基于无证书的格基代理签密方案

俞惠芳* 王 宁
(西安邮电大学网络空间安全学院 西安 710121)

摘 要：无证书代理签密在信息安全领域发挥着越来越重要的作用。现有的大多数无证书代理签密基于传统数学理论，无法抵制量子计算攻击。该文采用格密码技术提出基于无证书的格基代理签密(L-CLPSC)方案。L-CLPSC在带错误学习(LWE)问题和小整数解(SIS)问题的困难假设下满足自适应选择密文攻击下的不可区分性和自适应选择消息攻击下的不可伪造性。相比较而言，L-CLPSC具有更高的计算效率和更低的通信代价。

关键词：格密码；无证书代理签密；小整数解问题；带错误学习问题
中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2022)07-2584-08
DOI: 10.11999/JEIT210300

Certificateless Proxy Signcryption Scheme from Lattice

YU Huifang WANG Ning
(*School of Cyberspace*, *Xi'an University of Posts & Telecommunications*, *Xi'an* 710121, *China*)

Abstract: Certificateless proxy signcryption plays an increasingly significant role in information security fields. Most of certificateless proxy signcryption schemes are based on traditional mathematic theory and can not resist the quantum computing attacks. In this paper, a new CertificateLess Proxy SignCryption from Lattice (L-CLPSC) is proposed by using lattice-based cryptography technology. L-CLPSC is indistinguishable against adaptive chosen-ciphertext attacks and unforgeable against adaptive chosen-message attacks under Learning With Errors (LWE) and Small Integer Solution (SIS) assumptions. Comparison shows L-CLPSC has higher computation efficiency and lower communication overhead.

Key words: Lattice-based cryptography; Certificateless proxy signcryption; Small Integer Solution (SIS) problem; Learning With Errors (LWE) problem

1 引言

用户之间的相互认证在互联网时代不可或缺，认证过程中提高认证性尤为重要。现代密码体系中数字签名是实现用户之间认证的必要技术。如今，数字签名广泛用在电子商务、电子政务、在线管理等领域中。传统公钥密码体系需要证书来验证用户的身份，涉及大量的证书管理问题。身份密码体制[1]简化了证书管理过程，用户选取身份信息作为公钥，可信中心生成相应的私钥，可信中心掌握所有用户私钥，难免密钥托管的问题。无证书密码体制[2]中用户完整私钥含来自可信中心的部分密钥和自己选取的秘密值，用户计算得到自己的公钥。无证书代理签密[3]可使原始签密者对代理者授权，代理者代替原始签密者签密消息，接收者验证密文有效性和确定密文是代理者得到授权后的密文，代理者产生的密文和原始签密者产生的密文是可区分的。

量子算法[4]减少了RSA密码体制、ElGamal密码体制的破解时间。这说明建立在经典数论上的许多传统公钥密码不能抗量子计算的攻击，抗量子计算的格密码应运而生。格代数运算通常都是矩阵之间的加法运算或矩阵与向量的乘法运算，比起双线性对代数运算、模指数运算，这类线性运算更为简单，效率更高。格中计算问题至今都未被量子算法破解，这意味着格公钥密码体制有着较高的安全性，格密码方案研究[5–10]是信息安全领域的热点。

夏峰等人[6]提出安全高效的格代理签名方案。江明明等人[7]提出的格代理签名方案通过减小代理签名的私钥的维数降低代理签名私钥的尺寸，计算复杂度低。陈虎等人[8]提出格上无证书加密方案，并形式化证明自适应选择身份攻击下密文是不可区分的。路秀华等人[9]提出无陷门格基签密方案。欧海文等人[10]提出公私钥与签名长度较小的格上身份

收稿日期：2021-04-13；改回日期：2022-03-27；网络出版：2022-04-22
*通信作者： 俞惠芳 yuhuifang@xupt.edu.cn
基金项目：陕西省自然科学基金基础研究计划重点项目(2020JZ-54)
Foundation Item: The Key Project of Basic Research Program of Natural Science Foundation of Shannxi Province (2020JZ-54)

代理签名方案。目前还没有抗量子计算的格上无证书代理签密方案。

本文提出基于无证书的格基代理签密(CertificateLess Proxy SignCryption from Lattice, L-CLPSC)方案，用户公钥不需要管理，也无需密钥的托管。L-CLPSC的安全性依赖于小整数解问题和带错误学习问题的难解性。L-CLPSC运算复杂度低，具有抗量子计算攻击的特性。

2　基础知识

2.1　格理论

令$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\in\mathbb{Z}^m$是$m$个线性无关的向量，格$\Lambda$定义为所有这些向量的整系数线性组合，其中向量组$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\in\mathbb{Z}^m$是格$\Lambda$的一组基

$$\Lambda=\left\{y\in\mathbb{Z}^m|\boldsymbol{y}=\sum_{i=1}^{m}\boldsymbol{c}\boldsymbol{b}_i,\boldsymbol{c}\in\mathbb{Z}^m\right\}\tag{1}$$

定义1　给定整数q，矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，向量$\boldsymbol{u}\in\mathbb{Z}_q^n$，$\mathbb{Z}_q^{n\times m}$是$n$行$m$列的模$q$剩余类矩阵环，$q$模格定义为

$$\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{e}=0\bmod q\}\tag{2}$$

$$\Lambda_m^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{e}=\boldsymbol{u}\bmod q\}\tag{3}$$

2.2　困难问题

定义2　给定正整数q，矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，正整数$\beta$，小整数解问题是指找到一个非零向量$\boldsymbol{e}\in\Lambda_q^{\perp}(\boldsymbol{A})$，满足$Ae=0\bmod q$，其中$\|\boldsymbol{e}\|\le\beta$。

定义3　给定正整数$n\ge1$，$\mathbb{Z}_q^m$上高斯噪声分布χ，模数$q\ge2$。矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和向量$\boldsymbol{s}\in\mathbb{Z}_q^n$是随机均匀选取的，从高斯噪声分布$\chi$随机抽取得到噪声向量$\boldsymbol{e}\in\mathbb{Z}_q^m$，输出样本$(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e})$，区分得到的每一个样本$(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e})$，主要是区分样本是从分布$A_{s,\chi}$随机选取的，还是从$\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m$的均匀分布上随机选取的。

2.3　高斯分布

令$\Lambda\in\mathbb{R}^m$是一个格，在线性空间$\mathbb{R}^m$中，以向量$\boldsymbol{c}\in\mathbb{R}^m$为中心，实参数$s>0$，$n$维格$\Lambda$的离散高斯分布定义为

$$D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)}=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\sum\limits_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})},\forall\boldsymbol{x}\in\mathbb{R}^n\tag{4}$$

2.4　重要算法

陷门生成算法[11]：输入整数n，给定素数$q\ge3$和整数$m\ge5n\log_2 q$，多项式时间内输出服从均匀的矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和格$\Lambda_q^{\perp}(\boldsymbol{A})$上的短基$\boldsymbol{B}\in\mathbb{Z}_q^{m\times m}$，其中$\boldsymbol{A}\boldsymbol{B}=0\bmod q$，$\|\boldsymbol{B}\|\le\tilde{O}(\sqrt{n\log_2 q})$。利用陷门生成算法TrapGen($n$,$m$,$q$)输出单向陷门后，通过调用高斯抽样算法、原像取样算法和一般原像取样算法等函数可得到该单向陷门函数解的范数较小的原像。

一般原像取样算法：输入陷门生成算法TrapGen(n,m,q)输出的矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和短基$\boldsymbol{B}\in\mathbb{Z}_q^{m\times m}$，安全高斯参数$s\ge\|\boldsymbol{B}\|\cdot\omega(\sqrt{\log_2 n})$和任意服从均匀分布的随机矩阵$\boldsymbol{U}\in\mathbb{Z}_q^{n\times k}$，一般原像取样算法SampleMat($\boldsymbol{A}$,$\boldsymbol{B}$,$s$,$\boldsymbol{U}$)在多项式时间内输出服从高斯分布$D_{\Lambda_q^{\boldsymbol{U}}(A),s}^m$的随机矩阵$\boldsymbol{S}\in\mathbb{Z}_q^{m\times k}$，其中$\boldsymbol{A}\boldsymbol{S}=\boldsymbol{U}\bmod q$。

