# 基于 RLWE 的可证明安全无陷门签密方案

刘镇，韩益亮，杨晓元，柳曙光
（武警工程大学密码工程学院，陕西 西安 710086）

**摘 要**：针对现有基于格的签密存在的效率与安全性问题，基于 ABB16 的签名方案 ring-TESLA，构造了一个在机密性和认证性方面分别达到自适应抗选择密文攻击不可区分安全性和抗选择消息攻击强不可伪造安全性的无陷门签密方案 RLWE-SC，其安全性可规约到环上带差错的学习问题。环上的构造方式优化了方案的公私钥尺寸，无陷门的构造方式避免了方案使用复杂的陷门产生和原像抽样运算。效率分析与实验表明，与现有的同等安全强度的格签密方案相比，RLWE-SC 具有较高的计算和通信效率。

**关键词**：签密；环上带差错的学习；无陷门；可证明安全性；抗量子攻击
**中图分类号**：TP309
**文献标识码**：A
**doi:** 10.11959/j.issn.1000−436x.2020093

# Provable security signcryption scheme based on RLWE without trapdoor

LIU Zhen, HAN Yiliang, YANG Xiaoyuan, LIU Shuguang
College of Cryptography Engineering, Engineering University of PAP, Xi'an 710086, China

**Abstract:** In view of the existing efficiency and security problems of lattice based signcryption, with the ABB16's signature scheme ring-TESLA, a signcryption scheme without trapdoor named RLWE-SC was constructed, which achieved indistinguish ability against adaptive chosen cipher text attack (IND-CCA2) security and strongly existential unforgeability against chosen message attack (SUF-CMA) security respectively in terms of confidentiality and authentication based on the problem of learning with errors on ring. The size of the public and private keys was optimized by the construction on the ring. The complex trapdoor generation and preimage sample calculation was avoided by the structure without trapdoor. Efficiency analysis and experiment shows that RLWE-SC has better computational and communication performance than other similar lattice-based signcryption schemes with the same security strength.

**Key words:** signcryption, learning with errors on ring, without trapdoor, provable security, quantum attack resistance

## 1 引言

消息传输和存储过程中的机密性和认证性问题是信息系统安全的基本问题，传统的解决方法是先加密后签名。1997 年，Zheng[1]提出了一种新颖的解决方法——签密，它将加密与签名结合成了一步。与传统的先加密后签名的方法比，签密显著降低了计算和通信开销。近年来，签密已成为一个研究热点，大量的签密方案相继提出[2-3]。然而这些方案大多都是基于离散对数或双线性对来实现的，其安全性可以归约到离散对数或大整数因子分解问题。

**收稿日期**：2019–10–08；**修回日期**：2020–04–18
**通信作者**：韩益亮，hanyil@163.com
**基金项目**：国家自然科学基金资助项目（No.61572521, No.U1636114, No.61772550）；国家密码发展基金资助项目（No.2017YFB0802000）；武警工程大学科研创新团队基金资助项目（No.KYTD201805）
**Foundation Items:** The National Natural Science Foundation of China (No.61572521, No.U1636114, No.61772550), The National Cryptography Development Fund of China (No.2017YFB0802000), Research and Innovation Team of Engineering University of PAP(No.KYTD201805)

随着量子计算的突飞猛进，传统的基于离散对数或大整数因子分解问题构造的密码方案的安全性受到了极大的挑战。格作为一种新颖的密码学工具，引起了学术界的广泛关注。它具有计算效率高、构造功能灵活等诸多优点，是抗量子攻击密码最重要的成员之一。近年来，基于格的加密[4-5]和签名[6-7]的相关成果不断涌现，成果丰硕，然而基于格的签密研究并不充分[8-15]。研究基于格的签密，对丰富签密的密码学构造、增强签密在后量子时代的安全性具有重要意义。

WHW12[8]首次构造了一种基于格的混合签密方案，并证明方案的自适应抗选择密文攻击不可区分（IND-CCA2, indistinguishability against adaptive chosen ciphertext attack）安全性和抗选择消息攻击强不可伪造性（SUF-CMA, strongly existential unforgeability against chosen message attack）。随后，LBK13[9]构造了一种与 WHW12 具有同等安全性的格基标准签密方案，这 2 种方案的构造都是在随机预言机模型下的。YWWY13[10]构造了一种在标准模型下可证明安全的基于格的签密方案，遗憾的是该方案构造复杂，牺牲了太多的计算和通信效率，不具有实用性。再之后，LWJ14[11]和 SS18[16]分别构造了标准模型下同时满足 IND-CCA2 和 SUF-CMA 安全性的格签密方案，方案的效率较 YWWY13 有了较大的改进，但仍然较低。LTT19[17]将基于 NTRU 的密钥封装机制[18]与基于 NTRU 的签名方案[19]结合，构造了一种基于 NTRU 的签密方案，该方案在机密性和认证性方面分别达到 IND-CCA2 和 SUF-CMA 安全性，然而其在 IND-CCA2 安全性证明过程中没有考虑解密预言机。YCL19[20]采用混沌哈希函数和格上基于标签的陷门技术，进一步改进了标准模型下基于格的签密的效率，但效率仍然不高。值得一提的是，上述的格签密方案都是基于陷门构造的，格上的陷门产生和原像抽样算法计算复杂是影响格密码实用的重要因素。近年来，无陷门的格密码逐渐引起了学术界的重视。

