标准模型下基于格的变色龙签名方案

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科学与技术学院 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：作为一种比较理想的指定验证者签名，变色龙签名(CS)通过在签名算法中嵌入变色龙哈希函数(CHF)对消息进行散列，更简便地解决了签名的2次传递问题。在获得不可传递性的同时，变色龙签名还要求满足不可伪造性、签名者可拒绝性以及不可抵赖性等特性。针对基于大整数分解或离散对数等传统数论难题的CS无法抵御量子计算机攻击，以及随机预言机模型下可证明安全的数字签名方案在实际具体实现中未必安全的问题，该文给出了标准模型下基于格的变色龙签名；进一步地，针对签名者可拒绝性的获得需要耗费其较大的本地存储的问题，给出了标准模型下基于格的无需本地存储的变色龙签名，新方案彻底消除了签名者对本地签名库的依赖，使得签名者能够在不存储原始消息与签名的条件下辅助仲裁者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和差错学习问题，两个方案在标准模型下是可证明安全的。

关键词：变色龙签名；格；不可传递性；标准模型；无需本地存储
中图分类号：TN918;TP309 **文献标识码**：A **文章编号**：1009-5896(2022)YU-0001-08
DOI: 10.11999/JEIT231093

Chameleon Signature Schemes over Lattices in the Standard Model

ZHANG Yanhua① CHEN Yan① LIU Ximeng② YIN Yifeng① HU Yupu③
①(*School of Computer Science and Technology*, *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: As an ideal designated verifier signature, Chameleon Signature (CS) can solve the problem of signature secondary transmission more subtly by embedding an efficient Chameleon Hash Function (CHF) into the signing algorithm. 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 traditional number theory problems, such as the large integer factorization or discrete logarithm cannot resist quantum computing attacks, and the schemes that provably secure in the random oracle model may not be secure in a practical implementation, a lattice-based CS scheme in the standard model is proposed; Furthermore, to solve the problem of requiring a significant local storage to obtain deniability for the signer, a lattice-based CS scheme without local storage in the standard model is proposed, the new scheme completely eliminates the signer's dependence on the local signature library, and enables the signer to assist an arbitrator to reject a forged signature of any adversary without storing the original message and signature. Particularly, based on the hardness of the small integer solution problem and learning with errors problem, both schemes are proved secure in the standard model.

Key words: Chameleon Signature (CS); Lattice; Non-transferability; Standard model; Without local storage

收稿日期：2023-10-09；改回日期：2024-02-02；网络出版：2024-02-26
*通信作者： 张彦华 yhzhang@email.zzuli.edu.cn
基金项目：河南省自然科学基金(222300420371)，河南省网络密码技术重点实验室开放课题(LNCT2022-A09)，河南省高层次人才国际化培养项目(2023026)，河南省高等学校重点科研项目(24A520054)
Foundation Items: The Natural Science Foundation of Henan Province (222300420371), The Open Subject of Henan Key Laboratory of Network Cryptography Technology (LNCT2022-A09), The International Cultivation of Henan Advanced Talents (2023026), The Key Scientific Research Project of Higher Education of Henan Province (24A520054)

1 引言

传统的数字签名往往是公开可验证的，无法阻止不诚实的验证者对签名者所签署的敏感消息进行2次传播，即任意获得签名的用户都能够对消息的真实性进行验证，并对消息和签名进行无限制的2次传递。为避免上述行为，多种具有不可传递性的数字签名原语被相继提出。1989年，Chaum等人[1]提出了不可否认签名(Undeniable Signature, US)，其通过控制签名的验证解决该问题，但在验证环节要求签名者必须全程在线参与，且不可避免地涉及到繁重的零知识证明。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被赋予同等级的签名权限，任意第三方(即签名者和指定验证者之外)无法确认消息的签名是由签名者真实生成还是由指定验证者模拟，但在消息的可信度出现争议时无法提供有效的仲裁机制。1998年，Krawczyk等[3]创造性地提出了变色龙签名(Chameleon Signature, CS)，更简便地解决了签名的2次传递问题。

CS在签名算法中嵌入一个有效的变色龙哈希函数(Chameleon Hash Function, CHF)来对消息进行散列。对指定验证者而言，其利用秘密持有的陷门来计算CHF的碰撞是可行的，即能够在哈希值不变的条件下随意更换消息，从而使得2次传递的消息在任意第三方面前失去可信度；相反地，对不拥有陷门的用户，CHF仍保持抗碰撞性。相较于US, CS不依赖复杂的交互式协议和零知识证明，而是采用“哈希-签名”范式来实现离线验证。相较于DVS，对于指定验证者的伪造，CS中的签名者能够对其“证伪”，即满足签名者可拒绝性。具体地讲，签名者向仲裁者出示一个与争议组合“消息-随机数-签名值”有着相同变色龙哈希值的新3元组，由于签名者无法计算CHF的碰撞，其出示的3元组可被判定为消息的真实签名，由此证明争议为指定验证者伪造。显然地，CS在云医疗、电子选举和数字版权保护等应用场景中尤为适用[4–7]。

近年来，格密码在诸多抗量子计算的密码体制[8,9]中脱颖而出。2008年，Gentry等人[10]设计出格上原像采样算法，并基于小整数解(Small Integer Solution, SIS)难题假设，给出了随机预言机模型下基于格的强不可伪造的签名。2010年，Cash等人[11]创造性地设计出基于格的CHF。2013年，基于文献[10,11]的工作，谢等人[12]宣称构造了第1个基于格的CS方案，缺陷是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。2016年，采用文献[11]的CHF, Noh等人[13]给出了标准模型下基于格的强指定验证者签名方案，缺陷是签名必须携带大尺寸密文，且无法解决签名的争议问题。2017年，Xie等人[14]提出了同态CHF的概念，并宣称构造了基于格的有限级数的全同态签名方案，缺陷是同态CHF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需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。2023年，结合基于身份的密码体制，张等人[16]给出了两个随机预言机模型下可证明安全的格上基于身份的CS方案。

随机预言机模型下数字签名方案的安全性规约证明往往需要将哈希函数替换为一个理想化的随机预言机，即要求敌手不能利用哈希函数的弱点对方案进行攻击。而在现实中，并不存在完美的哈希函数，随机预言机模型下可证明安全的签名方案在实际具体实现中未必是安全的。进一步地，现有的CS在解决签名争议时往往遵循“谁主张，谁举证”的原则，即签名者在对指定验证者的伪造进行“打假”时，需要向仲裁者出示真实的消息和签名，因此，签名者往往需要在本地存储所有签署过的消息、签名以及相应的指定验证者身份信息，以耗费较大的本地存储来应对指定验证者的签名争议。