2.5　无抽样技术

引理1[12]　$\mathbb{R}^m$上的离散高斯分布D_σ^m上，对于$\sigma>0$，$\boldsymbol{x}\in\mathbb{R}^m$，有

$$\Pr\left[x\leftarrow D_\sigma^m:\|x\|>2\sigma\sqrt{m}\right]<2^{-m}\tag{5}$$

$$\Pr\left[x\leftarrow D_\sigma^1:\|x\|>12\sigma\right]<2^{-100}\tag{6}$$

在上述引理的基础上根据文献[13]可得结论($\boldsymbol{c}\in\mathbb{Z}^m$，$\sigma=\omega(\|\boldsymbol{c}\|\sqrt{\log_2 m})$)

$$\Pr\left[x\leftarrow D_\sigma^m|\frac{D_\sigma^m(x)}{D_{\sigma,c}^m(x)}=O(1)\right]=1-2^{-\omega(\log_2 m)}\tag{7}$$

3　L-CLPSC方案实例

3.1　设置系统参数

密钥生成中心(KGC)选取安全参数1^n、素数$q\ge3$、复杂度函数$L=O(\sqrt{n\log_2 q})$、正整数m,d,k、实数$\sigma=12dk\sqrt{m})$、高斯参数$s=L\cdot\omega(\sqrt{\log_2 n})$，$m>5n\log_2 q$。$D_\sigma$是均值为0、标准差为$\sigma$的高斯分布。$(E_\kappa(\cdot),D_\kappa(\cdot))$是一对安全加解密算法，$\kappa$是来自密钥空间$\Sigma$的对称密钥。KGC运行TrapGen$(n,m,q)$，输出一个服从随机均匀分布的矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和格$\Lambda^{\perp}(\boldsymbol{A})$的一组基$\boldsymbol{B}\in\mathbb{Z}_q^{m\times m}$，$\|\boldsymbol{B}\|\le\tilde{O}(\sqrt{n\log_2 q})$，$\boldsymbol{A}\boldsymbol{B}=0\bmod q$；然后选取满足条件的哈希函数($\Pi$为多次掷币空间)：

$$H_1:\{0,1\}^*\to\mathbb{Z}_q^{n\times k}$$

$$H_2:\{0,1\}^*\to\{\boldsymbol{c}:\boldsymbol{c}\in\{-1,0,1\}^k\}$$

$$H_3:\{0,1\}^k\to\Sigma$$

$$H_4:\{0,1\}^*\times\{0,1\}^*\to\Pi$$

最后，KGC保密系统的主私钥$\mathrm{sk}=\boldsymbol{B}$，公布系统的全局参数：

$$\tilde{p}=\{\boldsymbol{A},H_1,H_2,H_3,H_4,q,m,d,k,\sigma,s\}$$

3.2　提取部分私钥

KGC计算$\boldsymbol{F}_i=H_1(\mathrm{id}_i)$，然后运行SampleMat($\boldsymbol{A}$,$\boldsymbol{B}$,$s$,$\boldsymbol{F}_i$)输出矩阵$\boldsymbol{D}_i\in\mathbb{Z}^{m\times k}$，$\boldsymbol{A}\boldsymbol{D}_i=\boldsymbol{F}_i$，

$\|D_i\| \le s\sqrt{m}$。然后发送部分密钥D_i给用户id_i，其中id_A表示原始签密人的身份，id_B表示代理者的身份，id_R表示接收者的身份。

3.3 生成用户密钥

(1)用户id_i从$\{-d,\cdots,0,\cdots,d\}^{m\times k}$中选取一个服从均匀分布的矩阵$\boldsymbol{C}_i$作为其秘密值，$\|C_i\| \le d\sqrt{m}$；

(2)用户id_i利用部分密钥和秘密值计算公钥$\boldsymbol{T}_i = \boldsymbol{A}\boldsymbol{C}_i(\mathrm{mod}\ q) \in \mathbb{Z}^{n\times k}$，然后计算私钥$\boldsymbol{S}_i = \boldsymbol{C}_i + \boldsymbol{D}_i \in \mathbb{Z}^{m\times k}$，$\|S_i\| \le (s+d)\sqrt{m}$，$(T_i, S_i)$是用户$\mathrm{id}_i$的公私钥对。

(3)原始签密者、代理者和接收者的公私钥对分别是$(\boldsymbol{T}_\mathrm{A}, \boldsymbol{S}_\mathrm{A})$, $(\boldsymbol{T}_\mathrm{B}, \boldsymbol{S}_\mathrm{B})$和$(\boldsymbol{T}_\mathrm{R}, \boldsymbol{S}_\mathrm{R})$。

3.4 代理授权

(1)原始签密者根据需求生成授权证书m_ω(含原始签密者信息、代理者信息、授权的范围、授权的有效期限)，然后计算$\boldsymbol{x} = H_2(\boldsymbol{A}\boldsymbol{y}_1, m_w)$，$\boldsymbol{z}_1 = \boldsymbol{S}_A\boldsymbol{x} + \boldsymbol{y}_1$，$\boldsymbol{y}_1$是高斯分布$D_\sigma^m$上选取的一个向量；

(2)原始签密者发送m_ω给代理者，如果$\|z_1\| \le 2\sigma\sqrt{m}$，代理签密者计算：$\boldsymbol{x'} = H_2(\boldsymbol{A}\boldsymbol{z}_1 - (H_1(\mathrm{id}_\mathrm{A}) + \boldsymbol{T}_\mathrm{A})\boldsymbol{x}, m_w)$。如果$\boldsymbol{x'} = \boldsymbol{x}$成立，代理者计算代理签密密钥$\boldsymbol{S}_\mathrm{P} = \boldsymbol{S}_\mathrm{B} + \boldsymbol{D}_\mathrm{A}$；否则，要求重发。

3.5 代理签密

代理者在代理签密算法中的操作如下。

(1)在高斯分布D_σ^m上选取向量$\boldsymbol{y}_2$；

(2)计算$\boldsymbol{c} = H_2(\boldsymbol{A}\boldsymbol{y}_2, m')$，$\boldsymbol{z}_2 = \boldsymbol{S}_\mathrm{P}\boldsymbol{c} + \boldsymbol{y}_2$；以$\min\left\{\dfrac{D_\sigma^m(\boldsymbol{z}_2)}{MD^m_{\boldsymbol{c}\boldsymbol{S}_P,\sigma}(\boldsymbol{z}_2)}, 1\right\}$的概率输出$(\boldsymbol{z}_2, \boldsymbol{c})$；

(3)随机选取$\tau \in \{0,1\}^k$，计算$\boldsymbol{\mu} = E_{\kappa=H_3(\tau)}(m', \boldsymbol{z}_2, \boldsymbol{c})$；

(4)计算$\eta = H_4(\tau, \boldsymbol{\mu})$，由$\eta$的随机性可得：$\boldsymbol{v}_1^\mathrm{T} = -\boldsymbol{e}_1^\mathrm{T}\boldsymbol{A} + \boldsymbol{e}_2^\mathrm{T}$，噪声向量$\boldsymbol{e}_1 \leftarrow D_\sigma^n$，$\boldsymbol{v}_2^\mathrm{T} = \boldsymbol{e}_1^\mathrm{T}\boldsymbol{T}_R + \boldsymbol{e}_3^\mathrm{T} + \tau\cdot\lfloor q/2\rfloor$，噪声向量$\boldsymbol{e}_2, \boldsymbol{e}_3 \leftarrow D_\sigma^m$；