LWWD16[13]基于无陷门的格签名方案[12]构造了一种无陷门的格签密方案，与前面的格签密方案相比，LWWD16 方案的效率有了较大的改进，但是该方案的公私钥尺寸仍然较大，并且方案在认证性方面只达到了抗选择消息攻击不可伪造性（EUF-CMA, existential unforgeability against chosen message attack）安全，它的安全强度低于 SUF-CMA。FK18[14]基于 ABB16[7]环上的无陷门签名方案 ring-TESLA 和 ADP16[15]环上的密钥交换协议，采用密钥交换和密钥封装 2 种方式分别构造了无陷门的签密方案。由于在环上构造的密码方案公私钥尺寸较小，FK18 与 LWWD16 比公私钥尺寸有了明显改进，并且在认证性方面达到了更高的 SUF-CMA 安全性，但遗憾的是，FK18 在机密性上只达到抗选择明文攻击不可区分性（IND-CPA, indistinguishability against chosen plaintext attack）安全，安全性低于 LWWD16。LHY19[21]基于相同的底层签名和密钥交换协议，改进了 FK18 的构造，将 FK18 的机密性提高到了 IND-CCA2 安全，但计算量和密文尺寸增加很大。

基于 ABB16 的 ring-TESLA 签名方案，本文构造了一种在机密性和认证性方面分别达到 IND-CCA2 和 SUF-CMA 安全的无陷门的格基签密方案，并证明了方案的安全性。本文底层的签名方案与 FKK8 和 LHY19 一样，都是 ABB16 的高效无陷门的 ring-TESLA 签名方案，但是为实现机密性，本文没有使用 ADP16 的环上密钥交换协议，而是基于环上 LWE 问题，借鉴了 FO13[22]构造 IND-CCA2 安全的混合加密方案的方法，与 LHY19 相比计算和通信效率得到了改进。最后将本文的签密方案与相关的格基签密方案进行了效率对比，本文方案没有用到复杂的陷门生成和原像抽样运算，与其他同等安全强度的格签密方案相比，本文方案在效率上有明显的优势，与目前较高效的 FK18 具有相近的效率，但在机密性上要优于 FK18。如果利用一次签名技术将 FK18 转换成与本文方案同等安全强度的方案后，本文方案的计算和通信效率有明显优势。

## 2　相关基础知识

### 2.1　符号说明

设 $\mathbb{R}$、$\mathbb{N}$、$\mathbb{Z}$ 分别表示实数集、自然数集和整数集，对于 $k\in\mathbb{N}$，本文定义 $n=2^k\in\mathbb{N}$，素数 $q\in\mathbb{N}$，满足 $q\equiv 1(\bmod 2n)$。所有的对数运算都以 2 为底数，$\mathbb{Z}_q$ 表示有限域 $\frac{\mathbb{Z}}{q\mathbb{Z}}$。定义环 $\mathfrak{R}=\frac{\mathbb{Z}[x]}{x^n+1}$，有单位元的环用 $\mathfrak{R}^\times$ 表示，环 $\mathfrak{R}_q=\frac{\mathbb{Z}_q[x]}{x^n+1}$，$\mathfrak{R}_{q,B}=\left\{\sum_{i=0}^{n-1}a_i x^i\in\mathfrak{R}_q \mid i\in[0,n-1], a_i\in[-B,B]\right\}$，其中

$B \in \left[0, \frac{q}{2}\right]$。

给定一个同构 $\Theta_q : \mathbb{Z}_n \to \Re_q$，$(a_0, a_1, \cdots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$，则 $\Re_q$ 和 $\mathbb{Z}_q^n$ 在模 $\mathbb{Z}$ 的意义下是同构的。因此多项式 $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ 可以用它的系数向量 $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n-1})^{\mathrm{T}}$ 来表示。定义 $\mathbf{rot}(\boldsymbol{a}) = (a_{n-1}, a_0, \cdots, a_{n-2})^{\mathrm{T}}$，$\mathbf{Rot}(\boldsymbol{a}) = (\boldsymbol{a}, \mathbf{rot}(\boldsymbol{a}), \cdots, \mathbf{rot}(\boldsymbol{a})^{n-1})^{\mathrm{T}} \in \mathbb{Z}_q^{n \times n}$，当且仅当 $\mathbf{Rot}(\boldsymbol{a})$ 满秩时，有 $\boldsymbol{a} \in \Re_q^{\times}$。

定义 $\overline{B}_{n,\omega} = \{\boldsymbol{v} \in \{0,1\}^n \,|\, \|\boldsymbol{v}\|^2 = \omega\}$。对于任一向量，用 $\|\cdot\|$ 来表示向量的欧几里得范数。设问题的求解规模为 $n$，用 $T(n)$ 表示该算法的耗时，当 $n$ 趋向无穷大时，$T(n)$ 的数量级（阶）称为算法的渐进时间复杂度，用函数 $O(\cdot)$ 来表示，例如当 $n$ 趋向无穷大时，$T(n)$ 的阶为 2，那么 $T(n) = O(n^2)$。

