcal{M}\times\mathcal{R}\times\mathcal{S}$，$\mathrm{id}_{S^*}$无法对其抵赖。不妨假设$\mathrm{id}_{S^*}$为尝试进行抵赖的签名者，根据Denial Protocol，签名者id_{S^*}需要出示一个伪造$(\boldsymbol{\mu}', \boldsymbol{r}', \boldsymbol{\sigma}) \in \mathcal{M}\times\mathcal{R}\times\mathcal{S}$。若$\mathrm{id}_{S^*}$成功输出$(\boldsymbol{\mu}' \neq \boldsymbol{\mu}, \boldsymbol{r}', \boldsymbol{\sigma})$，则仲裁者可断定$(\boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma})$不是

id_{S^*}生成的，即id_{S^*}对其生成的签名抵赖成功。由于$(\boldsymbol{\mu}', \boldsymbol{r}', \boldsymbol{\sigma}) \in \mathcal{M} \times \mathcal{R} \times \mathcal{S}$满足算法Verify，则有

$$\begin{aligned}\mathcal{CH}(\boldsymbol{\mu}, \boldsymbol{r}) =& \boldsymbol{B} \cdot \boldsymbol{\mu} + \boldsymbol{F}_{V^*} \cdot \boldsymbol{r} = \mathcal{CH}(\boldsymbol{\mu}', \boldsymbol{r}') \\ =& \boldsymbol{B} \cdot \boldsymbol{\mu}' + \boldsymbol{F}_{V^*} \cdot \boldsymbol{r}' \\ =& (\boldsymbol{B}, \boldsymbol{F}_{V^*}) \cdot \begin{pmatrix} \boldsymbol{\mu} \\ \boldsymbol{r} \end{pmatrix} \\ =& (\boldsymbol{B}, \boldsymbol{F}_{V^*}) \cdot \begin{pmatrix} \boldsymbol{\mu}' \\ \boldsymbol{r}' \end{pmatrix} \Rightarrow (\boldsymbol{B}, \boldsymbol{F}_{V^*}) \\ & \cdot \begin{pmatrix} \boldsymbol{\mu} - \boldsymbol{\mu}' \\ \boldsymbol{r} - \boldsymbol{r}' \end{pmatrix} = 0 \bmod q \end{aligned} \tag{4}$$

综上可知，签名者id_{S^*}可求得$\mathrm{SIS}_{q,2m,2s\sqrt{m}}$难题实例$(\boldsymbol{B}, \boldsymbol{F}_{V^*}) \cdot \boldsymbol{e} = 0 \bmod q$的一个解$\boldsymbol{e} = \begin{pmatrix} \boldsymbol{\mu} - \boldsymbol{\mu}' \\ \boldsymbol{r} - \boldsymbol{r}' \end{pmatrix} \in Z^{2m}$，且$0 < \|\boldsymbol{e}\| \le 2s\sqrt{m}$。由引理1知，这与$\mathrm{id}_{S^*}$没有$\Lambda_q^{\perp}(\boldsymbol{B}, \boldsymbol{F}_{V^*})$的任何陷门信息仍求得$\mathrm{SIS}_{q,2m,2s\sqrt{m}}$难题实例的一个有效解相矛盾，即本文方案满足签名者不可抵赖性。