(5)输出密文$\varpi = (\boldsymbol{\mu}, \boldsymbol{v}_1, \boldsymbol{v}_2)$。

3.6 解签密

接收者在解签密算法中的操作如下。

(1)计算$\hat{\tau} = \boldsymbol{v}_1^\mathrm{T}\boldsymbol{S}_\mathrm{R} + \boldsymbol{v}_2^\mathrm{T}$。令$\hat{\tau} = (\tau_1', \tau_2', \cdots, \tau_k')$，对$i = 1, 2, \cdots, k$，如果$\tau_i' \in (-\lfloor q/4\rfloor, \lfloor q/4\rfloor)$，$\tau_i = 0$；否则，$\tau_i = 1$。$\tau = (\tau_1, \tau_2, \cdots, \tau_k)$。

(2)计算$D_{\kappa\leftarrow H_3(\tau)}(\boldsymbol{\mu}) = (m', \boldsymbol{z}_2, \boldsymbol{c})$。

(3)如果$\|z_2\| \le 2\sigma\sqrt{m}$，执行步骤(4)；否则，终止。

(4)计算：

$$\boldsymbol{c'} = H_2(\boldsymbol{A}\boldsymbol{z}_2 - (\boldsymbol{T}_B + H_1(\mathrm{id}_\mathrm{B}) + H_1(\mathrm{id}_\mathrm{A}))\boldsymbol{c}, m')$$

(5)如果$\boldsymbol{c'} = \boldsymbol{c}$，接受明文$m'$；否则，输出符号$\perp$。

3.7 代理授权阶段的正确性

$$\begin{aligned}&\boldsymbol{A}\boldsymbol{z}_1 - (H_1(\mathrm{id}_\mathrm{A}) + \boldsymbol{T}_\mathrm{A})\boldsymbol{x}\\ &= \boldsymbol{A}(\boldsymbol{S}_\mathrm{A}\boldsymbol{x} + \boldsymbol{y}_1) - (H_1(\mathrm{id}_\mathrm{A}) + \boldsymbol{T}_\mathrm{A})\boldsymbol{x}\\ &= \boldsymbol{A}\boldsymbol{S}_\mathrm{A}\boldsymbol{x} + \boldsymbol{A}\boldsymbol{y}_1 - \boldsymbol{A}(\boldsymbol{C}_\mathrm{A} + \boldsymbol{D}_\mathrm{A})\boldsymbol{x}\\ &= \boldsymbol{A}\boldsymbol{y}_1\end{aligned}$$

$$H_2(\boldsymbol{A}\boldsymbol{y}_1, m_\omega) = H_2(\boldsymbol{A}\boldsymbol{z}_1 - (H_1(\mathrm{id}_\mathrm{A}) + \boldsymbol{T}_\mathrm{A})\boldsymbol{x}, m_\omega)$$

3.8 解签密阶段的正确性

$$\begin{aligned}\hat{\tau} &= \boldsymbol{v}_1^\mathrm{T}\boldsymbol{S}_R + \boldsymbol{v}_2^\mathrm{T}\\ &= (-\boldsymbol{e}_1^\mathrm{T}\boldsymbol{A} + \boldsymbol{e}_2^\mathrm{T})\boldsymbol{S}_R + \boldsymbol{e}_1^\mathrm{T}\boldsymbol{T}_R + \boldsymbol{e}_3^\mathrm{T} + \tau\cdot\lfloor q/2\rfloor\\ &= -\boldsymbol{e}_1^\mathrm{T}\boldsymbol{A}\boldsymbol{S}_R + \boldsymbol{e}_2^\mathrm{T}\boldsymbol{S}_R + \boldsymbol{e}_1^\mathrm{T}\boldsymbol{T}_R + \boldsymbol{e}_3^\mathrm{T} + \tau\cdot\lfloor q/2\rfloor\\ &= \boldsymbol{e}_2^\mathrm{T}\boldsymbol{S}_R - \boldsymbol{e}_1^\mathrm{T}\boldsymbol{F}_R + \boldsymbol{e}_3^\mathrm{T} + \tau\cdot\lfloor q/2\rfloor\end{aligned}$$

$\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$分量都取自高斯分布$D_\sigma$，如果$m'$，$\tau_i = 0$；否则，$\tau_i = 1$。由此可还原$\tau$。下面验证解签密中的等式是成立的。

$$\begin{aligned}&\boldsymbol{A}\boldsymbol{z}_2 - (\boldsymbol{T}_\mathrm{B} + H_1(\mathrm{id}_\mathrm{B}) + H_1(\mathrm{id}_\mathrm{A}))\boldsymbol{c}\\ &= \boldsymbol{A}(\boldsymbol{S}_\mathrm{P}\boldsymbol{c} + \boldsymbol{y}_2) - (\boldsymbol{T}_\mathrm{B} + H_1(\mathrm{id}_\mathrm{B}) + H_1(\mathrm{id}_\mathrm{A}))\boldsymbol{c}\\ &= \boldsymbol{A}\boldsymbol{S}_\mathrm{P}\mathrm{c} - (\boldsymbol{T}_\mathrm{B} + H_1(\mathrm{id}_\mathrm{B}) + H_1(\mathrm{id}_\mathrm{A}))\boldsymbol{c} + \boldsymbol{A}\boldsymbol{y}_2\\ &= \boldsymbol{A}\boldsymbol{y}_2\end{aligned}$$

$$\begin{aligned}&H_2(\boldsymbol{A}\boldsymbol{z}_2 - (\boldsymbol{T}_\mathrm{B} + H_1(\mathrm{id}_\mathrm{B}) + H_1(\mathrm{id}_\mathrm{A}))\boldsymbol{c}, m')\\ &= H_2(\boldsymbol{A}\boldsymbol{y}_2, m')\end{aligned}$$

4 安全性证明

定义4 给出若干$(\boldsymbol{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$，判定型LWE问题判定$b$属于下列哪种情况：(1)服从均匀分布；(2)$b = \langle\boldsymbol{a}, \boldsymbol{s}\rangle + e$，$\boldsymbol{s}$服从高斯分布$D_\sigma^n$，$e$服从高斯分布$D_\sigma$。

定理1 如果敌手A_1能以优势ε攻破L-CLPSC的IND-CCA2-Ⅰ安全性，则存在算法C能以优势$\varepsilon' \ge \varepsilon/eq_2(q_\mathrm{usc}+q_\mathrm{r}+q_\mathrm{p})$解决判定LWE问题，其中$q_2$是询问$H_2$的次数，$q_r$是公钥替换次数，$q_p$是代理密钥询问次数，$q_\mathrm{usc}$是解签密询问的次数。

证明 给定判定LWE问题的一个随机实例，C判断$\boldsymbol{T}^*$是定义4中的情况(1)还是情况(2)。游戏中A_1充当挑战者C的子程序。C使用起初为空的6张列表list1～list6追踪不同谕言机询问。C选取$t \in \{1, 2, \cdots, q_1\}$，$q_1$是询问$H_1$的次数，$\mathrm{id}_t$是挑战身份，$\gamma$是$\mathrm{id}_i = \mathrm{id}_t$时的概率。

游戏开始时，C运行设置算法生成系统参数$\tilde{p}$，返回$\tilde{p}$给A_1。在阶段1，A_1在适应性条件下向C提交多项式有界次询问。

H_1询问：A_1希望得到身份id_i的哈希值。如果list1中含有$(\mathrm{id}_i, \boldsymbol{F}_i)$，C返回$\boldsymbol{F}_i \leftarrow H_1(\mathrm{id}_i)$给$\mathrm{A}_1$；否则，C返回在$\mathbb{Z}_q^{n\times k}$中随机抽取的$\boldsymbol{F}_i$给$\mathrm{A}_1$，添加$(\mathrm{id}_i, \boldsymbol{F}_i)$到list1中。