设 $\hat{\boldsymbol{\lambda}}$ 是一个随机算法，$r$ 为算法包含的随机数，$y \leftarrow \hat{\boldsymbol{\lambda}}(x, r)$ 表示算法 $\hat{\boldsymbol{\lambda}}$ 输入 $x$，选择随机数 $r$，输出 $y$，当省略随机数 $r$ 时，用 $y \leftarrow_{\mathrm{Rnd}} \hat{\boldsymbol{\lambda}}(x)$ 来表示。设 $o$ 是一个预言机，$\hat{\boldsymbol{\lambda}}^o$ 表示算法 $\hat{\boldsymbol{\lambda}}$ 可以访问 $o$。设 $\sigma \in \mathbb{R} > 0$，$D_\sigma$ 表示整数 $\mathbb{Z}$ 上的标准差为 $\sigma$ 的离散高斯分布。$d \leftarrow D_\sigma$ 表示 $d$ 服从高斯分布 $D_\sigma$，$\boldsymbol{v} \leftarrow D_\sigma^n$ 表示向量 $\boldsymbol{v}$ 的每一维元素都服从 $D_\sigma$ 的高斯分布。为了简化符号，本文把抽样一个多项式 $\boldsymbol{a} \in \Re$ 的所有系数也用 $\boldsymbol{a} \leftarrow D_\sigma^n$ 来表示。对于一个有限集合 $S$，用 $s \leftarrow U(S)$ 或者简式 $s \leftarrow_{\$} S$ 来表示从 $S$ 中随机均匀抽取一个元素 $s$，其中 $U(\cdot)$ 表示均匀抽样。

舍入运算。对于 $d \in \mathbb{N}$，$c \in \mathbb{Z}$，用 $[c]_{2^d}$ 来表示 $c \bmod 2^d$ 在区间 $[-2^{d-1}, 2^{d-1}]$ 的唯一值，本文定义舍入运算 $\lfloor \cdot \rceil_d : \mathbb{Z} \to \mathbb{Z}, c \mapsto \frac{c - [c]_{2^d}}{2^d}$。通过分别应用 $\lfloor \cdot \rceil_d$ 或 $[\cdot]_{2^d}$ 运算到向量或者多项式的每一个组成元素，该定义可以自然扩展到向量的情况。为了描述简单，后面将 $\lfloor v \bmod q \rceil_d$ 缩写成 $\lfloor v \rceil_{d,q}$。

### 2.2 格

设 $n \geqslant k > 0$，$k$ 维格 $\Lambda$ 是 $\mathbb{R}^n$ 的一个子群，它包含 $k$ 个线性独立的向量 $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_k\} = \boldsymbol{B}$ 的所有线性组合，例如 $\Lambda = \Lambda(\boldsymbol{B}) = \{\boldsymbol{Bx} | \boldsymbol{x} \in \mathbb{Z}^k\}$。定义格的秩为 $\det(\Lambda(\boldsymbol{B})) = \sqrt{\det(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B})}$。如果 $q\mathbb{Z} \subset \Lambda$，那么 $\Lambda \in \mathbb{Z}^n$ 被称作 $q-$ary 格。定义 $q-$ary 格 $\Lambda_q^{\perp}(\boldsymbol{B}) = \{\boldsymbol{x} \in \mathbb{Z}^n \,|\, \boldsymbol{B}^{\mathrm{T}}\boldsymbol{x} = 0 \bmod q\}$ 和 $\Lambda_q(\boldsymbol{B}) = \{\boldsymbol{x} \in \mathbb{Z}^n \,|\, \exists \boldsymbol{s} \in \mathbb{Z}^k, \text{s.t.} \boldsymbol{x} = \boldsymbol{Bs} \bmod q\}$。进一步地，对于 $\boldsymbol{u} \in \mathbb{Z}_q^k$，定义 $\Lambda_{\boldsymbol{u},q}^{\perp}(\boldsymbol{B}) = \{\boldsymbol{x} \in \mathbb{Z}^n \,|\, \boldsymbol{B}^{\mathrm{T}}\boldsymbol{x} = \boldsymbol{u} \bmod q\}$，例如 $\Lambda_q^{\perp}(\boldsymbol{B}) = \Lambda_{0,q}^{\perp}(\boldsymbol{B})$。$\Lambda_{\boldsymbol{u},q}^{\perp}(\boldsymbol{B})$ 也可以看作向量 $\boldsymbol{u}$ 的转换格，例如 $\Lambda_{\boldsymbol{u},q}^{\perp}(\boldsymbol{B}) = \Lambda_q^{\perp}(\boldsymbol{B}) + \boldsymbol{y}$，其中 $\boldsymbol{y} \in \mathbb{Z}^n$ 是 $\boldsymbol{B}^{\mathrm{T}}\boldsymbol{x} = \boldsymbol{u} \bmod q$ 的整数解[7]。

### 2.3 环上的 LWE 问题

**定义 1**[7] 环上 LWE 分布。设 $n$、$q$ 为正整数，$\boldsymbol{s} \in \Re_q$，$\chi$ 是环 $\Re$ 上的某个分布，均匀随机选取 $\boldsymbol{a} \leftarrow \Re_q$，$\boldsymbol{e} \leftarrow \chi$，则称 $A_{\boldsymbol{s},\chi} = (\boldsymbol{a}, \boldsymbol{t} = \boldsymbol{as} + \boldsymbol{e})$ 为环 $\Re_q \times \Re_q$ 上的 LWE 分布。