本文提出了标准模型下基于格的CS方案，安全性证明完全不依赖于针对哈希函数的随机预言机假设。在此基础上，给出的CS方案2彻底消除了签名者对本地签名库的依赖，使得签名者能够在不存储原始消息与签名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SIS问题和差错学习(Learning With Errors, LWE)问题是困难的，在标准模型下严格证明了两个方案满足抗自适应性选择消息攻击下强不可伪造性、签名不可传递性、签名者可拒绝性以及不可抵赖性。

2 预备知识

2.1 格

定义1 设q,m,n为正整数，给定$\boldsymbol{A}\in Z_q^{n\times m}$和$\boldsymbol{u}\in Z_q^n$，定义格$\Lambda_q^{\perp}(\boldsymbol{A})$及其陪集

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

定义2 设m为正整数，给定$\boldsymbol{c}\in R^m$和$s\in R^+$，定义格Λ上以$\boldsymbol{c}$为中心，s为参数的离散高斯分布为

$$\mathcal{D}_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\rho_{s,\boldsymbol{c}}(\boldsymbol{x})\Big/\sum_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})\tag{2}$$

其中，$\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2\Big/s^2\right)$。若$\boldsymbol{c}=\boldsymbol{0}$，

则$\mathcal{D}_{\Lambda,s,\boldsymbol{c}}$可简写为$\mathcal{D}_{\Lambda,s}$。

定义3　给定素数q, $\boldsymbol{A}\in Z_q^{n\times m}$和实数$\beta>0$，$\mathrm{SIS}_{q,m,\beta}$问题的定义为：求解齐次线性方程组$\boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{0}\bmod q$的小尺寸非0整数解$\boldsymbol{e}\in Z^m$，满足$0<\|\boldsymbol{e}\|\le\beta$。

引理1[10,17]　设整数m和实数β是关于n的多项式函数，素数$q\ge\beta\cdot\omega\left(\sqrt{n\log_2 n}\right)$和因子$\gamma\ge\beta\cdot\tilde{\mathcal{O}}\left(\sqrt{n}\right)$，则平均情况下的$\mathrm{SIS}_{q,m,\beta}$与最差情况下的最短独立向量组问题$\mathrm{SIVP}_\gamma$的难度是等价的。

定义4　给定整数q，整数环Z上的差错分布χ，$\mathrm{LWE}_{n,q,\chi}$问题的定义为：求解$\boldsymbol{b}=\boldsymbol{A}^{\mathrm{T}}\cdot s+\boldsymbol{e}\bmod q\in Z_q^m$中隐藏的秘密向量$\boldsymbol{s}\in Z_q^n$，其中$\boldsymbol{A}\in Z_q^{n\times m}$, $\boldsymbol{e}\in\chi$。

引理2[18]　设整数$m=\mathrm{poly}(n)$，实数$\beta\ge\sqrt{n}\cdot\omega(\log_2 n)$，$q$是一个素数幂，$\chi$是一个上界为$\beta$的差错分布和因子$\gamma\ge\tilde{\mathcal{O}}(nq/\beta)$，则平均情况下的$\mathrm{LWE}_{n,q,\chi}$与最差情况下的$\mathrm{SIVP}_\gamma$的难度是等价的。

引理3[11]　给定素数q, $\boldsymbol{A}_0,\boldsymbol{A}_1\in Z_q^{n\times m}$和参数$s>\left\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}_1}\right\|\cdot\omega\left(\sqrt{\log_2 n}\right)$，则$\mathrm{CHF}(\mu,\boldsymbol{r})=\boldsymbol{A}_0\cdot\boldsymbol{\mu}+\boldsymbol{A}_1\cdot\boldsymbol{r}\bmod q$的抗碰撞性与$\mathrm{SIS}_{q,m,2s\sqrt{m}}$的难度是等价的，其中$\boldsymbol{\mu}\in\{0,1\}^m$, $\boldsymbol{r}\in\mathcal{D}_{Z^m,s}$。

引理4[19,20]　设素数$q\ge 2$和整数$m\ge 2n\log_2 q$，存在概率多项式时间(Probabilistic Polynomial Time, PPT)算法TrapGen，输入q, n和m，输出$\boldsymbol{A}$和$\Lambda_q^{\perp}(\boldsymbol{A})$的一组陷门$\boldsymbol{T}_{\boldsymbol{A}}$，其中$\boldsymbol{A}$统计接近$Z_q^{n\times m}$上的均匀分布。

引理5[10]　设素数$q\ge 2$和整数$m\ge 2n\log_2 q$，存在PPT算法SamplePre，输入$\Lambda_q^{\perp}(\boldsymbol{A})$的陷门$\boldsymbol{T}_{\boldsymbol{A}}$,$\boldsymbol{u}\in Z_q^n$和高斯参数$s>\left\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\right\|\cdot\omega\left(\sqrt{\log_2 m}\right)$，输出统计接近$\mathcal{D}_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}),s}$的短向量$\boldsymbol{e}\in Z^m$，且满足$\boldsymbol{u}=\boldsymbol{A}\cdot\boldsymbol{e}\bmod q$。

2.2 变色龙签名

令消息空间为$\mathcal{M}$，随机数空间为$\mathcal{R}$以及签名值空间为$\mathcal{S}$。一个标准的变色龙签名[3]主要包括3个参与方：签名者S，指定验证者V以及仲裁者J，且由以下6个多项式时间算法构成：

Setup：由系统运行的概率性算法。输入安全参数λ，输出公共参数pp。

KeyGen：由系统运行的概率性算法。输入参数pp，输出S与V的公私钥对$(\mathrm{pk_S},\mathrm{sk_S})$和$(\mathrm{pk_V},\mathrm{sk_V})$。

Sign：由签名者S运行的概率性算法。输入参数pp，S的公私钥对$(\mathrm{pk_S},\mathrm{sk_S})$，V的公钥$\mathrm{pk_V}$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：由指定验证者V运行的确定性算法。输入参数pp，S的公钥$\mathrm{pk_S}$，V的公钥$\mathrm{pk_V}$，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：由指定验证者V运行的概率性算法。输入参数pp，S的公钥$\mathrm{pk_S}$，V的公私钥对$(\mathrm{pk_V},\mathrm{sk_V})$以及由S运行算法$\mathrm{Sign}(\mathrm{pp},\mathrm{pk_S},\mathrm{sk_S},\mathrm{pk_V},\mu)$生成的$\mu\in\mathcal{M}$，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$\mathrm{Verify}(\mathrm{pp},\mathrm{pk_S},\mathrm{pk_V},\mu',r',\sigma)\to 1$。