H_2询问：A_1希望得到$(\boldsymbol{A}, \boldsymbol{y}_i, m', -, -)$的哈希

值。如果list2中已有$(\boldsymbol{A},\boldsymbol{y}_i,m',\boldsymbol{z}_i,\boldsymbol{c}_i)$，C返回$(\boldsymbol{z}_i,\boldsymbol{c}_i)$给$\mathrm{A}_1$；否则，C从高斯分布$D_\sigma^m$抽取$\boldsymbol{z}_i$,$\boldsymbol{y}_i$，选取$\boldsymbol{c}_i\in\mathbb{Z}^k$，然后返回$(\boldsymbol{z}_i,\boldsymbol{c}_i)$给$\mathrm{A}_1$，添加$(\boldsymbol{A},\boldsymbol{y}_i,m',\boldsymbol{z}_i,\boldsymbol{c}_i)$到list2中。

H_3询问：C收到H_3询问时，检查list3中是否含有$(\tau,H_3(\tau))$。如果有，C返回κ给A_1；否则，C随机抽取$H_3(\tau)\leftarrow\Sigma$，返回$\kappa\leftarrow H_3(\tau)$给$\mathrm{A}_1$，添加$(\tau,H_3(\tau))$到list3中。

H_4询问：C收到H_4询问时，检查元组list4中是否含有$(\tau,\boldsymbol{\mu},\eta\leftarrow H_4(\tau,\boldsymbol{\mu}))$。如果有，C返回$\eta$给$\mathrm{A}_1$；否则，C随机抽取$H_4(\tau,\boldsymbol{\mu})\leftarrow\Pi$，返回$\eta\leftarrow H_4(\tau,\boldsymbol{\mu})$，添加$(\tau,\boldsymbol{\mu},\eta\leftarrow H_4(\tau,\boldsymbol{\mu}))$到list4中。

公钥询问：A_1询问身份id_i的公钥。C查询list5中是否含有公钥$\boldsymbol{T}_i$，如果有，C发送公钥$\boldsymbol{T}_i$给A_1；否则，C从$\{-d,\cdots,0,\cdots,d\}^{m\times k}$中选取服从随机均匀分布的矩阵$\boldsymbol{C}_i$，返回$\boldsymbol{T}_i=\boldsymbol{A}\boldsymbol{C}_i(\mathrm{mod}\ q)$，添加$(\mathrm{id}_i,\boldsymbol{C}_i,\boldsymbol{T}_i,-,-)$到list5中。

部分私取询问：A_1询问id_i的部分私钥时，如果$\mathrm{id}_i=\mathrm{id}_t$，C放弃游戏；否则，C随机选择$\boldsymbol{D}_i\in\mathbb{Z}^{m\times k}$，返回$\boldsymbol{D}_i$给$\mathrm{A}_1$，使用$(\mathrm{id}_i,\boldsymbol{C}_i,\boldsymbol{D}_i,\boldsymbol{T}_i,-)$更新list5。

私钥询问：A_1询问id_i的私钥时，如果$\mathrm{id}_i=\mathrm{id}_t$，C放弃游戏；否则，C从list5中获得$(\boldsymbol{T}_i,\boldsymbol{D}_i,\boldsymbol{S}_i)$，使用$(\mathrm{id}_i,\boldsymbol{C}_i,\boldsymbol{D}_i,\boldsymbol{T}_i,\boldsymbol{S}_i)$更新list5，返回$\boldsymbol{S}_i=\boldsymbol{C}_i+\boldsymbol{D}_i$给$\mathrm{A}_1$。

公钥替换：A_1选取随机数$\boldsymbol{T'}_i$替换身份id_i的公钥T_i。如果$\mathrm{id}_i=\mathrm{id}_t$，C放弃游戏；否则，用$(\mathrm{id}_i,\boldsymbol{C}_i,\boldsymbol{D}_i,\boldsymbol{T'}_i,-)$替换list5中的$(\mathrm{id}_i,\boldsymbol{C}_i,\boldsymbol{D}_i,\boldsymbol{T}_i,\boldsymbol{S}_i)$。

代理密钥询问：A_1询问$(\mathrm{id}_\mathrm{A},\mathrm{id}_\mathrm{B},\boldsymbol{m}_w)$的代理密钥。如果$\mathrm{id}_\mathrm{A}=\mathrm{id}_t$，C失败；否则，C计算$\boldsymbol{x'}=H_2(\boldsymbol{A}\boldsymbol{z}_2-(H_1(\mathrm{id}_A)+\boldsymbol{T}_A)\boldsymbol{x},m_\omega)$，如果$\boldsymbol{x'}=\boldsymbol{x}$，C计算$\boldsymbol{S}_\mathrm{P}$，返回代理密钥$\boldsymbol{S}_\mathrm{P}$给$\mathrm{A}_1$，添加$(x,S_\mathrm{P},m_\omega)$到list6中。

签密询问：A_1询问$(m',\mathrm{id}_\mathrm{B},\mathrm{id}_\mathrm{R},m_\omega)$的密文。如果$\mathrm{id}_\mathrm{B}\neq\mathrm{id}_t$，C运行签密算法返回密文$\varpi$给$\mathrm{A}_1$。否则，C从list5中检索到$(\boldsymbol{S}_\mathrm{P},\boldsymbol{T}_\mathrm{R})$，反应如下：

(1)随机在高斯分布D_σ^m上选取向量$\boldsymbol{y}_2$；

(2)计算$\boldsymbol{c}=H_2(\boldsymbol{A}\boldsymbol{y}_2,m')$，$\boldsymbol{z}_2=\boldsymbol{S}_\mathrm{P}\boldsymbol{c}+\boldsymbol{y}_2$；

(3)随机选取$\tau\in\{0,1\}^k$，计算$\boldsymbol{\mu}=E_{\kappa=H_3(\tau)}(m',\boldsymbol{z}_2,\boldsymbol{c})$；

(4)令$\eta=H_4(\tau,\mu)$，由η的随机性可得：$\boldsymbol{v}_1^\mathrm{T}=-\boldsymbol{e}_1^\mathrm{T}\boldsymbol{A}+\boldsymbol{e}_2^\mathrm{T}$，噪声向量$\boldsymbol{e}_1\leftarrow D_\sigma^n$，$\boldsymbol{v}_2^\mathrm{T}=\boldsymbol{e}_1^\mathrm{T}\boldsymbol{T}_R^*+\boldsymbol{e}_3^\mathrm{T}+\tau\cdot\lfloor q/2\rfloor$，噪声向量$\boldsymbol{e}_2,\boldsymbol{e}_3\leftarrow D_\sigma^m$。

(5)返回密文$\varpi=(\boldsymbol{\mu},\boldsymbol{v}_1,\boldsymbol{v}_2)$给$\mathrm{A}_1$。

解签密询问：A_1询问$(\mathrm{id}_\mathrm{B},\mathrm{id}_\mathrm{R},\varpi,m_\omega)$的解签密结果。如果$\mathrm{id}_\mathrm{R}\neq\mathrm{id}_t$，C运行解签密算法返回一个结果。否则，C应答如下：

(1)$\hat{\tau}=\boldsymbol{v}_1^\mathrm{T}\boldsymbol{S}_R+\boldsymbol{v}_2^\mathrm{T}$，设$\hat{\tau}=(\tau_1',\tau_2',\cdots,\tau_k')$对$i=1,2,\cdots,k$，如果$\tau_i'\in(-\lfloor q/4\rfloor,\lfloor q/4\rfloor)$，$\tau_i=0$；否则，$\tau_i=1$。则$\tau=(\tau_1,\tau_2,\cdots,\tau_k)$。

(2)计算$D_{\kappa\leftarrow H_3(\tau)}(\boldsymbol{\mu})=(m',\boldsymbol{z}_2,\boldsymbol{c})$；

(3)如果$\|z_2\|\le2\sigma\sqrt{m}$，执行步骤(4)，否则，终止；

(4)通过调用H_2谕言机获得c，如果$\boldsymbol{c'}=H_2(\boldsymbol{A}\boldsymbol{z}_2-(\boldsymbol{T}_B+H_1(\mathrm{id}_\mathrm{B})+H_1(\mathrm{id}_\mathrm{A}))\boldsymbol{c},m')$，接受明文$m'$；否则，输出符号$\perp$。