**定义 2**[7] 环上的判定性 LWE 问题。设 $n$、$q$、$k$ 为正整数，$q = 2^k$，$\chi$ 是环 $\Re$ 上的某个分布，$o_x$ 是一个预言机，当输入 $\boldsymbol{s} \in \Re_q$ 时，$o_x(\boldsymbol{s})$ 返回一个抽样 $A_{\boldsymbol{s},\chi}$。本文称一个判定性环上带差错学习问题 $\mathrm{RLWE}_{q,n,m,\chi}$ 是 $(\boldsymbol{t}, \varepsilon)$ 困难的，如果对于任意概率多项式时间（PPT, probabilistic polynomial time）算法 $\hat{\boldsymbol{\lambda}}$，运行时间为 $t$，最多进行 $m$ 次预言机 $o_x$ 询问，则有以下等式成立。

$$\mathrm{Adv}_{n,q,\mathcal{X}}^{\mathrm{RLWE}}(\hat{\boldsymbol{\lambda}}) = |\Pr[\hat{\boldsymbol{\lambda}}^{o_x(\boldsymbol{s})} = 1] - \Pr[\hat{\boldsymbol{\lambda}}^{U(\Re_q \times \Re_q)} = 1]| \leqslant \varepsilon$$

其中，$\boldsymbol{s} \leftarrow U(\Re_q)$，$A_{\boldsymbol{s},\chi}$ 是随机选取的。

ACP09[23]证明了即使秘密分布 $\boldsymbol{s}$ 同错误分布 $\chi$ 相同时，上述带差错的学习问题依然是同等困难的。特别地，当 $\chi$ 为标准差为 $\sigma$ 的离散高斯分布时，本文用 $\mathrm{RLWE}_{q,n,m,\sigma}$ 来表示。

## 3 签密

**定义 3** 签密。设 $k$ 为安全参数，一个语义安全的标准签密方案 $\sum_{\mathrm{SC}}$ 包括 4 种多项式时间算法，即 $\sum_{\mathrm{SC}} = (\mathrm{Gen}, \mathrm{KeyGen}, \mathrm{SC}, \mathrm{DSC})$，其中 $\mathrm{KeyGen} = (\mathrm{KeyGen}_R, \mathrm{KeyGen}_S)$。

$\mathrm{Gen}(1^k)$ 是随机化的参数生成算法，输入安全参数 $k \in \mathbb{N}$，输出随机化系统参数 parm，可表示为 $\mathrm{parm} \leftarrow_{\mathrm{Rnd}} \mathrm{Gen}(1^k)$。

$\mathrm{KeyGen}_R(\mathrm{parm})$ 是随机化密钥生成算法，它接收公开参数 parm 作为输入，输出接收方的公钥 $\mathrm{pk}_R$ 与私钥 $\mathrm{sk}_R$，可表示为 $(\mathrm{pk}_R, \mathrm{sk}_R) \leftarrow_{\mathrm{Rnd}} \mathrm{KeyGen}_R(\mathrm{parm})$。

$\mathrm{KeyGen}_S(\mathrm{parm})$ 是随机化密钥生成算法，它接收公开参数 parm 作为输入，输出发送方的公钥 $\mathrm{pk}_S$

与私钥 $\mathrm{sk}_S$，可表示为 $(\mathrm{pk}_S,\mathrm{sk}_S)\leftarrow_{\mathrm{Rnd}}\mathrm{KeyGen}_S(\mathrm{parm})$。

$\mathrm{SC}(m,\mathrm{pk}_R,\mathrm{sk}_S)$ 是随机化签密算法，它接收接收方的公钥 $\mathrm{pk}_R$、发送方的私钥 $\mathrm{sk}_S$ 及消息 $m\in\mathrm{msp}$（msp 是消息空间）作为输入，输出一个签密文 $c$，可表示为 $c\leftarrow_{\mathrm{Rnd}}\mathrm{SC}(m,\mathrm{pk}_R,\mathrm{sk}_S)$。

$\mathrm{DSC}(c,\mathrm{pk}_S,\mathrm{sk}_R)$ 是一种确定性解签密算法，它接收发送方的公钥 $\mathrm{pk}_S$、接收方的私钥 $\mathrm{pk}_R$ 及签密文 $c$ 作为输入，输出一个消息 $m$ 或者终止符号 $\perp$，可表示为 $(m,\perp)\leftarrow_{\mathrm{Rnd}}\mathrm{DSC}(c,\mathrm{pk}_S,\mathrm{sk}_R)$。

正确性。上述签密方案是正确的，当且仅当对于 $(\mathrm{pk}_S,\mathrm{sk}_S)\leftarrow_{\mathrm{Rnd}}\mathrm{KeyGen}_S(\mathrm{parm})$，$(\mathrm{pk}_R,\mathrm{sk}_R)\leftarrow_{\mathrm{Rnd}}\mathrm{KeyGen}_R(\mathrm{parm})$，解签密算法 $\mathrm{DSC}(\mathrm{SC}(m,\mathrm{pk}_R,\mathrm{sk}_S),\mathrm{pk}_S,\mathrm{sk}_R)$ 的输出为 $m$。

安全性。安全的签密方案应当同时满足机密性和认证性。

机密性方面，标准的安全概念有 IND-CPA 和 IND-CCA2。IND-CPA 安全性限制了敌手只能访问加密预言机；而 IND-CCA2 安全性意味着敌手拥有很强的攻击能力，可以访问解密预言机，它是一个较 IND-CPA 更强的安全概念。