DenialPro：由签名者S和仲裁者J共同执行的一个公开的拒绝协议。给定S的公钥$\mathrm{pk_S}$，V的公钥$\mathrm{pk_V}$以及V提交给J的一个争议签名$(\mu',r',\sigma)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$，S向J提交碰撞$(\mu,r,\sigma)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$，最终，J判定争议组合$(\mu',r',\sigma)$为S真实生成或V伪造。

一个安全的CS方案满足以下性质：

定义5　若任意PPT的敌手$\mathcal{A}$赢得以下游戏的优势$\mathrm{Adv}_{\mathrm{CS},\mathcal{A}}^{\mathrm{unforgeability}}$是可忽略的，则称CS是抗自适应性选择消息攻击下强不可伪造的。

Setup：挑战者$\mathcal{C}$运行算法Setup和算法KeyGen生成系统公共参数pp，签名者S和指定验证者V的公私钥对$(\mathrm{pk_S},\mathrm{sk_S})$和$(\mathrm{pk_V},\mathrm{sk_V})$。$\mathcal{C}$秘密持有$\mathrm{sk_S}$和$\mathrm{sk_V}$，并将$(\mathrm{pp},\mathrm{pk_S},\mathrm{pk_V})$发送给敌手$\mathcal{A}$。

Sign query：$\mathcal{A}$自适应性地询问任意消息$\sigma\in\mathcal{M}$的签名，$\mathcal{C}$返回(μ,r,σ)。

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

(1) $\mathrm{Verify}(\mathrm{pp},\mathrm{pk_S},\mathrm{pk_V},\mu^*,r^*,\sigma^*)\to 1$；

(2) (μ^*,r^*,σ^*)不是Sign query的返回。

定义6　若任意PPT的敌手$\mathcal{A}$赢得以下游戏的优势$\mathrm{Adv}_{\mathrm{CS},\mathcal{A}}^{\mathrm{non-transferability}}$是可忽略的，则称CS是不可传递的。

Setup：挑战者$\mathcal{C}$运行算法Setup和算法KeyGen生成系统公共参数pp，签名者S和指定验证者V的公私钥对$(\mathrm{pk_S},\mathrm{sk_S})$和$(\mathrm{pk_V},\mathrm{sk_V})$，并将其全部发送给敌手$\mathcal{A}$。

Challenge：$\mathcal{C}$随机选取消息$\mu_0\in\mathcal{M}$，运行算法$\mathrm{Sign}(\mathrm{pp},\mathrm{pk_S},\mathrm{pk_V},\mathrm{sk_S},\mu_0)$生成$r_0\in\mathcal{R}$和$\sigma\in\mathcal{S}$；运行算法$\mathrm{Forge}(\mathrm{pp},\mathrm{pk_S},\mathrm{pk_V},\mathrm{sk_V},\mu_0,r_0,\sigma)$生成新消息$\mu_1\in\mathcal{M}$和$r_1\in\mathcal{R}$；随机选取$b\in\{0,1\}$，并返回$(\mu_b,r_b,\sigma)$。

Output：$\mathcal{A}$输出$b^*\in\{0,1\}$。若$b^*=b$，则$\mathcal{A}$获胜。

定义7　若$(\mu',r',\sigma)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$为指定验证者V伪造，且签名者S有能力说服仲裁者J拒绝该签名，则称CS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S真实生成，且其无法否认，则称CS满足签名者不可抵赖性。上述性质可由S与J之间的一个公开的拒绝协议DenialPro来保证：

对于V向J提交的争议签名$(\mu',r',\sigma)\in\mathcal{M}\times$

$\mathcal{R}\times\mathcal{S}$，S向J提交碰撞$(\mu,r,\sigma)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$：

(1) 若$\mu\neq\mu'$，且$\text{Verify}\left(\text{pp},\text{pk}_\text{S},\text{pk}_\text{V},\mu,r,\sigma\right)\to 1$，则J可断定$(\mu',r',\sigma)$非S生成，而是由V伪造；

(2) 否则，J判定(μ',r',σ)为S生成。

3 标准模型下基于格的变色龙签名

3.1 方案构造

$\text{Setup}\left(1^\lambda\right)\to(\text{pp})$：输入安全参数$\lambda$，令整数$n=\text{poly}\left(\lambda\right)$，素数$q=\tilde{\mathcal{O}}\left(n^3\right)$，整数$m\geq 2n\log_2 q$，高斯参数$s=\tilde{\mathcal{O}}\left(n\right)$，消息空间$\mathcal{M}=\{0,1\}^m$，随机数空间$\mathcal{R}=\mathcal{D}_{Z^m,s}$以及签名值空间$\mathcal{S}=\mathcal{D}_{Z^m,s}$。系统执行以下操作：

(1) 随机选取$\boldsymbol{A}\in Z_q^{n\times m}$,$\boldsymbol{v}_0\in Z_q^n$和$n$个线性独立的$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n\in Z_q^n$；

(2) 选取抗碰撞哈希函数$\mathcal{H}$：$\{0,1\}^*\to\{0,1\}^n$；

(3) 输出公共参数$\text{pp}=(\boldsymbol{A},\boldsymbol{v}_0,\boldsymbol{v}_1,\cdots,\boldsymbol{v}_n,\mathcal{H})$。

$\text{KeyGen}\left(\text{pp}\right)\to(\text{pk}_\text{S},\text{sk}_\text{S},\text{pk}_\text{V},\text{sk}_\text{V})$：输入公共参数pp，系统执行以下操作：

(1) 运行$\text{TrapGen}\left(q,n,m\right)$两次，生成$\boldsymbol{A}_\text{S}$和$\Lambda_q^\perp\left(\boldsymbol{A}_\text{S}\right)$的陷门$\boldsymbol{T}_{\boldsymbol{A}_\text{S}}$以及$\boldsymbol{A}_\text{V}$和$\Lambda_q^\perp\left(\boldsymbol{A}_\text{V}\right)$的陷门$\boldsymbol{T}_{\boldsymbol{A}_\text{V}}$；

(2) 输出S的公私钥对$(\text{pk}_\text{S},\text{sk}_\text{S})=(\boldsymbol{A}_\text{S},\boldsymbol{T}_{\boldsymbol{A}_\text{S}})$和V的公私钥对$(\text{pk}_\text{V},\text{sk}_\text{V})=(\boldsymbol{A}_\text{V},\boldsymbol{T}_{\boldsymbol{A}_\text{V}})$。

$\text{Sign}\left(\text{pp},\text{pk}_\text{S},\text{pk}_\text{V},\text{sk}_\text{S},\boldsymbol{\mu}\right)\to(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})$：输入公共参数pp，S的公私钥对$(\text{pk}_\text{S},\text{sk}_\text{S})=(\boldsymbol{A}_\text{S},\boldsymbol{T}_{\boldsymbol{A}_\text{S}})$，V的公钥$\text{pk}_\text{V}=\boldsymbol{A}_\text{V}$以及消息$\boldsymbol{\mu}\in\{0,1\}^m$，签名者S执行以下操作：