接下来，A_1输出m_ω,m_b',$(\mathrm{id}_\mathrm{B}^*,\mathrm{id}_\mathrm{R}^*)$给C，$b\in(0,1)$。挑战前，$\mathrm{A}_1$不能询问$\mathrm{id}_\mathrm{R}^*$的私钥，$\mathrm{id}_\mathrm{R}^*$的公钥不能替换且其部分私钥不能提取。如果$\mathrm{id}_\mathrm{R}^*\neq\mathrm{id}_t$，C放弃游戏；否则，C回应如下：

(1)随机在高斯分布D_σ^m上抽取向量$\boldsymbol{y}_2^*$；

(2) $\boldsymbol{c}=H_2(\boldsymbol{A}\boldsymbol{y}_2^*,m_b')$,$z_2^*=\boldsymbol{S}_\mathrm{P}^*\boldsymbol{c}^*+\boldsymbol{y}_2^*$；

(3)随机选取$\tau\in\{0,1\}^k$，并且计算$\boldsymbol{\mu}=E_{\kappa=H_3(\tau)}(m',\boldsymbol{z}_2,\boldsymbol{c})$；

(4)令$\eta=H_4(\tau,\mu)$，由η的随机性可知，$\boldsymbol{v}_1^\mathrm{T}=-\boldsymbol{e}_1^\mathrm{T}\boldsymbol{A}+\boldsymbol{e}_2^\mathrm{T}$，噪声向量$\boldsymbol{e}_1\leftarrow D_\sigma^n$，$\boldsymbol{v}_2^\mathrm{T}=\boldsymbol{e}_1^\mathrm{T}\boldsymbol{T}_R+\boldsymbol{e}_3^\mathrm{T}+\tau\cdot\lfloor q/2\rfloor$，噪声向量$\boldsymbol{e}_2,\boldsymbol{e}_3\leftarrow D_\sigma^m$。

(5)输出挑战密文$\varpi^*=(\boldsymbol{\mu}^*,\boldsymbol{v}_1^*,\boldsymbol{v}_2^*)$给$\mathrm{A}_1$。

A_1再次发出多项式有界次询问。挑战前，A_1不能提取id_R^*的私钥和部分私钥，id_R^*的公钥不能替换；挑战后，A_1不能针对挑战密文ϖ^*询问解签密谕言机。

最后，A_1输出对b的猜测b'给C。如果$b=b'$，C获知$\boldsymbol{S}^*\in\mathbb{Z}^{m\times k}$和$\boldsymbol{F}^*\in\mathbb{Z}^{n\times k}$，$\boldsymbol{S}^*$和$\boldsymbol{F}^*$的所有分量不超过$7\sigma$，使公钥满足$\boldsymbol{T}^*=\boldsymbol{A}\boldsymbol{S}^*-\boldsymbol{F}^*(\mathrm{mod}q)$。否则，C获知$\boldsymbol{T}^*$服从均匀分布。这说明判定型LWE问题实例获得求解。

在游戏中，C解决判定型LWE问题的概率$\varepsilon'\ge\varepsilon/q_2e(q_\mathrm{usc}+q_\mathrm{r}+q_\mathrm{p})$[14]。　　证毕

定理2　如果敌手A_2(知道系统主私钥但不能修改用户公钥)以优势ε攻破L-CLPSC的IND-CCA2-II安全性，则存在算法C能以优势$\varepsilon'\ge\varepsilon/eq_2(q_\mathrm{usc}+q_\mathrm{p})$解决判定型LWE问题。

证明　挑战者C收到判定LWE问题的随机实例，判定$\boldsymbol{T}^*$是定义4中的情况(1)还是情况(2)。在游戏中A_2扮演C的子程序。list1～list6的情况和**定理1**相同。C选取$t\in\{1,2,\cdots,q_1\}$，q_1是询问H_1的次数，id_t是挑战身份，γ是$\mathrm{id}_i=\mathrm{id}_t$时的概率。

游戏开始时，C运行设置算法生成系统参数$\tilde{p}$和主私钥sk，输出$(\tilde{p},\mathrm{sk})$给A_2。然后，在适应性条件下A_2向C提交多项式有界次询问。H_1～H_4的询问与**定理1**第1阶段完全相同。

公钥询问：A_2询问id_i的公钥。C从$\{-d,$

$\cdots,0,\cdots,d\}^{m\times k}$中选取服从随机均匀分布的矩阵$\boldsymbol{C}_i$，计算$\boldsymbol{T}_i=\boldsymbol{A}\boldsymbol{C}_i(\mathrm{mod}q)$，添加$(\mathrm{id}_i,\boldsymbol{C}_i,\boldsymbol{T}_i,-,-)$到list5中，返回公钥$\boldsymbol{T}_i$。

私钥询问：A_2询问id_i的私钥。如果$\mathrm{id}_i=\mathrm{id}_t$，C放弃游戏；否则，C计算部分私钥$\boldsymbol{D}_i$，查询列表list5计算$\boldsymbol{S}_i=\boldsymbol{C}_i+\boldsymbol{D}_i$，返回$(\boldsymbol{D}_i,\boldsymbol{C}_i,\boldsymbol{T}_i,\boldsymbol{S}_i)$，更新$(\mathrm{id}_i,\boldsymbol{D}_i,\boldsymbol{C}_i,\boldsymbol{T}_i,\boldsymbol{S}_i)$到list5中。

代理密钥询问：A_2询问$(\mathrm{id}_\mathrm{A},\mathrm{id}_\mathrm{B},m_\omega)$的代理密钥。如果$\mathrm{id}_\mathrm{A}=\mathrm{id}_t$，C放弃游戏；否则，计算$\boldsymbol{x}'=H_2(\boldsymbol{A}\boldsymbol{z}_2-(H_1(\mathrm{id}_\mathrm{A})+\boldsymbol{T}_\mathrm{A})\boldsymbol{x},m_\omega)$，如果$\boldsymbol{x}'=\boldsymbol{x}$，C计算代理密钥$\boldsymbol{S}_\mathrm{P}$，返回$\boldsymbol{S}_\mathrm{P}$给$\mathrm{A}_2$，添加$(x,\boldsymbol{S}_\mathrm{P},m_\omega)$到list6中。

签密询问：A_2询问$(m',\mathrm{id}_\mathrm{B},\mathrm{id}_\mathrm{R},m_\omega)$的密文。如果$\mathrm{id}_\mathrm{B}\neq\mathrm{id}_t$，C运行签密算法返回密文$\varpi$给$\mathrm{A}_2$；否则，C反应如下：

(1)随机在高斯分布D_σ^m上选取向量$\boldsymbol{y}_2$；

(2)计算$\boldsymbol{c}=H_2(\boldsymbol{A}\boldsymbol{y}_2,m')$，$\boldsymbol{z}_2=\boldsymbol{S}_\mathrm{P}\boldsymbol{c}+\boldsymbol{y}_2$；

(3)随机选取$\tau\in\{0,1\}^k$，计算$\mu=E_{\kappa=H_3(\tau)}(m',\boldsymbol{z}_2,\boldsymbol{c})$；

(4)令$\eta=H_4(\tau,\mu)$，由η的随机型可得：$\boldsymbol{v}_1^\mathrm{T}=-\boldsymbol{e}_1^\mathrm{T}\boldsymbol{A}+\boldsymbol{e}_2^\mathrm{T}$，噪声向量$\boldsymbol{e}_1\leftarrow D_\sigma^n$，$\boldsymbol{v}_2^\mathrm{T}=\boldsymbol{e}_1^\mathrm{T}\boldsymbol{T}_R+\boldsymbol{e}_3^\mathrm{T}+\tau\cdot\lfloor q/2\rfloor$，噪声向量$\boldsymbol{e}_2,\boldsymbol{e}_3\leftarrow D_\sigma^m$。

(5)返回密文$\varpi=(\mu,\boldsymbol{v}_1,\boldsymbol{v}_2)$给$\mathrm{A}_2$。

解签密询问：A_2询问$(\mathrm{id}_\mathrm{B},\mathrm{id}_\mathrm{R},\varpi,m_\omega)$的解签密结果。如果$\mathrm{id}_\mathrm{R}\neq\mathrm{id}_t$，C运行解签密算法返回结果；否则，C应答如下：