相反的，id_{S^*}生成签名$(\boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma}) \in \mathcal{M} \times \mathcal{R} \times \mathcal{S}$，发送给指定验证者$\mathrm{id}_{V^*}$，而$\mathrm{id}_{V^*}$运行算法Forge生成一个伪造$(\boldsymbol{\mu}', \boldsymbol{r}', \boldsymbol{\sigma}) \in \mathcal{M} \times \mathcal{R} \times \mathcal{S}$。在Denial Protocol中，$\mathrm{id}_{S^*}$可通过出示其真实生成的$(\boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma})$来说服仲裁者对伪造$(\boldsymbol{\mu}', \boldsymbol{r}', \boldsymbol{\sigma})$进行拒绝。由于方案是签名者不可抵赖的，即$\mathrm{id}_{S^*}$不具备伪造其真实生成的$(\boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma})$的能力，对于$\mathrm{id}_{S^*}$出示的$(\boldsymbol{\mu}, \boldsymbol{r}, \boldsymbol{\sigma})$，仲裁者可完全断定是由$\mathrm{id}_{S^*}$真实生成的；进一步地，仲裁者由$\mu' \ne \mu$可完全断定$(\boldsymbol{\mu}', \boldsymbol{r}', \boldsymbol{\sigma})$为$\mathrm{id}_{V^*}$伪造。特别地，由于方案是抗选择身份和自适应性选择消息攻击下强不可伪造的，id_{V^*}伪造出一个id_{S^*}无法拒绝的$(\boldsymbol{\mu}', \boldsymbol{r}', \boldsymbol{\sigma}) \in \mathcal{M} \times \mathcal{R} \times \mathcal{S}$的概率是可忽略的，即本文方案满足签名者可拒绝性。 证毕

4 格上抗消息暴露的基于身份的变色龙签名

大多数变色龙签名方案均不具备抗消息暴露安全性，即若签名者试图拒绝指定验证者伪造的签名，必须在仲裁阶段出示自己真实生成的消息和签名，这将导致签名者原本希望防止二次传递的签名被完全公开，从而造成不可传递性的失效。本节给出格上抗消息暴露的IBCS方案，使得签名者仅需出示某些不暴露真实消息和签名的信息，仍能够辅助仲裁者有效地拒绝指定验证者伪造的签名。

新方案采用对消息的随机分割策略，通过增添拒绝算法Denial来实现签名者在仲裁阶段的抗消息暴露性。算法Setup和KeyGen与已给出的格上IBCS方案中相同，将不再赘述，重点介绍新的算法设计细节。

4.1 方案构造

$\mathrm{Setup}\left(1^{\lambda}\right) \to (\mathrm{pp}, \mathrm{msk})$：输入安全参数$\lambda$，输出公共参数$\mathrm{pp} = (\boldsymbol{A}, \boldsymbol{B}, \mathcal{H}_1, \mathcal{H}_2)$和主私钥$\mathrm{msk} = \boldsymbol{T}_{\boldsymbol{A}}$。

$\mathrm{KeyGen}(\mathrm{pp}, \mathrm{msk}, \mathrm{id}) \to (\mathrm{sk}_{\mathrm{id}})$：输入参数pp，主私钥msk以及身份$\mathrm{id} \in \mathcal{ID}$，输出私钥$\mathrm{sk}_{\mathrm{id}} = \boldsymbol{T}_{\boldsymbol{F}_{\mathrm{id}}}$。

$\mathrm{Sign}(\mathrm{pp}, \mathrm{id}_S, \mathrm{id}_V, \mathrm{sk}_{\mathrm{id}_S}, \boldsymbol{\mu}) \to (\boldsymbol{\mu}_0, \boldsymbol{\mu}_1, \boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{\sigma})$：输入参数pp，签名者身份$\mathrm{id}_S \in \mathcal{ID}$，指定验证者身份$\mathrm{id}_V \in \mathcal{ID}$，签名者私钥$\mathrm{sk}_{\mathrm{id}_S} = \boldsymbol{T}_{\boldsymbol{F}_S}$以及消息$\mu \in \{0,1\}^m$，签名者执行以下操作：

(1) 首先查找本地签名库是否存储$(\mathrm{id}_V, \boldsymbol{\mu}_0, \boldsymbol{\mu}_1, \boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{\sigma})$，其中$\boldsymbol{\mu}_0, \boldsymbol{\mu}_1 \in \{0,1\}^m$，且$\boldsymbol{\mu}_0 + \boldsymbol{\mu}_1 = \boldsymbol{\mu} \bmod 2$。若存在，执行(6)，否则执行(2)；