(1) 首先查找本地签名库是否存储$(\text{pk}_\text{V},\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})$，若存在，执行(5)，否则执行(2)～(5)；

(2) 随机选取$\boldsymbol{r}\in\mathcal{R}$，计算关于$\boldsymbol{\mu}$的变色龙哈希值$\boldsymbol{y}=\text{CHF}\left(\boldsymbol{\mu},\boldsymbol{r}\right)=\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_\text{V}\cdot\boldsymbol{r}\text{mod}q$；

(3) 令$\boldsymbol{h}=(h_1,h_2,\cdots,h_n)=\mathcal{H}\left(\text{pk}_\text{S},\text{pk}_\text{V},\boldsymbol{y}\right)$，计算$\boldsymbol{v}=\boldsymbol{v}_0+\sum_{i=1}^n h_i\cdot\boldsymbol{v}_i\text{mod}q$；

(4) 运行$\text{SamplePre}\left(\boldsymbol{A}_\text{S},\boldsymbol{T}_{\boldsymbol{A}_\text{S}},\boldsymbol{v},s\right)$，生成签名值$\boldsymbol{\sigma}\in Z^m$，并存储$(\text{pk}_\text{V},\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})$于本地签名库；

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

$\text{Verify}\left(\text{pp},\text{pk}_\text{S},\text{pk}_\text{V},\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma}\right)\to(1\text{ or }0)$：输入公共参数pp，S的公钥$\text{pk}_\text{S}=\boldsymbol{A}_\text{S}$，V的公钥$\text{pk}_\text{V}=\boldsymbol{A}_\text{V}$，消息$\boldsymbol{\mu}\in\mathcal{M}$，随机数$\boldsymbol{r}\in\mathcal{R}$以及签名值$\boldsymbol{\sigma}\in\mathcal{S}$，指定验证者V执行以下操作：

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

(2) 计算$\boldsymbol{y}=\text{CHF}\left(\boldsymbol{\mu},\boldsymbol{r}\right)=\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_\text{V}\cdot\boldsymbol{r}\text{mod}q$，$\boldsymbol{h}=(h_1,h_2,\cdots,h_n)=\mathcal{H}\left(\text{pk}_\text{S},\text{pk}_\text{V},\boldsymbol{y}\right)\in\{0,1\}^n$；

(3) 验证$\boldsymbol{A}_\text{S}\cdot\boldsymbol{\sigma}=\boldsymbol{v}_0+\sum_{i=1}^n h_i\cdot\boldsymbol{v}_i\text{mod}q$是否成立；

(4) 若以上条件全部成立，输出1，否则输出0。

$\text{Forge}\left(\text{pp},\text{pk}_\text{S},\text{pk}_\text{V},\text{sk}_\text{V},\boldsymbol{\mu},\boldsymbol{r},\sigma\right)\to(\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma})$：输入公共参数pp，V的公私钥对$(\text{pk}_\text{V},\text{sk}_\text{V})=(\boldsymbol{A}_\text{V},\boldsymbol{T}_{\boldsymbol{A}_\text{V}})$，S的公钥$\text{pk}_\text{S}=\boldsymbol{A}_\text{S}$以及由S生成的$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$，指定验证者V执行以下操作：

(1) 计算$\boldsymbol{y}=\text{CHF}\left(\boldsymbol{\mu},\boldsymbol{r}\right)=\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_\text{V}\cdot\boldsymbol{r}\text{mod}q$；

(2) 选取新消息$\boldsymbol{\mu}'\in\{0,1\}^m$，运行$\text{SamplePre}\left(\boldsymbol{A}_\text{V},\boldsymbol{T}_{\boldsymbol{A}_\text{V}},\boldsymbol{y}-\boldsymbol{A}\cdot\boldsymbol{\mu}',s\right)$，生成随机数$\boldsymbol{r}'\in\mathcal{R}$；

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

$\text{DenialPro}\left(\text{pp},\text{pk}_\text{S},\text{pk}_\text{V},\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma}\right)\to(\text{S or V})$：输入公共参数pp，S的公钥$\text{pk}_\text{S}$，V的公钥$\text{pk}_\text{V}$以及V提交给J的一个争议组合$(\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma})\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$，签名者S和仲裁者J执行以下操作：

(1) S查找本地签名库，向J提交碰撞$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$；

(2) J执行算法Verify，若输出为1，且$\boldsymbol{\mu}\neq\boldsymbol{\mu}'$，则判定$(\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma})$为V伪造；否则判定为S真实生成。

3.2 安全性分析

定理1 假设$\text{SIS}_{q,m,2s\sqrt{m}}$和$\text{SIS}_{q,2m,2s\sqrt{m}}$是困难的，则本方案满足抗自适应性选择消息攻击下强不可伪造性。

证明 假设$\mathcal{A}$为向本文方案发起自适应性选择消息攻击的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$\text{SIS}_{q,m,2s\sqrt{m}}$难题实例$\boldsymbol{A}^*\cdot\boldsymbol{e}^*=\boldsymbol{0}\text{mod}q$或$\text{SIS}_{q,2m,2s\sqrt{m}}$难题实例$(\boldsymbol{A}|\boldsymbol{A}_\text{V})\cdot\boldsymbol{e}^*=\boldsymbol{0}\text{mod}q$的挑战者，其中$\boldsymbol{A}^*,\boldsymbol{A},\boldsymbol{A}_\text{V}\in Z_q^{n\times m}$。挑战者$\mathcal{C}$与敌手$\mathcal{A}$之间的交互游戏如下：

Setup:$\mathcal{C}$模拟以下环境：

(1) 令$\boldsymbol{A}$为构造变色龙哈希函数CHF的公共矩阵，选取抗碰撞哈希函数$\mathcal{H}$：$\{0,1\}^*\to\{0,1\}^n$；

(2) 随机选取$n+1$个短向量$\boldsymbol{\sigma}_0,\boldsymbol{\sigma}_1,\cdots,\boldsymbol{\sigma}_n\in\mathcal{D}_{Z^m,s'}$，其中$s'=s/\left(n+1\right)$；

(3) 令$\boldsymbol{v}_0=\boldsymbol{A}^*\cdot\boldsymbol{\sigma}_0\text{mod}q$和$\boldsymbol{v}_i=\boldsymbol{A}^*\cdot\boldsymbol{\sigma}_i\text{mod}q$，其中$i\in\{1,2,\cdots,n\}$(需注意：若$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n$不是线性独立的，重新选取$\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2,\cdots,\boldsymbol{\sigma}_n\in\mathcal{D}_{Z^m,s'}$)；