认证性方面，标准的安全概念是 EUF-CMA 和 SUF-CMA。给定消息 $m$ 及相应的签名 $\sigma$，EUF-CMA 安全性意味着敌手不能伪造其他消息 $m'$ 的签名 $\sigma'$，而 SUF-CMA 安全性意味着敌手不能伪造消息 $m$ 的其他签名 $\sigma'$。同 EUF-CMA 相比，SUF-CMA 在敌手获胜的判定条件上更加严格，它意味着敌手具有更强的攻击能力，是一个更强的安全概念。SUF-CMA 安全的方案是构造群签名和认证密钥交换协议的重要工具[24]。

本文主要考虑 IND-CCA2 安全性和 SUF-CMA 安全性。

1) 机密性（IND-CCA2）

考虑挑战者 B 和攻击者 A 之间进行下面的游戏。

**初始化**　B 运行密钥生成算法，获得接收方的公私钥对 $(\mathrm{pk}_R^*,\mathrm{sk}_R^*)$，并把 $\mathrm{pk}_R^*$ 发送给攻击者 A，$\mathrm{sk}_R^*$ 保密。

**阶段 1**　A 以适应性方式进行多项式边界次解签密询问。在进行解签密询问时，A 发送密文 $c$ 以及公私钥对 $(\mathrm{pk}_S,\mathrm{sk}_S)$ 给 B，如果密文是合法的，B 运行解签密算法 $\mathrm{DSC}(c,\mathrm{pk}_S,\mathrm{sk}_R^*)$ 得到消息，否则输出拒绝标识 $\perp$。

**挑战**　阶段 1 结束后，A 选择消息空间中 2 个等长的明文 $(m_0,m_1)$ 以及发送方的公私钥对 $(\mathrm{pk}_S^*,\mathrm{sk}_S^*)$ 发送给 B。接下来 B 抛硬币选择一个随机比特 $b\in\{0,1\}$ 运行签密算法，得到挑战密文 $c^*=\mathrm{SC}(m_b,\mathrm{pk}_R^*,\mathrm{sk}_S^*)$，发送给 A。

**阶段 2**　A 继续同阶段 1 一样适应性地进行多项式边界次解签密询问，但是要求不能对发送方的公私钥对 $(\mathrm{pk}_S^*,\mathrm{sk}_S^*)$ 生成的挑战密文 $c^*$ 进行询问。

**猜测**　A 输出一个猜测的比特 $b'$，如果 $b'=b$，那么 A 赢得游戏。

定义敌手 A 的优势为 $\mathrm{Adv}_{\mathrm{SC,A}}^{\mathrm{CCA2}}(k)=|2\Pr[b'=b]-1|$，本文称一个签密方案 $\sum_{\mathrm{SC}}$ 是 $(\varepsilon,t,q_{\mathrm{DSC}})$ -IND-CCA2 安全的，如果在上述的 IND-CCA2 游戏中，对于任意概率多项式时间 $t$ 的敌手 A，进行不超过 $q_{\mathrm{DSC}}$ 次解签密询问，优势不超过 $\varepsilon$。

在上述安全模型定义中，由于 A 知道发送方的私钥 $\mathrm{sk}_S^*$，因此它是一个非常强的安全概念，对应着签密方案机密性中的内部安全性，详见文献[25]，由于大部分同类方案都满足此性质，本文不做特别强调。

2) 认证性（SUF-CMA）

考虑挑战者 B 和伪造者 F 之间进行下面的游戏。

**初始化**　B 运行密钥生成算法，生成发送方的公私钥对 $(\mathrm{pk}_S^*,\mathrm{sk}_S^*)$，并把 $\mathrm{pk}_S^*$ 发送给伪造者 F，$\mathrm{sk}_S^*$ 保密。

**询问阶段**　F 自适应地进行多项式边界次签密询问。在进行解签密询问时，F 发送消息 $m$ 以及接收方的公私钥对 $(\mathrm{pk}_R,\mathrm{sk}_R)$ 给 B，B 运行签密算法 $\mathrm{SC}(m,\mathrm{sk}_S^*,\mathrm{pk}_R)$ 得到密文 $c$，并将 $c$ 发送给伪造者 F。

**伪造阶段**　询问阶段结束后，F 选定接收方公私钥对 $(\mathrm{pk}_S^*,\mathrm{sk}_S^*)$ 和一个消息 $m^*$，伪造一个签密文 $c^*$，并发送 $(m^*,c^*)$ 给挑战者 B，要求 $m^*$ 的签密 $c^*$ 没有被询问过。

如果 $\mathrm{DSC}(c^*,\mathrm{pk}_S^*,\mathrm{sk}_S^*)=m^*$，那么伪造者 F 赢得游戏。

本文定义伪造者 F 的优势为 $\mathrm{Adv}_{\varepsilon,\mathrm{F}}^{\mathrm{SUF\text{-}CMA}}(k)=\max\{\Pr[\mathrm{DSC}(c^*,\mathrm{pk}_{\mathrm{S}}^*,\mathrm{sk}_R^*)=m^*]\}$。如果任意敌手 F

的优势 $\mathrm{Adv}_{\mathcal{E},\mathrm{F}}^{\text{SUF-CMA}}(k)$ 是可以忽略的，则称 $\varepsilon$ 是一个抗选择消息攻击强不可伪造性（SUF-CMA）安全的签密方案。