(1)计算$\hat{\tau}=\boldsymbol{v}_1^\mathrm{T}\boldsymbol{S}_\mathrm{R}+\boldsymbol{v}_2^\mathrm{T}$，令$\hat{\tau}=(\tau_1',\tau_2',\cdots,\tau_k')$，对$i=1,2,\cdots,k$，如果$\tau_i'\in(-\lfloor q/4\rfloor,\lfloor q/4\rfloor)$，$\tau_i=0$；否则，$\tau_i=1$。则$\tau=(\tau_1,\tau_2,\cdots,\tau_k)$。

(2)计算$D_{\kappa\leftarrow H_3(\tau)}(\boldsymbol{\mu})=(m',\boldsymbol{z}_2,\boldsymbol{c})$；

(3)如果$\|z_2\|\le2\sigma\sqrt{m}$，执行步骤(4)；否则，终止；

(4)通过调用H_2预言机获得c，如果$\boldsymbol{c}'=H_2(\boldsymbol{A}\boldsymbol{z}_2-(\boldsymbol{T}_\mathrm{B}+H_1(\mathrm{id}_\mathrm{B})+H_1(\mathrm{id}_\mathrm{A}))\boldsymbol{c},m')$，则接受明文；否则，输出符号$\perp$。

接下来，A_2输出m_b',$(\mathrm{id}_\mathrm{B}^*,\mathrm{id}_\mathrm{R}^*,m_\omega)$，$b\in(0,1)$。挑战前，$\mathrm{A}_2$不能询问$\mathrm{id}_\mathrm{R}^*$的私钥。如果$\mathrm{id}_\mathrm{R}^*=\mathrm{id}_t$，C放弃游戏；否则，C输出计算得到的挑战密文$\varpi^*=(\mu^*,\boldsymbol{v}_1^*,\boldsymbol{v}_2^*)$给$\mathrm{A}_2$。

A_2再次发出多项式有界次询问。挑战前，A_2不能提取id_R^*的私钥。挑战后，A_2不能针对密文ϖ^*询问解签密谕言机。

最后，A_2输出对b的猜测b'给C。如果$b=b'$，获知$\boldsymbol{S}^*\in\mathbb{Z}^{m\times k}$和$\boldsymbol{F}^*\in\mathbb{Z}^{n\times k}$，$\boldsymbol{S}^*$,$\boldsymbol{F}^*$的所有分量不超过$7\sigma$，使公钥满足$\boldsymbol{T}^*=\boldsymbol{A}\boldsymbol{S}^*-\boldsymbol{F}^*(\mathrm{mod}q)$。否则，C获知$\boldsymbol{T}^*$服从均匀分布。这说明判定型LWE问题实例获得求解。

在游戏中，C解决判定型LWE问题的概率是$\varepsilon'\ge\varepsilon/q_2e(q_\mathrm{usc}+q_\mathrm{p})$[14]。 证毕

定理3 如果敌手A_1能以优势ε攻破L-CLPSC的UF-CMA-Ⅰ安全性，则必存在算法C能以优势$\varepsilon'\leftarrow\varepsilon(1-2^{-\omega(\log_2n)})$解决小整数解(SIS)问题。

证明 给定SIS问题的随机实例，挑战者C可找到非零的短向量$\boldsymbol{e}'$和$\boldsymbol{e}''$使得$A\boldsymbol{e}'+\boldsymbol{e}''=0\ (\mathrm{mod}\ q)$。

游戏开始时，C运行设置算法生成系统的全局参数$\tilde{p}$，返回$\tilde{p}$给A_1。然后，A_1提交和**定理1**中第1阶段完全相同的询问。

最后，A_1输出针对消息m'^*的伪造密文ϖ^*，根据密文能伪造对任意消息m'^*的签名$(\boldsymbol{z}_2^*,\boldsymbol{c}^*)$。如果$\mathrm{id}_\mathrm{B}^*\neq\mathrm{id}_t$，C放弃游戏；否则，$\mathrm{A}_1$伪造出另一个密文$\varpi'$且计算得到对应的签名$(\boldsymbol{z'}_2,\boldsymbol{c}')$，使得$(\boldsymbol{c}^*\neq\boldsymbol{c}')$

$$\begin{aligned}&\boldsymbol{A}\boldsymbol{z}_2^*-(\boldsymbol{T}_\mathrm{B}^*+H_1(\mathrm{id}_\mathrm{B}^*)+H_1(\mathrm{id}_\mathrm{A}^*))\boldsymbol{c}^*\\&\quad=A\boldsymbol{z'}_2-(\boldsymbol{T}_\mathrm{B}^*+H_1(\mathrm{id}_\mathrm{B}^*)+H_1(\mathrm{id}_\mathrm{A}^*))c'\end{aligned}$$

已知$\boldsymbol{T}_\mathrm{B}^*=\boldsymbol{A}\boldsymbol{C}_\mathrm{B}^*(\mathrm{mod}q)$，$AD_i=H_1(\mathrm{id}_i)$，上式可化简为

$$\begin{aligned}&\boldsymbol{A}(\boldsymbol{z}_2^*-\boldsymbol{z'}_2+\boldsymbol{C}_\mathrm{B}^*(\boldsymbol{c}'-\boldsymbol{c}^*)\\&\quad+\boldsymbol{D}_\mathrm{B}^*(\boldsymbol{c}'-\boldsymbol{c}^*)+\boldsymbol{D}_\mathrm{A}^*(\boldsymbol{c}'-\boldsymbol{c}^*)=0\end{aligned}$$

根据分叉引理[13]可知，至少以$\varepsilon'\leftarrow\varepsilon(1-2^{-\omega(\log_2n)})$的概率存在另一个伪造部分密钥$\boldsymbol{D'}_\mathrm{B}$，使得$H_1(\mathrm{id}_\mathrm{B}^*)=\boldsymbol{A}\boldsymbol{D}_\mathrm{B}^*=\boldsymbol{A}\boldsymbol{D'}_\mathrm{B}$且$\boldsymbol{D}_\mathrm{B}^*\neq\boldsymbol{D'}_\mathrm{B}$。如果部分私钥$\boldsymbol{D}_\mathrm{B}^*$能使等式

$$\begin{aligned}&\boldsymbol{z}_2^*-\boldsymbol{z'}_2+\boldsymbol{C}_\mathrm{B}^*(\boldsymbol{c}'-\boldsymbol{c}^*)\\&\quad+\boldsymbol{D}_\mathrm{B}^*(\boldsymbol{c}'-\boldsymbol{c}^*)+\boldsymbol{D}_\mathrm{A}^*(\boldsymbol{c}'-\boldsymbol{c}^*)=0\end{aligned}$$

则另一个部分私钥$\boldsymbol{D}'_\mathrm{B}$一定能使等式

$$\begin{aligned}&\boldsymbol{z}_2^*-\boldsymbol{z'}_2+\boldsymbol{C}_\mathrm{B}^*(\boldsymbol{c}'-\boldsymbol{c}^*)\\&\quad+\boldsymbol{D'}_\mathrm{B}(\boldsymbol{c}'-\boldsymbol{c}^*)+\boldsymbol{D}_\mathrm{A}^*(\boldsymbol{c}'-\boldsymbol{c}^*)\neq0\end{aligned}$$