(2) 令$\boldsymbol{R}_{\mathrm{id}_S} = \mathcal{H}_1(\mathrm{id}_S)$和$\boldsymbol{R}_{\mathrm{id}_V} = \mathcal{H}_1(\mathrm{id}_V)$，计算$\boldsymbol{F}_S = \boldsymbol{A} \cdot \boldsymbol{R}_{\mathrm{id}_S}^{-1} \bmod q$和$\boldsymbol{F}_V = \boldsymbol{A} \cdot \boldsymbol{R}_{\mathrm{id}_V}^{-1} \bmod q$；

(3) 随机选取$\boldsymbol{\mu}_0 \in \{0,1\}^m$，计算$\boldsymbol{\mu}_1 = \boldsymbol{\mu}_0 + \boldsymbol{\mu} \bmod 2$；

(4) 随机选取$\boldsymbol{r}_0, \boldsymbol{r}_1 \in \mathcal{R}$，计算关于$\boldsymbol{\mu}_0$和$\boldsymbol{\mu}_1$的变色龙哈希值$\boldsymbol{y}_0 = \mathcal{CH}(\boldsymbol{\mu}_0, \boldsymbol{r}_0) = \boldsymbol{B} \cdot \boldsymbol{\mu}_0 + \boldsymbol{F}_V \cdot \boldsymbol{r}_0 \bmod q$和$\boldsymbol{y}_1 = \mathcal{CH}(\boldsymbol{\mu}_1, \boldsymbol{r}_1) = \boldsymbol{B} \cdot \mu_1 + \boldsymbol{F}_V \cdot \boldsymbol{r}_1 \bmod q$；

(5) 令$\boldsymbol{h} = \mathcal{H}_2(\mathrm{id}_S, \mathrm{id}_V, \mathrm{bin}(\boldsymbol{y}_0, \boldsymbol{y}_1))$，运行$\mathrm{SamplePre}(\boldsymbol{F}_S, \boldsymbol{T}_{\boldsymbol{F}_S}, \boldsymbol{h}, s)$，生成签名值$\boldsymbol{\sigma} \in Z^m$；

(6) 输出$(\boldsymbol{\mu}_0, \boldsymbol{\mu}_1, \boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{\sigma})$，并存储$(\mathrm{id}_V, \boldsymbol{\mu}_0, \boldsymbol{\mu}_1, \boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{\sigma})$于本地签名库。

$\mathrm{Verify}(\mathrm{pp}, \mathrm{id}_S, \mathrm{id}_V, \boldsymbol{\mu}_0, \boldsymbol{r}_0, \boldsymbol{\mu}_1, \boldsymbol{r}_1, \boldsymbol{\sigma}) \to (1 \text{ or } 0)$：输入参数pp，签名者身份$\mathrm{id}_S \in \mathcal{ID}$，指定验证者身份$\mathrm{id}_V \in \mathcal{ID}$，比特串$\boldsymbol{\mu}_0, \boldsymbol{\mu}_1 \in \{0,1\}^m$，随机数$\boldsymbol{r}_0, \boldsymbol{r}_1 \in \mathcal{R}$以及签名值$\boldsymbol{\sigma} \in \mathcal{S}$，指定验证者执行以下操作：

(1) 验证$0 < \|\boldsymbol{r}_0\|, \|\boldsymbol{r}_1\|, \|\boldsymbol{\sigma}\| \le s\sqrt{m}$是否成立；

(2) 令$\boldsymbol{R}_{\mathrm{id}_S} = \mathcal{H}_1(\mathrm{id}_S)$和$\boldsymbol{R}_{\mathrm{id}_V} = \mathcal{H}_1(\mathrm{id}_V)$，计算$\boldsymbol{F}_S = \boldsymbol{A} \cdot \boldsymbol{R}_{\mathrm{id}_S}^{-1} \bmod q$和$\boldsymbol{F}_V = \boldsymbol{A} \cdot \boldsymbol{R}_{\mathrm{id}_V}^{-1} \bmod q$；