(4) 令签名者S的公钥$\text{pk}_\text{S}=\boldsymbol{A}^*$，指定验证者V的公钥$\text{pk}_\text{V}=\boldsymbol{A}_\text{V}$；

(5) 将$(\boldsymbol{A},\boldsymbol{v}_0,\boldsymbol{v}_1,\cdots,\boldsymbol{v}_n,\mathcal{H},\boldsymbol{A}^*,\boldsymbol{A}_\text{V})$发送给$\mathcal{A}$。

Sign query：$\mathcal{A}$输入任意消息$\boldsymbol{\mu}\in\mathcal{M}$，$\mathcal{C}$执行以下操作：

(1) 查找本地签名库，若存在$(\text{pk}_\text{V},\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})$，直接返回$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$；

(2) 否则，随机选取$\boldsymbol{r}\in\mathcal{R}$，计算关于$\boldsymbol{\mu}$的变色龙哈希值$\boldsymbol{y}=\text{CHF}\left(\boldsymbol{\mu},\boldsymbol{r}\right)=\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_\text{V}\cdot\boldsymbol{r}\text{mod}q$；

(3) 令$\boldsymbol{h}=(h_1,h_2,\cdots,h_n)=\mathcal{H}\left(\text{pk}_\text{S},\text{pk}_\text{V},\boldsymbol{y}\right)\in\{0,1\}^n$，计算$\boldsymbol{\sigma}=\boldsymbol{\sigma}_0+\sum_{i=1}^n h_i\cdot\boldsymbol{\sigma}_i\in Z^m$；

(4) 将$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})$发送给$\mathcal{A}$，并存储$(\text{pk}_\text{V},\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})$于本地签名库。

Output：$\mathcal{A}$输出一个伪造$(\boldsymbol{\mu}^*,\boldsymbol{r}^*,\boldsymbol{\sigma}^*)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$，满足：

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

(2) $(\boldsymbol{\mu}^*,\boldsymbol{r}^*,\boldsymbol{\sigma}^*)$不是Sign query的返回。

当$\mathcal{A}$输出一个有效的伪造$(\boldsymbol{\mu}^*,\boldsymbol{r}^*,\boldsymbol{\sigma}^*)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$，$\mathcal{C}$计算$\boldsymbol{y}^*=\text{CHF}\,(\boldsymbol{\mu}^*,\boldsymbol{r}^*)=\boldsymbol{A}\cdot\boldsymbol{\mu}^*+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r}^*\text{mod}q$，令$\boldsymbol{h}^*=(h_1^*,h_2^*,\cdots,h_n^*)=\mathcal{H}\,(\text{pk}_{\text{S}},\text{pk}_{\text{V}},\boldsymbol{y}^*)$，易知$\boldsymbol{A}^*\cdot\boldsymbol{\sigma}^*=\boldsymbol{v}_0+\sum_{i=1}^{n}h_i^*\cdot\boldsymbol{v}_i=\boldsymbol{A}^*\cdot(\boldsymbol{\sigma}_0+\sum_{i=1}^{n}h_i^*\cdot\boldsymbol{\sigma}_i)\,\text{mod}q$。

分以下两种情况进行讨论：

(1) 若$\mathcal{H}\,(\text{pk}_{\text{S}},\text{pk}_{\text{V}},\boldsymbol{A}\cdot\boldsymbol{\mu}^*+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r}^*)=\mathcal{H}\,(\text{pk}_{\text{S}},\text{pk}_{\text{V}},\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r})$，其中$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$为$\mathcal{A}$的某个Sign query的返回。显然地，$\boldsymbol{A}\cdot\boldsymbol{\mu}^*+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r}^*=\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r}\text{mod}q$，又分两种情况讨论：

(a) $\boldsymbol{\mu}^*\neq\boldsymbol{\mu}$或$\boldsymbol{r}^*\neq\boldsymbol{r}$，则输出CHF的碰撞$(\boldsymbol{\mu}^*,\boldsymbol{r}^*)$和$(\boldsymbol{\mu},\boldsymbol{r})$。由引理3可知，$\mathcal{C}$以优势$\text{Adv}_{\text{CS},\mathcal{A}}^{\text{unforgeability}}\approx\varepsilon$输出$\text{SIS}_{q,2m,2s\sqrt{m}}$难题的一个有效解$\boldsymbol{e}^*=\begin{pmatrix}\boldsymbol{\mu}^*-\boldsymbol{\mu}\\ \boldsymbol{r}^*-\boldsymbol{r}\end{pmatrix}\in Z^{2m}$，即满足$(\boldsymbol{A}\,|\boldsymbol{A}_{\text{V}})\cdot\boldsymbol{e}^*=\boldsymbol{0}\text{mod}q$，且$0<\|\boldsymbol{e}^*\|\leq 2s\sqrt{m}$。

(b) $\boldsymbol{\mu}^*=\boldsymbol{\mu}$且$\boldsymbol{r}^*=\boldsymbol{r}$，则由于$\mathcal{A}$赢得游戏的条件是输出一个有效的强伪造签名，即$(\boldsymbol{\mu}^*,\boldsymbol{r}^*,\boldsymbol{\sigma}^*)$不是Sign query的返回，因此，$\boldsymbol{\sigma}^*\neq\boldsymbol{\sigma}_0+\sum_{i=1}^{n}\boldsymbol{h}_i^*\cdot\boldsymbol{\sigma}_i$。

(2) 若$\mathcal{H}\,(\text{pk}_{\text{S}},\text{pk}_{\text{V}},\boldsymbol{A}\cdot\boldsymbol{\mu}^*+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r}^*)\neq\mathcal{H}\,(\text{pk}_{\text{S}},\text{pk}_{\text{V}},\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r})$，其中$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma})\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}$为$\mathcal{A}$的任意Sign query。令$\boldsymbol{\sigma}=\boldsymbol{\sigma}_0+\sum_{i=1}^{n}h_i^*\cdot\boldsymbol{\sigma}_i$，显然地，$\|\boldsymbol{\sigma}\|\leq(n+1)\cdot s'\sqrt{m}=s\sqrt{m}$，又可知

$$\boldsymbol{A}^*\cdot\boldsymbol{\sigma}=\boldsymbol{v}_0+\sum_{i=1}^{n}h_i^*\cdot\boldsymbol{v}_i\text{mod}q=\boldsymbol{A}^*\cdot\boldsymbol{\sigma}^*\qquad(3)$$