然后进一步化简上述等式可得$\boldsymbol{A}(\boldsymbol{z}_2^*-\boldsymbol{z'}_2+\boldsymbol{S}_\mathrm{B}^*(\boldsymbol{c}'-\boldsymbol{c}^*))+\boldsymbol{F}_\mathrm{A}^*(\boldsymbol{c}'-\boldsymbol{c}^*)=0$。SIS问题就是找到非零短向量$\boldsymbol{e}'$和$\boldsymbol{e}''$使得$A\boldsymbol{e}'+\boldsymbol{e}''=0(\mathrm{mod}q)$。由上式可得$e'=\boldsymbol{z}_2^*-\boldsymbol{z'}_2+\boldsymbol{S}_\mathrm{B}^*(\boldsymbol{c}'-\boldsymbol{c}^*)$，$e''=\boldsymbol{F}_\mathrm{A}^*(\boldsymbol{c}'-\boldsymbol{c}^*)$，已知$\|e'\|\neq0$，由于$\boldsymbol{S}_\mathrm{B}^*$,$\boldsymbol{F}_\mathrm{A}^*$不唯一，$\mathrm{A}_1$无法确定$\boldsymbol{S}_\mathrm{B}^*$,$\boldsymbol{F}_\mathrm{A}^*$和部分私钥。

因此，C解决小整数解(SIS)问题的优势$\varepsilon'\leftarrow\varepsilon(1-2^{-\omega(\log_2n)})$是可忽略的。 证毕

定理4 如果敌手A_2能以优势ε攻破L-CLPSC的UF-CMA-Ⅱ安全性，则必存在算法C能以优势$\varepsilon'\leftarrow\varepsilon(1-2^{-\omega(\log_2n)})$解决小整数解(SIS)问题。

证明 给定SIS问题的随机实例，挑战者C可找到非零的短向量$\boldsymbol{e}'$和$\boldsymbol{e}''$使得$A\boldsymbol{e}'+\boldsymbol{e}''=0\,\mathrm{mod}\,q$。

游戏开始时，C运行设置算法生成系统全局参数$\tilde{p}$和主私钥sk，返回$\tilde{p}$,sk给A_2。A_2提交和**定理2**第1阶段那样的询问。

最后，A_2输出消息m'^*的伪造密文ϖ^*，根据密文能伪造任意消息m'^*的签名$(\boldsymbol{z}_2^*, \boldsymbol{c}^*)$。如果$\mathrm{id}_B \neq id_t$，C放弃游戏；否则，$A_2$还可以伪造出对消息的另一个密文$\varpi'$，计算得到对应的$(\boldsymbol{z'}_2, \boldsymbol{c'})$，使得$(\boldsymbol{c}^* \neq \boldsymbol{c'})$

$$\begin{aligned}&\boldsymbol{A}\boldsymbol{z}_2^* - (\boldsymbol{T}_B^* + H_1(\mathrm{id}_B^*) + H_1(\mathrm{id}_A^*))\boldsymbol{c}^*\\&= A\boldsymbol{z'}_2 - (\boldsymbol{T}_B^* + H_1(\mathrm{id}_B^*) + H_1(\mathrm{id}_A^*))c'\end{aligned}$$

已知$\boldsymbol{T}_B^* = \boldsymbol{A}\boldsymbol{C}_B^* (\mathrm{mod}q)$，$AD_i = H_1(\mathrm{id}_i)$，化简上式可得

$$\begin{aligned}&\boldsymbol{A}(\boldsymbol{z}_2^* - \boldsymbol{z'}_2 + \boldsymbol{C}_B^*(\boldsymbol{c'} - \boldsymbol{c}^*)\\&+ \boldsymbol{D}_B^*(\boldsymbol{c'} - \boldsymbol{c}^*) + \boldsymbol{D}_A^*(\boldsymbol{c'} - \boldsymbol{c}^*)) = 0\end{aligned}$$

根据分叉引理[13]可知，至少以$\varepsilon' \leftarrow \varepsilon(1 - 2^{-\omega(\log_2 n)})$的概率存在另一个伪造秘密值为$\boldsymbol{C'}_B$，使得$\boldsymbol{T}_B^* = \boldsymbol{A}\boldsymbol{C}_B^* = AC'_B$且$\boldsymbol{C}_B^* \neq \boldsymbol{C'}_B$。如果秘密值$\boldsymbol{C}_B^*$能使等式

$$\begin{aligned}&\boldsymbol{z}_2^* - \boldsymbol{z'}_2 + \boldsymbol{C}_B^*(\boldsymbol{c'} - \boldsymbol{c}^*)\\&+ \boldsymbol{D}_B^*(\boldsymbol{c'} - \boldsymbol{c}^*) + \boldsymbol{D}_A^*(\boldsymbol{c'} - \boldsymbol{c}^*) = 0\end{aligned}$$

则另一个秘密值$\boldsymbol{C'}_B$一定能使等式

$$\begin{aligned}&\boldsymbol{z}_2^* - \boldsymbol{z'}_2 + \boldsymbol{C'}_B(\boldsymbol{c'} - \boldsymbol{c}^*)\\&+ \boldsymbol{D}_B^*(\boldsymbol{c'} - \boldsymbol{c}^*) + \boldsymbol{D}_A^*(\boldsymbol{c'} - \boldsymbol{c}^*) \neq 0\end{aligned}$$

然后进一步化简上式可得：$\boldsymbol{A}(\boldsymbol{z}_2^* - \boldsymbol{z'}_2 + \boldsymbol{S}_B^*(\boldsymbol{c'} - \boldsymbol{c}^*)) + \boldsymbol{F}_A^*(\boldsymbol{c'} - \boldsymbol{c}^*) = 0$，SIS问题就是找到非零短向量$\boldsymbol{e'}$和$\boldsymbol{e''}$使得$A\boldsymbol{e'} + \boldsymbol{e''} = (0\mathrm{mod}q)$。由上式可得$e' = \boldsymbol{z}_2^* - \boldsymbol{z'}_2 + \boldsymbol{S}_B^*(\boldsymbol{c'} - \boldsymbol{c}^*)$，$e'' = \boldsymbol{F}_A^*(\boldsymbol{c'} - \boldsymbol{c}^*)$，已知$\|e'\| \neq 0$，由于$\boldsymbol{S}_B^*$,$\boldsymbol{F}_A^*$不唯一，$A_2$无法确定$\boldsymbol{S}_B^*$,$\boldsymbol{F}_A^*$和秘密值。

因此，C解决小整数解(SIS)问题的优势$\varepsilon' \leftarrow \varepsilon(1 - 2^{-\omega(\log_2 n)})$是可忽略的。　　证毕

5　效率分析

本节分析L-CLPSC和现有密码算法[15,16]的计算效率。比较中涵盖了各个密码算法的空间和时间两个维度上的需求，S_T表示带陷门的矩阵原像抽样算法(运行1次需要耗费35.42 ms)，S_D表示高斯采样运算(运行1次需要耗费23.03 ms)，M_v表示矩阵向量乘法运算(运行1次需要耗费5.32 ms)。此处的时间是将密码开源库PBC在VC 6.0上运行所得出的平均时间。

仿真实验中用到的参数如表1所列，本文使用不同参数进行了6次模拟实验，表1的参数是根据文献[17,18]所选取的，不同设置号对应的参数不同，对应的密码算法的安全级别也不同。

计算效率比较中忽略了向量间的加法运算和哈希函数的运算。表2给出各个密码算法公钥大小、私钥大小、密文长度的比较。表3给出各个密码算法签密运算量、解签密运算量和整体运算量的比较。在空间维度上，L-CLPSC的公钥、私钥和密文长度都有不同程度减小。

为了更方便直观得到几种密码算法在时间维度上的差距，本节依据计算时间成本做了3个模拟实验，实验使用的实验环境如下：Inte1(R) Core-i7处理器、16 GB内存、64位Windows10操作系统笔记本电脑。实验使用的软件平台是MATLAB 2018b。通过实验做出几个密码算法的签密、解签

表 1　实验参数的设置

	参数设置号					
	1	2	3	4	5	6
n	128	136	192	214	256	320
m	2816	2992	4608	5992	6144	7680
q	2048	2048	4096	16384	4096	4096

表 2　方案之间在空间维度比较

方案	公钥大小	私钥大小	密文长度
方案[15]	$3n^2\log_2 q$	$6n^3\log_2 q\log_2 n$	$12n^2\log_2 n\log_2 q$
方案[16]	$m(1+n)\log_2 q$	$2n^2k\log_2 q$	$2kn\log_2 q$
L-CLPSC	$nk\log_2 q$	$mk\log_2 q$	$2n\log_2 q$