(3) 计算$\boldsymbol{y}_0 = \mathcal{CH}(\boldsymbol{\mu}_0, \boldsymbol{r}_0) = \boldsymbol{B} \cdot \boldsymbol{\mu}_0 + \boldsymbol{F}_V \cdot \boldsymbol{r}_0 \bmod q$和$\boldsymbol{y}_1 = \mathcal{CH}(\boldsymbol{\mu}_1, \boldsymbol{r}_1) = \boldsymbol{B} \cdot \boldsymbol{\mu}_1 + \boldsymbol{F}_V \cdot \boldsymbol{r}_1 \bmod q$；

(4) 验证$\boldsymbol{F}_S \cdot \boldsymbol{\sigma} = \mathcal{H}_2(\mathrm{id}_S, \mathrm{id}_V, \mathrm{bin}(\boldsymbol{y}_0, \boldsymbol{y}_1))$是否成立；

(5) 若以上条件全部成立，输出1，否则输出0。

$\mathrm{Forge}\quad(\mathrm{pp}, \mathrm{id}_V, \mathrm{sk}_{\mathrm{id}_V}, \boldsymbol{\mu}_0, \boldsymbol{\mu}_1, \boldsymbol{r}_0, \boldsymbol{r}_1, \sigma) \to (\boldsymbol{\mu}'_b, \boldsymbol{\mu}_{1-b}, \boldsymbol{r}'_b, \boldsymbol{r}_{1-b}, \boldsymbol{\sigma})$：输入参数pp，指定验证者身份$\mathrm{id}_V$，私钥$\mathrm{sk}_{\mathrm{id}_V} = \boldsymbol{T}_{\boldsymbol{F}_V}$以及由签名者生成的$(\boldsymbol{\mu}_0, \boldsymbol{\mu}_1, \boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{\sigma}) \in \mathcal{M}^2 \times \mathcal{R}^2 \times \mathcal{S}$，指定验证者执行以下操作：

(1) 令$\boldsymbol{R}_{\mathrm{id}_V} = \mathcal{H}_1(\mathrm{id}_V)$，计算$\boldsymbol{F}_V = \boldsymbol{A} \cdot \boldsymbol{R}_{\mathrm{id}_V}^{-1} \bmod q$；

(2) 选取$b \in \{0,1\}$和$\boldsymbol{\mu}'_b \in \{0,1\}^m$，其中$\boldsymbol{\mu}'_b \ne \boldsymbol{\mu}_b$；

(3) 计算$\boldsymbol{y}_b = \mathcal{CH}(\boldsymbol{\mu}_b, \boldsymbol{r}_b) = \boldsymbol{B} \cdot \boldsymbol{\mu}_b + \boldsymbol{F}_V \cdot \boldsymbol{r}_b \bmod q$和$\boldsymbol{v} = \boldsymbol{y}_b - \boldsymbol{B} \cdot \mu'_b \bmod q$；

(4) 运行$\mathrm{SamplePre}(\boldsymbol{F}_V, \boldsymbol{T}_{\boldsymbol{F}_V}, \boldsymbol{v}, s)$，生成随机数$\boldsymbol{r}'_b \in \mathcal{R}$；

(5) 输出$(\boldsymbol{\mu'}_b, \boldsymbol{\mu}_{1-b}, \boldsymbol{r'}_b, \boldsymbol{r}_{1-b}, \boldsymbol{\sigma})$。