## 4 基于环上 LWE 问题的签密（RLWE-SC）

FK18 将 ABB16 的 ring-TESLA 签名方案与 ADP16 的环上密钥交换协议相结合，采用密钥交换和密钥封装 2 种方式分别构造了环上无陷门的签密方案，该方案的效率较高，然而在机密性方面仅达到 IND-CPA 安全性。为了在机密性方面达到 IND-CCA2 安全性，LHY19 改进了 FK18 的构造，但仍然是采用 ABB16 的 ring-TESLA 签名方案和 ADP16 的环上密钥交换协议相结合的方法，并且还牺牲了较多的通信效率和计算效率。本节放弃使用 ADP16 的密钥交换协议，将 ABB16 的 ring-TESLA 签名方案与 LP13 的环上公钥加密方案相结合，并借鉴 F013 的方法，构造一种在机密性和认证性上分别达到 IND-CCA2 和 SUF-CMA 安全的签密方案。

### 4.1 具体方案

发送方 $S$ 将消息 $m$ 签密后发送给接收方 $R$，接收方 $R$ 获得消息 $m$，签密算法具体如下。

1) 参数生成算法 $\mathrm{parm} \leftarrow_{\mathrm{Rnd}} \mathrm{Gen}$

系统初始化，产生系统参数 parm 如下。

① 设 $\lambda$ 为安全参数，$n$、$k$ 为自然数且满足 $n>k>\lambda$，为了方便多项式乘法运算，令 $n=2^k$。

② 令 $U=14\sigma\sqrt{\omega}$，$B=14\sigma(n-1)\sqrt{\omega}$，$M=\left(\dfrac{2(B-U)+1}{2B+1}\right)^n$。

③ 选取小自然数 $d$ 作为舍入值（满足 $d>\log B$，典型地可取 24），参数 $0<\alpha<1$，模数 $q\geqslant\left(\dfrac{2^k+2n(d+1)}{(2B)^n}\right)^{\frac{1}{n}}$ 且 $q\geqslant 4B$，令 $\sigma=\alpha q$。

④ 令 $D_\sigma$ 表示均值为 0、标准差为 $\sigma$ 的高斯分布。

⑤ 设 $F:\{0,1\}^k\rightarrow\overline{B}_{n,\omega}$ 为编码函数，它将哈希函数的输出作为输入，输出一个权重为 $\omega$、长度为 $n$ 的向量，详见文献[9]，其中参数 $\omega$ 使不等式 $2^k\geqslant|\overline{B}_{n,\omega}|=2^\omega\binom{k}{\omega}\geqslant 128$ 成立，进一步地，设 $\boldsymbol{a}_1,\boldsymbol{a}_2\in\Re_q^\times$ 是环 $\Re_q$ 上 2 个随机均匀抽样，它们为方案公开的全局常量。

⑥ 选取一个安全的对称加密算法 $(E_{\text{key}}(\cdot),D_{\text{key}}(\cdot))$，其中 key 为对称密钥，密钥空间用 $\mathrm{keysp}(k)$ 表示。

⑦ 选取 3 个抗碰撞的哈希函数 $(H_1,H_2,H_3)$，其中 $H_1:\{0,1\}^*\rightarrow\{0,1\}^k$（典型地可实例化为 SHA-256），$H_2:\{0,1\}^n\rightarrow\mathrm{keysp}(\lambda)$，$H_3:\{0,1\}^*\times\{0,1\}^*\Rightarrow\prod$（其中 $\mathrm{keysp}(k)$ 表示密钥空间，$\prod$ 表示多次抛硬币得到的随机空间，设 $\mathrm{keysp}(k)$ 和 $\prod$ 空间大小分别为 $f_2$ 和 $f_3$）。

⑧ 设 CheckE 为拒绝抽样（rejection sampling）条件检测函数：对于多项式 $\boldsymbol{e}_S$，函数 $\max_k(\boldsymbol{e}_S)$ 返回它第 $k$ 个最大系数值（即第 $k$ 大系数值），如果 $\sum_{k=1}^{\omega}\max_k(\boldsymbol{e}_S)>L$，$\mathrm{CheckE}(\boldsymbol{e}_S)$ 返回 1，否则返回 0。设定参数 $L$ 满足 $\left(1-\dfrac{2L}{2^d}\right)^{2n}\geqslant 0.4$，其描述详见文献[7]。

2) 密钥生成算法

$(\mathrm{pk}_S,\mathrm{sk}_S)\leftarrow_{\mathrm{Rnd}}\mathrm{KeyGen}_S(\mathrm{parm})$

① 随机选取 $\boldsymbol{x}_S,\boldsymbol{e}_{1S},\boldsymbol{e}_{2S}\leftarrow D_\sigma^n$，满足 $\mathrm{CheckE}(\boldsymbol{e}_{1S})\neq 0\vee\mathrm{CheckE}(\boldsymbol{e}_{2S})\neq 0$。

② 计算 $\boldsymbol{t}_{1S}=\boldsymbol{a}_1\boldsymbol{x}_S+\boldsymbol{e}_{1S}(\mathrm{mod}\,q)$ 和 $\boldsymbol{t}_{2S}=\boldsymbol{a}_2\boldsymbol{x}_S+\boldsymbol{e}_{2S}(\mathrm{mod}\,q)$。

③ 令 $\mathrm{sk}_S\leftarrow\{\boldsymbol{x}_S,\boldsymbol{e}_{1S},\boldsymbol{e}_{2S}\}$，$\mathrm{pk}_S\leftarrow\{\boldsymbol{t}_{1S},\boldsymbol{t}_{2S}\}$。

④ 返回 $(\mathrm{pk}_S,\mathrm{sk}_S)$。

$(\mathrm{pk}_R,\mathrm{sk}_R)\leftarrow_{\mathrm{Rnd}}\mathrm{KeyGen}_R(\mathrm{parm})$