表 3　方案之间在时间维度比较

方案	签密运算量	解签密运算量	方案整体运算量
方案[15]	S_T+5S_D+6M_v	S_T+5M_v	2S_T+6S_D+13M_v
方案[16]	6S_D+6M_v	4M_v	S_T+6S_D+13M_v
L-CLPSC	4S_D+4M_v	3M_v	S_T+4S_D+8M_v

密和整体方案的运行时间比较仿真图，从图1(a)可看出，在签密算法的比较中，L-CLPSC总体花费时间更少，随着安全参数的增大，时间减小更快，说明L-CLPSC的计算效率也越高。图1(b)说明，在解签密算法的比较中，L-CLPSC的计算效率有绝对的优势。图1(c)说明L-CLPSC的计算成本最低。因此，L-CLPSC是一个效率更高的密码算法。

6 结束语

本文提出IND-CCA2和UF-CMA安全的基于无证书的格基代理签密(L-CLPSC)方案。性能分析说明，L-CLPSC在空间和时间维度方面的尺寸与耗时更少，因而效率更高。L-CLPSC采用格密码技术，故具有抗量子计算攻击的特性。

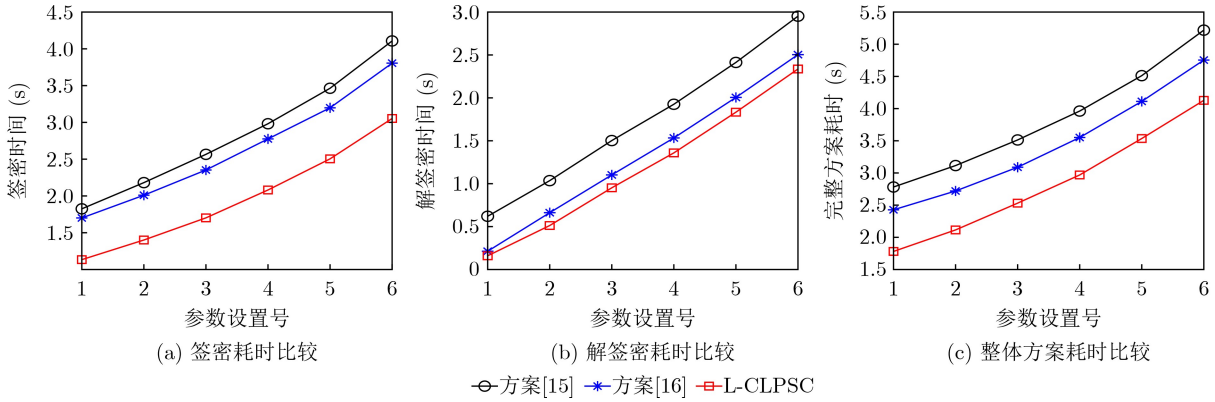

图 1 各方案耗时比较图

参 考 文 献

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]. CRYPTO 84 on Advances in Cryptology, Santa Barbara, USA, 1984: 47–53. doi: 10.1007/3-540-39568-7_5.

[2] AL-RIYAMI S S and PATERSON K G. Certificateless public key cryptography[C]. The 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, China, 2003: 452–473. doi: 10.1007/978-3-540-40061-5_29.

[3] YU Huifang and WANG Zhicang. Construction of certificateless proxy signcryption scheme from CMGs[J]. *IEEE Access*, 2019, 7: 141910–141919. doi: 10.1109/ACCESS.2019.2943718.

[4] SHOR P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]. The 35th Annual Symposium on Foundations of Computer Science, Santa Fe, USA, 1994: 124–134. doi: 10.1109/SFCS.1994.365700.

[5] GENTRY C. Fully homomorphic encryption using ideal lattices[C]. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, USA, 2009: 169–178. doi: 10.1145/1536414.1536440.

[6] 夏峰, 杨波, 马莎, 等. 基于格的代理签名方案[J]. 湖南大学学报:自然科学版, 2011, 38(6): 84–88.
XIA Feng, YANG Bo, MA Sha, *et al*. Lattice-based proxy signature scheme[J]. *Journal of Hunan University:Natural Sciences*, 2011, 38(6): 84–88.

[7] 江明明, 胡予濮, 王保仓, 等. 格上的高效代理签名[J]. 北京邮电大学学报, 2014, 37(3): 89–92. doi: 10.13190/j.jbupt.2014.03.018.
JIANG Mingming, HU Yupu, WANG Baocang, *et al*. Efficient proxy signature over lattices[J]. *Journal of Beijing University of Posts and Telecommunications*, 2014, 37(3): 89–92. doi: 10.13190/j.jbupt.2014.03.018.

[8] 陈虎, 胡予濮, 连至助, 等. 有效的格上无证书加密方案[J]. 软件学报, 2016, 27(11): 2884–2897. doi: 10.13328/j.cnki.jos.004884.
CHEN Hu, HU Yupu, LIAN Zhizhu, *et al*. Efficient certificateless encryption schemes from lattices[J]. *Journal of Software*, 2016, 27(11): 2884–2897. doi: 10.13328/j.cnki.jos.004884.

[9] 路秀华, 温巧燕, 王励成, 等. 无陷门格基签密方案[J]. 电子与信息学报, 2016, 38(9): 2287–2293. doi: 10.11999/JEIT151044.
LU Xiuhua, WEN Qiaoyan, WANG Licheng, *et al*. A lattice-based signcryption scheme without trapdoors[J]. *Journal of Electronics & Information Technology*, 2016, 38(9): 2287–2293. doi: 10.11999/JEIT151044.

[10] 欧海文, 范祯, 蔡斌思, 等. 理想格上基于身份的代理签名[J]. 计算机应用与软件, 2018, 35(1): 312–317. doi: 10.3969/j.issn.1000-386x.2018.01.054.
OU Haiwen, FAN Zhen, CAI Binsi, *et al*. Identity-based proxy signature scheme over ideal lattices[J]. *Computer Applications and Software*, 2018, 35(1): 312–317. doi: 10.3969/j.issn.1000-386x.2018.01.054.

[11] 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.

[12] MICCIANCIO D and REGEV O. Worst-case to average-case reductions based on Gaussian measures[J]. *SIAM Journal on Computing*, 2007, 37(1): 267–302. doi: 10.1137/S0097539705447360.

[13] LYUBASHEVSKY V. Lattice signatures without trapdoors[C]. The 31st Annual International Conference on Theory and Applications of Cryptographic Techniques, Cambridge, UK, 2012: 738–755. doi: 10.1007/978-3-642-29011-4_43.

[14] 俞惠芳, 杨波. 可证安全的无证书混合签密[J]. 计算机学报, 2015, 38(4): 804–813.
YU Huifang and YANG Bo. Provably secure certificateless hybrid signcryption[J]. *Chinese Journal of Computers*, 2015, 38(4): 804–813.

[15] SATO S and SHIKATA J. Lattice-based signcryption without random oracle[C]. The 9th International Conference on Post- Quantum Cryptography, Fort Lauderdale, USA, 2018: 331–351. doi: 10.1007/978-3-319-79063-3_16.

[16] YU Huifang, BAI Lu, HAO Ming, *et al*. Certificateless signcryption scheme from lattice[J]. *IEEE Systems Journal*, 2021, 15(2): 2687–2695. doi: 10.1109/JSYST.2020.3007519.

[17] LINDNER R and PEIKERT C. Better key sizes (and attacks) for LWE-based encryption[C]. The Cryptographers' Track at the RSA Conference on Topics in Cryptology, San Francisco, USA, 2011: 319–339. doi: 10.1007/978-3-642-19074-2_21.

[18] 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.

俞惠芳：女，1972年生，博士，教授，研究方向为密码理论与信息安全.

王　宁：男，1996年生，硕士生，研究方向为格密码理论与网络编码密码理论.

责任编辑：马秀强