请注意：在上述算法中，指定验证者id_V最终伪造的消息为$\boldsymbol{\mu'} = \boldsymbol{\mu}_{1-b} + \boldsymbol{\mu}'_b \bmod 2$。事实上，$\mathrm{id}_V$也可以同时任意选取$\boldsymbol{\mu}'_0 \in \{0,1\}^m$和$\boldsymbol{\mu}'_1 \in \{0,1\}^m$来进行伪造，此时，$\mathrm{id}_V$最终伪造的消息为$\boldsymbol{\mu'} = \boldsymbol{\mu}'_0 + \boldsymbol{\mu}'_1 \bmod 2$。

$\mathrm{Denial}(\mathrm{pp}, \mathrm{id}_S, \mathrm{id}_V, \boldsymbol{\mu'}_0, \boldsymbol{\mu'}_1, \boldsymbol{r'}_0, \boldsymbol{r'}_1, \boldsymbol{\sigma}) \to (1 \text{ or } 0)$：输入参数pp，签名者身份$\mathrm{id}_S$，指定验证者身份$\mathrm{id}_V$以及由指定验证者伪造的$(\boldsymbol{\mu'}_0, \boldsymbol{\mu'}_1, \boldsymbol{r'}_0, \boldsymbol{r'}_1, \boldsymbol{\sigma}) \in \mathcal{M}^2 \times \mathcal{R}^2 \times \mathcal{S}$，签名者和仲裁者执行以下操作：

(1) 签名者查找本地签名库$(\mathrm{id}_V, \boldsymbol{\mu}_0, \boldsymbol{\mu}_1, \boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{\sigma})$，其中$\boldsymbol{\mu}_0 \neq \boldsymbol{\mu}'_0$或$\boldsymbol{\mu}_1 \neq \boldsymbol{\mu}'_1$；

(2) 不失一般性，假设$\boldsymbol{\mu}_0 \neq \boldsymbol{\mu}'_0$，签名者输出碰撞$(\boldsymbol{\mu}_0, \boldsymbol{r}_0)$；

(3) 仲裁者验证$\boldsymbol{\mu}_0 \neq \boldsymbol{\mu}'_0$和$\mathcal{CH}(\boldsymbol{\mu}_0, \boldsymbol{r}_0) = \mathcal{CH}(\boldsymbol{\mu'}_0, \boldsymbol{r'}_0)$是否成立；

(4) 若以上条件全部成立，仲裁者输出1，即断定$(\boldsymbol{\mu'}_0, \boldsymbol{\mu'}_1, \boldsymbol{r'}_0, \boldsymbol{r'}_1, \boldsymbol{\sigma})$是由指定验证者伪造的，否则输出0。

4.2 安全性分析

定理4　假设$\mathrm{SIS}_{q,m,2s\sqrt{m}}$是困难的，则本文方案满足抗选择身份和自适应性选择消息攻击下强不可伪造性、签名不可传递性、签名者可拒绝性和不可抵赖性以及抗消息暴露性。

证明　证明思路与已给出的格上IBCS方案的安全性证明思路基本相同；因篇幅所限，将不再赘述。

5　效率分析

本文提出的两个格上IBCS方案与其他抗量子攻击的不可传递性签名方案在功能、存储与传输成本方面的对比，如表1所示。

从功能方面看，方案1结合了格密码体制和基于身份的变色龙签名的安全特性，避免了文献[12]中任意第三方可伪造签名和签名者无法拒绝指定验证者伪造的签名的安全性漏洞，弥补了格上安全的变色龙签名的空缺；解决了文献[13]中签名者与指定验证者关于签名的争议问题。方案2采用了对消息的随机分割策略，增添了新的拒绝算法，解决了方案1在仲裁阶段签名不可传递性失效的问题，获得了抗消息暴露安全性。