① 随机选取 $\boldsymbol{x}_R,\boldsymbol{e}_{1R},\boldsymbol{e}_{2R}\leftarrow D_\sigma^n$，满足 $\mathrm{CheckE}(\boldsymbol{e}_{1R})\neq 0\vee\mathrm{CheckE}(\boldsymbol{e}_{2R})\neq 0$。

② 计算 $\boldsymbol{t}_{1R}=\boldsymbol{a}_1\boldsymbol{x}_R+\boldsymbol{e}_{1R}(\mathrm{mod}\,q)$ 和 $\boldsymbol{t}_{2R}=\boldsymbol{a}_2\boldsymbol{x}_R+\boldsymbol{e}_{2R}(\mathrm{mod}\,q)$。

③ 令 $\mathrm{sk}_R\leftarrow\{\boldsymbol{x}_R,\boldsymbol{e}_{1R},\boldsymbol{e}_{2R}\}$，$\mathrm{pk}_R\leftarrow\{\boldsymbol{t}_{1R},\boldsymbol{t}_{2R}\}$。

④ 返回 $(\mathrm{pk}_R,\mathrm{sk}_R)$。

3) 签密算法 $c\leftarrow_{\mathrm{Rnd}}\mathrm{SC}(m,\mathrm{pk}_R,\mathrm{sk}_S)$

① 随机选择 $\boldsymbol{y}\leftarrow_{\$}\Re_{q,[B]}$，计算 $\boldsymbol{b}'=H_1(\lfloor\boldsymbol{a}_1\boldsymbol{y}\rceil_{d,q},\lfloor\boldsymbol{a}_2\boldsymbol{y}\rceil_{d,q},m,\mathrm{pk}_S,\mathrm{pk}_R)$。

② 编码 $\boldsymbol{b}=F(b')$，计算 $\boldsymbol{z}=\boldsymbol{x}_S\boldsymbol{b}+\boldsymbol{y}$、$\boldsymbol{w}_1\leftarrow\boldsymbol{a}_1\boldsymbol{y}-\boldsymbol{e}_{1S}\boldsymbol{b}$ 和 $\boldsymbol{w}_2\leftarrow\boldsymbol{a}_2\boldsymbol{y}-\boldsymbol{e}_{2S}\boldsymbol{b}$。

③ 如果 $[\boldsymbol{w}_1]_{2^d},[\boldsymbol{w}_2]_{2^d}\notin\Re_{q,2^d-L}$ 或者 $\boldsymbol{z}\notin\Re_{q,[B-U]}$，重选随机数 $\boldsymbol{y}$ 并重复以上步骤。

④ 选取随机数 $\boldsymbol{\tau}\in\{0,1\}^n$，计算 $\mu=E_{H_2(\boldsymbol{\tau})}(m,\boldsymbol{z},b')$。

⑤ 令 $\theta=H_3(\boldsymbol{\tau},\mu)$，由 $\theta$ 的随机性选取错误向

量 $\boldsymbol{e}_1,\boldsymbol{e}_2 \leftarrow D_\sigma^n$ 和 $\boldsymbol{e}_3 \leftarrow D_\sigma^n$，计算 $\boldsymbol{v}_1=\boldsymbol{a}_1\boldsymbol{e}_1+\boldsymbol{e}_2(\mathrm{mod}\,q)$，$\boldsymbol{v}_2=\boldsymbol{t}_{1R}\boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{\tau}\left\lfloor\frac{q}{2}\right\rfloor(\mathrm{mod}\,q)$。

⑥ 返回 $c\leftarrow(\boldsymbol{v}_1,\boldsymbol{v}_2,\mu)$。

4) 解签密算法 $m\leftarrow \mathrm{DSC}(c,\mathrm{pk}_S,\mathrm{sk}_R)$

① 计算 $\boldsymbol{\tau}'=(\tau_1',\tau_2',\cdots,\tau_n')\leftarrow \boldsymbol{v}_2-\boldsymbol{v}_1\boldsymbol{x}_R$。

② 对 $i=1,2,\cdots,n$，如果 $\tau_i'\in\left[-\frac{q}{4},\frac{q}{4}\right]$，令 $\tau_i'=0$，否则令 $\tau_i'=1$。

③ 令 $\boldsymbol{\tau}\leftarrow\boldsymbol{\tau}'$，计算 $(m,\boldsymbol{z},b')=D_{H_2(\boldsymbol{\tau})}(\mu)$。

④ 编码 $\boldsymbol{b}=F(b')$，计算 $\boldsymbol{w}_1\leftarrow\boldsymbol{a}_1\boldsymbol{z}-\boldsymbol{t}_{1S}\boldsymbol{b}$ 和 $\boldsymbol{w}_2\leftarrow\boldsymbol{a}_2\boldsymbol{z}-\boldsymbol{t}_{2S}\boldsymbol{b}$。

⑤ 验证 $b'=H_1(\lfloor\boldsymbol{w}_1\rceil_{d,q},\lfloor\boldsymbol{w}_2\rceil_{d,q},m,\mathrm{pk}_S,\mathrm{pk}_R)$ 和 $\boldsymbol{z}\notin\mathfrak{R}_{q,[B-U]}$ 是否成立，如果成立返回 $m$，否则返回 $\perp$。