进一步地，由最小熵性质[10]可知，给定原像采样函数$f_{\boldsymbol{A}^*}(\boldsymbol{e}^*)=\boldsymbol{A}^*\cdot\boldsymbol{e}^*\text{mod}q$，短向量$\boldsymbol{e}^*\in\mathcal{D}_{Z^m,s}$的最小熵为$\omega\,(\log_2 n)$。因此，$\boldsymbol{\sigma}^*\neq\boldsymbol{\sigma}$以压倒性概率$1-2^{-\omega(\log_2 n)}$成立。

综上可知，若$\boldsymbol{\sigma}^*\neq\boldsymbol{\sigma}_0+\sum_{i=1}^{n}h_i^*\cdot\boldsymbol{\sigma}_i$，则$\mathcal{C}$可求得原像采样函数$f_{\boldsymbol{A}^*}(\boldsymbol{e}^*)=\boldsymbol{A}^*\cdot\boldsymbol{e}^*\text{mod}q$的一个有效碰撞$(\boldsymbol{\sigma}^*,\boldsymbol{\sigma})$，即$\mathcal{C}$以优势$\text{Adv}_{\text{CS},\mathcal{A}}^{\text{unforgeability}}=\left(1-2^{-\omega(\log_2 n)}\right)\cdot\varepsilon$输出$\text{SIS}_{q,m,2s\sqrt{m}}$难题的一个有效解$\boldsymbol{e}^*=\boldsymbol{\sigma}^*-\boldsymbol{\sigma}\in Z^m$，即满足$\boldsymbol{A}^*\cdot\boldsymbol{e}^*=\boldsymbol{0}\text{mod}q$，且$0<\|\boldsymbol{e}^*\|\leq 2s\sqrt{m}$。

定理2　本文方案满足签名不可传递性、签名者可拒绝性和不可抵赖性。

证明　与文献[16]中定理2和定理3的证明思路相同，鉴于篇幅原因，将不再详细赘述。

4　标准模型下基于格的无需本地存储的变色龙签名

大多数CS方案在解决签名争议，即S在对V的伪造进行“打假”时，需要向J出示真实的消息和签名，因此，S往往需要在本地存储所有签署过的消息、签名以及V的公钥，以耗费较大的存储来应对V的签名争议。本节给出无需本地存储的CS方案，使得S能够在不存储原始消息与签名的条件下辅助J拒绝任意敌手伪造的签名，彻底消除了S对本地签名库的依赖。除了增添一个随机选取的$\boldsymbol{B}\in Z_q^{n\times m}$，算法Setup和算法KeyGen与已给出的标准模型下基于格的CS方案中完全相同，将不再赘述，重点介绍新的算法设计细节。

4.1　方案构造

$\text{Setup}\,(1^\lambda)\to(\text{pp})$：输入安全参数$\lambda$，输出公共参数$\text{pp}=(\boldsymbol{A},\boldsymbol{B},\boldsymbol{v}_0,\boldsymbol{v}_1,\cdots,\boldsymbol{v}_n,\mathcal{H})$。

$\text{KeyGen}\,(\text{pp})\to(\text{pk}_{\text{S}},\text{sk}_{\text{S}},\text{pk}_{\text{V}},\text{sk}_{\text{V}})$：输入公共参数pp，输出S和V的公私钥对$(\text{pk}_{\text{S}},\text{sk}_{\text{S}})$和$(\text{pk}_{\text{V}},\text{sk}_{\text{V}})$。

$\text{Sign}\,(\text{pp},\text{pk}_{\text{S}},\text{pk}_{\text{V}},\text{sk}_{\text{S}},\boldsymbol{\mu})\to(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)$输入参数pp，S的公私钥对$(\text{pk}_{\text{S}},\text{sk}_{\text{S}})=(\boldsymbol{A}_{\text{S}},\boldsymbol{T}_{\boldsymbol{A}_{\text{S}}})$，V的公钥$\text{pk}_{\text{V}}=\boldsymbol{A}_{\text{V}}$以及消息$\boldsymbol{\mu}\in\mathcal{M}$，签名者S执行以下操作：

(1) 随机选取$\boldsymbol{r}\in\mathcal{R}$，计算关于$\boldsymbol{\mu}$的变色龙哈希值$\boldsymbol{y}=\text{CHF}\,(\boldsymbol{\mu},\boldsymbol{r})=\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r}\text{mod}q$；

(2) 随机选取$\boldsymbol{s}_1\in Z_q^n$和$\boldsymbol{e}_0,\boldsymbol{e}_1\in\mathcal{R}$，计算$\boldsymbol{b}_0=\boldsymbol{A}_{\text{S}}^{\text{T}}\cdot\boldsymbol{s}_1+\boldsymbol{e}_0\text{mod}q$和$\boldsymbol{b}_1=\boldsymbol{B}^{\text{T}}\cdot\boldsymbol{s}_1+\boldsymbol{e}_1+\boldsymbol{\mu}\cdot\lfloor q/2\rfloor\,\text{mod}q$；

(3) 随机选取$\boldsymbol{s}_2\in Z_q^n$，计算$\boldsymbol{b}_2=\boldsymbol{A}_{\text{S}}^{\text{T}}\cdot\boldsymbol{s}_2+\boldsymbol{r}\text{mod}q$；

(4) 令$\boldsymbol{h}=(h_1,h_2,\cdots,h_n)=\mathcal{H}\,(\text{pk}_{\text{S}},\text{pk}_{\text{V}},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2,\boldsymbol{y})\in\{0,1\}^n$，计算$\boldsymbol{v}=\boldsymbol{v}_0+\sum_{i=1}^{n}h_i\cdot\boldsymbol{v}_i\text{mod}q$；

(5) 运行$\text{SamplePre}\,(\boldsymbol{A}_{\text{S}},\boldsymbol{T}_{\boldsymbol{A}_{\text{S}}},\boldsymbol{v},s)$，生成签名值$\boldsymbol{\sigma}\in Z^m$；

(6) 输出$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)$。

$\text{Verify}\,(\text{pp},\text{pk}_{\text{S}},\text{pk}_{\text{V}},\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)\to(1\text{ or }0)$：输入参数pp，S的公钥$\text{pk}_{\text{S}}=\boldsymbol{A}_{\text{S}}$，V的公钥$\text{pk}_{\text{V}}=\boldsymbol{A}_{\text{V}}$，消息$\boldsymbol{\mu}\in\mathcal{M}$，随机数$\boldsymbol{r}\in\mathcal{R}$以及签名$(\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)\in\mathcal{S}\times\left(Z_q^m\right)^3$，指定验证者V执行以下操作：