从存储和传输成本方面看，方案1将最终签名中的随机矩阵作为公共参数，不再由签名者每次选取后与随机数和签名值一起发送，降低了文献[12]中签名的传输代价；公共参数仅包含$Z_q^{n\times m}$上的两个随机矩阵，最终的签名仅包含一个消息$\mu \in \mathcal{M}$和$\mathcal{D}_{Z^m,s}$上的两个短向量，减少了文献[13-15]中公共参数的存储成本，提高了签名的传输效率。方案2的签名过程采用了对消息的随机分割进行两次变色龙哈希计算和一次高斯原像采样，最终的签名仅包含两个比特串$\mu_0 \in \mathcal{M}$和$\mu_1 \in \mathcal{M}$，以及$\mathcal{D}_{Z^m,s}$上的3个短向量，即签名长度虽有所增加，但渐进复杂度仍与方案1相同。

综上所述，本文提出的两个方案在功能方面更加全面，获得了抗选择身份和自适应性选择消息攻击下强不可伪造性、签名不可传递性、签名者可拒绝性和不可抵赖性以及抗消息暴露性；在存储和传输成本方面，减少了公共参数的存储成本与签名生成和传输的开销，可满足轻量级设备进行数字签名的实用性需求。

6　结束语

通过结合抗量子计算攻击的格密码体制和基于身份的变色龙签名的安全特性，本文提出了格上基于身份的变色龙签名方案，弥补了格上安全的变色龙签名方案的空缺；进一步地，针对变色龙签名在仲裁阶段签名不可传递性失效的问题，提出了格上抗消息暴露的基于身份的变色龙签名方案。本文在随机预言机模型下严格证明了两个方案满足抗选择身份和自适应性选择消息攻击下强不可伪造性、签名不可传递性、签名者可拒绝性和不可抵赖性，以及方案2的抗消息暴露性。此外，给出的两个变色龙签名方案也减少了签名生成和传输的开销，符合轻量级签名的实用性需求。

表 1　效率分析

方案	公共参数长度	签名长度	不可伪造性	不可传递性	可拒绝性	不可抵赖性	抗消息暴露性	安全模型
文献[12]	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n^2)$	×	√	×	√	×	随机预言机
文献[13]	$\tilde{\mathcal{O}}(n^3)$	$\tilde{\mathcal{O}}(n^2)$	√	√	×	√	×	标准
文献[14]	$\tilde{\mathcal{O}}(k_0 \cdot n^2)$	$\tilde{\mathcal{O}}(n^2)$	√	×	–	–	–	标准
文献[15]	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(k_1 \cdot n)$	√	√	√	√	×	随机预言机
本文方案1	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	√	√	√	√	×	随机预言机
本文方案2	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	√	√	√	√	√	随机预言机

注：k_0表示同态计算的数据集尺寸，k_1表示有向无环图的内部顶点数；×表示不满足，√表示满足，–表示不考虑。

参 考 文 献

[1] CHAUM D and VAN ANTWERPEN H. Undeniable signatures[C]. The Conference on the Theory and Application of Cryptology, Santa Barbara, USA, 1989: 212–216. doi: 10.1007/0-387-34805-0_20.

[2] JAKOBSSON M, SAKO K, and IMPAGLIAZZO R. Designated verifier proofs and their applications[C]. The International Conference on the Theory and Applications of Cryptographic Techniques, Saragossa, Spain, 1996: 143–154. doi: 10.1007/3-540-68339-9_13.

[3] KRAWCZYK H and RABIN T. Chameleon hashing and signatures[OL]. http://eprint.iacr.org/1998/10.1998.3.

[4] SHAMIR A. Identity-based cryptosystems and signature schemes[C]. The Workshop on the Theory and Application of Cryptographic Techniques, Santa Barbara, USA, 1984: 47–53. doi: 10.1007/3-540-39568-7_5.

[5] ATENIESE G and DE MEDEIROS B. Identity-based chameleon hash and applications[C]. The 8th International Conference on Financial Cryptography, Key West, USA, 2004: 164–180. doi: 10.1007/978-3-540-27809-2_19.

[6] XIE Zhikang, SHEN Qingni, LI Cong, *et al*. Identity-based chameleon hash without random oracles and application in the mobile internet[C]. ICC 2021-IEEE International Conference on Communications, Montreal, Canada, 2021: 1–6. doi: 10.1109/ICC42927.2021.9500446.