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

(2) 计算$\boldsymbol{y}=\text{CHF}\,(\boldsymbol{\mu},\boldsymbol{r})=\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_{\text{V}}\cdot\boldsymbol{r}\text{mod}q$，$\boldsymbol{h}=(h_1,h_2,\cdots,h_n)=\mathcal{H}\,(\text{pk}_{\text{S}},\text{pk}_{\text{V}},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2,\boldsymbol{y})\in\{0,1\}^n$；

(3) 验证$\boldsymbol{A}_{\text{S}}\cdot\boldsymbol{\sigma}=\boldsymbol{v}_0+\sum_{i=1}^{n}h_i\cdot\boldsymbol{v}_i\text{mod}q$是否成立；

(4) 若以上条件全部成立，输出1，否则输出0。

$\text{Forge}(\text{pp},\text{pk}_{\text{S}},\text{pk}_{\text{V}},\text{sk}_{\text{V}},\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)\to(\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)$：输入参数pp，S的公钥$\text{pk}_{\text{S}}=\boldsymbol{A}_{\text{S}}$，V的公私钥对$(\text{pk}_{\text{V}},\text{sk}_{\text{V}})=(\boldsymbol{A}_{\text{V}},\boldsymbol{T}_{\boldsymbol{A}_{\text{V}}})$以及由S生成的

$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}\times\left(Z_q^m\right)^3$，V执行以下操作：

(1) 计算$\boldsymbol{y}=\mathrm{CHF}(\boldsymbol{\mu},\boldsymbol{r})=\boldsymbol{A}\cdot\boldsymbol{\mu}+\boldsymbol{A}_{\mathrm{V}}\cdot\boldsymbol{r}\mathrm{mod}q$；

(2) 选取新消息$\boldsymbol{\mu}'\in\mathcal{M}$，运行SamplePre$(\boldsymbol{A}_{\mathrm{V}},\boldsymbol{T}_{\boldsymbol{A}_{\mathrm{V}}},\boldsymbol{y}-\boldsymbol{A}\cdot\boldsymbol{\mu}',s)$，生成随机数$\boldsymbol{r}'\in\mathcal{R}$；

(3) 输出$(\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)$。

DenialPro$(\mathrm{pp},\mathrm{pk_S},\mathrm{pk_V},\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)\to$(S or V)输入参数pp，S的公钥$\mathrm{pk_S}$，V的公钥$\mathrm{pk_V}$以及V提交给J的一个争议组合$(\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)\in\mathcal{M}\times\mathcal{R}\times\mathcal{S}\times\left(Z_q^m\right)^3$，签名者S和仲裁者J执行以下操作：

(1) S运行SamplePre$(\boldsymbol{A}_{\mathrm{S}},\boldsymbol{T}_{\boldsymbol{A}_{\mathrm{S}}},\boldsymbol{B},s)$，生成$\boldsymbol{E}\in Z^{m\times m}$，并计算$\boldsymbol{\mu}=\left[\left(\boldsymbol{b}_1-\boldsymbol{E}^{\mathrm{T}}\cdot\boldsymbol{b}_0\mathrm{mod}q\right)\cdot 2/q\right]$；

(2) S计算$\boldsymbol{r}=\boldsymbol{T}_{\boldsymbol{A}_{\mathrm{S}}}^{-\mathrm{T}}\cdot\left(\boldsymbol{T}_{\boldsymbol{A}_{\mathrm{S}}}^{\mathrm{T}}\cdot\boldsymbol{b}_2\right)$，在这里，$\boldsymbol{T}_{\boldsymbol{A}_{\mathrm{S}}}^{-\mathrm{T}}$是$\boldsymbol{T}_{\boldsymbol{A}_{\mathrm{S}}}^{\mathrm{T}}$的逆矩阵；

(3) S向J提交碰撞$(\boldsymbol{\mu},\boldsymbol{r},\boldsymbol{\sigma},\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2)$；

(4) J执行算法Verify，若输出为1，且$\boldsymbol{\mu}\neq\boldsymbol{\mu}'$，则判定$(\boldsymbol{\mu}',\boldsymbol{r}',\boldsymbol{\sigma})$为V伪造；否则判定为S真实生成。

4.2 安全性分析

定理3 假设$\mathrm{SIS}_{q,m,2s\sqrt{m}}$问题、$\mathrm{SIS}_{q,2m,2s\sqrt{m}}$问题和$\mathrm{LWE}_{n,q,\mathcal{D}_{Z^m,s}}$问题是困难的，则本文方案满足抗自适应性选择消息攻击下强不可伪造性、签名不可传递性、签名者可拒绝性以及不可抵赖性。

证明 与已给方案1的安全性证明思路相同，鉴于篇幅原因，将不再详细赘述。

5 效率分析

本文提出的两个标准模型下基于格的CS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，本文提出的方案1结合了抗量子计算攻击的格密码体制和标准模型下可证明安全方案强的安全性保证，避免了文献[12]中任意第三方可伪造签名和签名者S无法拒绝指定验证者V伪造的签名的安全性漏洞；解决了文献[13]中S与V关于签名的争议问题；弥补了文献[16]中标准模型下可证明安全的基于格的CS的空缺。方案2采用了对消息和随机数的随机编码策略，在签名算法中对真实消息和随机数进行基于LWE难题假设的保密认证，解决了方案1在仲裁阶段对本地签名库严重依赖的问题，使得S能够在不存储原始消息与签名的条件下辅助仲裁者J拒绝任意敌手伪造的签名，进而获得无需本地存储的签名者可拒绝性。特别地，本文提出的方案1和2虽未获得文献[16]中方案2的抗消息暴露安全性，但是对消息的随机分割策略很容易迁移到本文方案，构造细节不再赘述。

从存储和传输成本方面看，本文提出的方案1与张等人[16]给出的随机预言机模型下可证明安全的格上基于身份的CS类似，将最终签名中的随机矩阵作为系统的公共参数，不再由S每次选取后与随机数$\boldsymbol{r}\in\mathcal{R}$和签名值$\boldsymbol{\sigma}\in\mathcal{S}$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$Z_q^{n\times m}$上的一个随机矩阵、Z_q^n上的$n+1$个随机向量和一个输出为n长比特串的抗碰撞哈希函数，最终的签名仅包含一个消息$\boldsymbol{\mu}\in\mathcal{M}$和$\mathcal{D}_{Z^m,s}$上的两个短向量，减少了文献[13–16]中公共参数的存储成本，提高了签名的传输效率。方案2的签名过程采用了基于LWE难题假设的随机编码策略，对消息$\boldsymbol{\mu}\in\mathcal{M}$进行公钥加密和对随机数$\boldsymbol{r}\in\mathcal{R}$进行随机编码、一次变色龙哈希计算和一次高斯原像采样，最终的签名仅包含一个消息$\boldsymbol{\mu}\in\mathcal{M}$,$\mathcal{D}_{Z^m,s}$上的两个短向量以及$Z_q^m$上的3个随机向量，即签名长度有所增加，但渐进复杂度仍与方案1相同；特别地，彻底消除了文献[12–16]和方案1中签名者S对本地签名库的依赖，较大地节约了本地存储成本。

为了更直观地比较本文的两个方案与现有基于格的可证明安全的CS方案[16]在签名生成算法Sign、签名模拟算法Forge和签名验证算法Verify中的运行时间，进行了6次仿真实验，分别采用不同的系统参数，如表2所示。

为便于表述，用ST表示原像采样算法SamplePre

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	无需本地存储	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
文献[16]	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	√	√	√	√	×	随机预言机
本文方案1	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	√	√	√	√	×	标准
本文方案2	$\tilde{\mathcal{O}}(n^2)$	$\tilde{\mathcal{O}}(n)$	√	√	√	√	√	标准

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。

的运行时间，MT表示矩阵向量乘法的运行时间。在这里，所有算法的运行均以操作系统Windows 10，处理器Intel(R) Core(TM) i7-8565U 1.80 Ghz，内存8 GB的主机，密码开源库PALISADE以及MATLAB 2023b为实验环境得出，如表3和图1所示。

表 2　参数设置

参数	设置号					
	1	2	3	4	5	6
n	128	136	192	214	256	320
q	14680063	17608247	56623093	78402743	134217803	294912113
m	6144	6528	9984	11556	13824	17920

表 3　不同方案的运行时间

方案	Sign	Forge	Verify
文献[16]方案1	$\mathrm{ST}+(2m+2)\,\mathrm{MT}$	$\mathrm{ST}+(m+3)\,\mathrm{MT}$	$(2m+3)\,\mathrm{MT}$
文献[16]方案2	$\mathrm{ST}+(2m+4)\,\mathrm{MT}$	$\mathrm{ST}+(m+3)\,\mathrm{MT}$	$(2m+5)\,\mathrm{MT}$
本文方案1	ST + 2MT	ST + 3MT	3MT
本文方案2	ST + 5MT	ST + 3MT	3MT

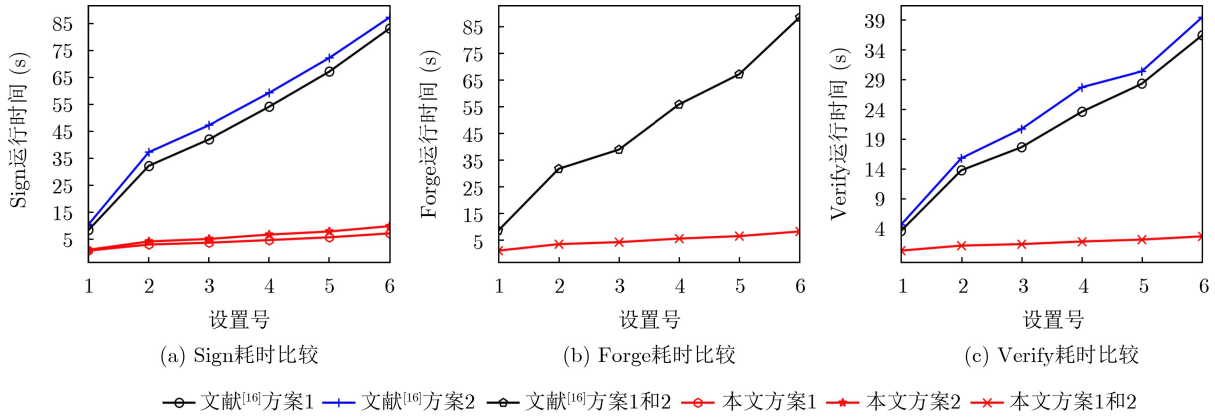

图 1 各方案耗时比较

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、签名者可拒绝性以及不可抵赖性，抗消息暴露安全性也可通过简单的方案调整获得，且标准模型下的安全性证明完全不依赖于针对哈希函数的随机预言机假设，在实际具体实现中获得了更强的安全性保证；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，较大地节约了签名者S的本地存储成本，更适用于低存储的轻量级设备生成不可传递性的数字签名；进一步地，运行耗时更少，计算效率有较好的优势，因而方案整体效率更高。

6　结束语

通过结合抗量子计算攻击的格密码体制和标准模型下可证明安全方案强的安全性保证，本文提出了标准模型下基于格的变色龙签名方案，弥补了标准模型下可证明安全的基于格的变色龙签名的空缺；进一步地，针对签名者需要耗费较大的本地存储来应对指定验证者的签名争议的问题，提出了标准模型下基于格的无需本地存储的变色龙签名方案，通过对消息和随机数进行保密认证，使得签名者完全消除了对本地签名库的依赖。在小整数解难题和差错学习难题假设下，本文在标准模型下严格证明了两个方案满足抗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，以及第2个方案的无需本地存储的签名者可拒绝性。此外，给出的两个变色龙签名方案也具有轻量级的数字签名适配性，可满足相应的实用性需求。

参 考 文 献

[1] CHAUM D and VAN ANTWERPEN H. Undeniable signatures[M]. BRASSARD G. Advances in Cryptology -

CRYPTO '89. New York: Springer, 1990: 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[EB/OL]. http://eprint.iacr.org/1998/10, 1998.

[4] 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.

[5] JIA Meng, CHEN Jing, HE Kun, *et al*. Redactable blockchain from decentralized chameleon hash functions[J]. *IEEE Transactions on Information Forensics and Security*, 2022, 17: 2771–2783. doi: 10.1109/TIFS.2022.3192716.

[6] TSUNODA T, NIMURA K, YAMAMOTO D, *et al*. A chameleon hash-based method for proving execution of business processes[J]. *Journal of Information Processing*, 2022, 30: 613–625. doi: 10.2197/ipsjjip.30.613.

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

[8] 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.

[9] 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.

[10] 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.

[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, French Riviera, France, 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] 张彦华, 陈岩, 刘西蒙, 等. 格上基于身份的变色龙签名方案[J]. 电子与信息学报, 2024, 46(2): 757–764. doi: 10.11999/JEIT230155.

ZHANG Yanhua, CHEN Yan, LIU Ximeng, *et al*. Identity-based chameleon signature schemes over lattices[J]. *Journal of Electronics & Information Technology*, 2024, 46(2): 757–764. doi: 10.11999/JEIT230155.

[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] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]. The 37th Annual ACM Symposium on Theory of Computing, Baltimore, USA, 2005: 84–93. doi: 10.1145/1060590.1060603.

[19] 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.

[20] 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.

张彦华：男，讲师，研究方向为格公钥密码学、隐私保护、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：余 蓉