[7] WU Chunhui, KE Lishan, and DU Yusong. Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain[J]. *Information Sciences*, 2021, 548: 438–449. doi: 10.1016/j.ins.2020.10.008.

[8] LI Cong, SHEN Qingni, XIE Zhikang, *et al*. Efficient identity-based chameleon hash for mobile devices[C]. ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing, Singapore, 2022: 3039–3043. doi: 10.1109/ICASSP43922.2022.9746617.

[9] NIST. PQC standardization process: Announcing four candidates to be standardized, plus fourth round candidates[EB/OL]. https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4, 2022.

[10] JOSEPH D, MISOCZKI R, MANZANO M, *et al*. Transitioning organizations to post-quantum cryptography [J]. *Nature*, 2022, 605(7909): 237–243. doi: 10.1038/s41586-022-04623-2.

[11] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai trees, or how to delegate a lattice basis[C]. The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, French, 2010: 523–552. doi: 10.1007/978-3-642-13190-5_27.

[12] 谢璇, 喻建平, 王廷, 等. 基于格的变色龙签名方案[J]. 计算机科学, 2013, 40(2): 117–119. doi: 10.3969/j.issn.1002-137X.2013.02.026.

XIE Xuan, YU Jianping, WANG Ting, *et al*. Chameleon signature scheme based on lattice[J]. *Computer Science*, 2013, 40(2): 117–119. doi: 10.3969/j.issn.1002-137X.2013.02.026.

[13] NOH G and JEONG I R. Strong designated verifier signature scheme from lattices in the standard model[J]. *Security and Communication Networks*, 2016, 9(18): 6202–6214. doi: 10.1002/sec.1766.

[14] XIE Dong, PENG Haipeng, LI Lixiang, *et al*. Homomorphic signatures from chameleon hash functions[J]. *Information Technology and Control*, 2017, 46(2): 274–286. doi: 10.5755/j01.itc.46.2.14320.

[15] THANALAKSHMI P, ANITHA R, ANBAZHAGAN N, *et al*. A hash-based quantum-resistant chameleon signature scheme[J]. *Sensors*, 2021, 21(24): 8417. doi: 10.3390/s21248417.

[16] GENTRY C, PEIKERT C, and VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]. The 40th Annual ACM Symposium on Theory of Computing, Victoria, Canada, 2008: 197–206. doi: 10.1145/1374376.1374407.

[17] AJTAI M. Generating hard instances of lattice problems (extended abstract)[C]. The 28th Annual ACM Symposium on Theory of Computing, Philadelphia, USA, 1996: 99–108. doi: 10.1145/237814.237838.

[18] ALWEN J and PEIKERT C. Generating shorter bases for hard random lattices[J]. *Theory of Computing Systems*, 2011, 48(3): 535–553. doi: 10.1007/s00224-010-9278-3.

[19] MICCIANCIO D and PEIKERT C. Trapdoors for lattices: Simpler, tighter, faster, smaller[C]. The 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 2012: 700–718. doi: 10.1007/978-3-642-29011-4_41.

[20] AGRAWAL S, BONEH D, and BOYEN X. Lattice basis delegation in fixed dimension and shorter-Ciphertext hierarchical IBE[C]. The 30th Annual Cryptology Conference, Santa Barbara, USA, 2010: 98–115. doi: 10.1007/978-3-642-14623-7_6.

张彦华：男，讲师，研究方向为格公钥密码学、属性基密码学和后量子密码学等.

陈 岩：男，硕士生，研究方向为格公钥密码、基于身份的密码等.

刘西蒙：男，研究员，研究方向为私计算、密文数据挖掘等.

尹毅峰：男，教授，研究方向为群组密钥协商等.

胡予濮：男，教授，研究方向为多线性映射、后量子密码学等.

责任编辑：马秀强