### 4.2　正确性

如果 $c=(\boldsymbol{v}_1,\boldsymbol{v}_2,\mu)$ 是一个有效的密文，则 $\boldsymbol{\tau}'=(\tau_1',\tau_2',\cdots,\tau_n')=\boldsymbol{v}_2-\boldsymbol{v}_1\boldsymbol{x}_R=\boldsymbol{t}_{1R}\boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{\tau}\left\lfloor\frac{q}{2}\right\rfloor-\boldsymbol{a}_1\boldsymbol{e}_1x_R+\boldsymbol{e}_2\boldsymbol{x}_R=\boldsymbol{e}_{1R}\boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{e}_2\boldsymbol{x}_R+\boldsymbol{\tau}\left\lfloor\frac{q}{2}\right\rfloor$。

由于 $\boldsymbol{x}_R,\boldsymbol{e}_{1R},\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3\leftarrow D_\sigma^n$，$|\boldsymbol{e}_{1R}\boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{e}_2\boldsymbol{x}_R|<\left\lfloor\frac{q}{4}\right\rfloor$，因此如果 $\tau_i'\in\left[-\frac{q}{4},\frac{q}{4}\right]$，则有 $\tau_i'=0$，否则有 $\tau_i'=1$。再由 $D_{H_2(\boldsymbol{\tau})}(\mu)$ 可恢复 $(m,\boldsymbol{z},b')$。

进一步地，$\boldsymbol{w}_1=\boldsymbol{a}_1\boldsymbol{z}-\boldsymbol{t}_{1S}\boldsymbol{b}=\boldsymbol{a}_1\boldsymbol{x}_Sb+\boldsymbol{a}_1\boldsymbol{y}-\boldsymbol{a}_1\boldsymbol{x}_S\boldsymbol{b}-\boldsymbol{e}_{1S}\boldsymbol{b}=\boldsymbol{a}_1\boldsymbol{y}-\boldsymbol{e}_{1S}\boldsymbol{b}$，$\boldsymbol{w}_2=\boldsymbol{a}_2\boldsymbol{z}-\boldsymbol{t}_{2S}\boldsymbol{b}=\boldsymbol{a}_2\boldsymbol{x}_S\boldsymbol{b}+\boldsymbol{a}_2\boldsymbol{y}-\boldsymbol{a}_2\boldsymbol{x}_S\boldsymbol{b}-\boldsymbol{e}_{2S}\boldsymbol{b}=\boldsymbol{a}_2\boldsymbol{y}-\boldsymbol{e}_{2S}\boldsymbol{b}$，再由 $\mathrm{CheckE}(\boldsymbol{e}_{1R})\neq 0\vee\mathrm{CheckE}(\boldsymbol{e}_{2R})\neq 0$ 可得，$\lfloor\boldsymbol{a}_1\boldsymbol{y}-\boldsymbol{e}_{1S}\boldsymbol{b}(\mathrm{mod}\,q)\rceil_{d,q}=\lfloor\boldsymbol{a}_1\boldsymbol{y}(\mathrm{mod}q)\rceil_{d,q}$，$\lfloor\boldsymbol{a}_2\boldsymbol{y}-\boldsymbol{e}_{2S}\boldsymbol{b}(\mathrm{mod}q)\rceil_{d,q}=\lfloor\boldsymbol{a}_2\boldsymbol{y}(\mathrm{mod}q)\rceil_{d,q}$。从而通过验证 $b'=H_1(\lfloor\boldsymbol{w}_1\rceil_{d,q},\lfloor\boldsymbol{w}_2\rceil_{d,q},m,\mathrm{pk}_S,\mathrm{pk}_R)$ 和 $\boldsymbol{z}\notin\mathfrak{R}_{q,[B-U]}$ 是否成立就可以验证签名的正确性，最后返回 $m$ 或 $\perp$。

### 4.3　安全性

下面给出上述 RLWE-SC 方案的 IND-CCA2 安全性和 SUF-CMA 安全性规约（方案的 IND-CCA2 安全性可以借鉴 FO13 的方法来证明，SUF-CMA 安全性可以借鉴 ABB16 的方法来证明）。

**定理 1**　机密性。在随机预言机模型下，如果存在着敌手 A 在多项式时间 $t_{\mathrm{A}}$ 内，进行不多于 $q_{\mathrm{SC}}$ 次签密询问，不多于 $q_{\mathrm{DSC}}$ 次解签密询问，$q_{H_1}$ 次哈希预言机 $H_1$ 询问，$q_{H_2}$ 次哈希预言机 $H_2$ 询问，$q_{H_3}$ 次哈希预言机 $H_3$ 询问以不可忽略的优势 $\varepsilon_{\mathrm{A}}$ 攻击 RLWE-SC 方案的 IND-CCA2 安全性，那么存在着一个敌手 B 在多项式时间 $t_{\mathrm{B}}\approx t_{\mathrm{A}}+O((q_{\mathrm{SC}}+q_{\mathrm{DSC}})n^2+q_{H_1}+q_{H_2}+q_{H_3})$ 内（其中 $O(\cdot)$ 表示渐进时间复杂度函数），以优势 $\varepsilon_{\mathrm{B}}\geqslant\varepsilon_{\mathrm{A}}\left[1-q_{\mathrm{DSC}}\left(\frac{q_{H_1}}{2^k}+\frac{q_{H_2}}{2^{f_2}}+\frac{q_{H_3}}{2^{f_3}}\right)\right]$ 攻击判定性 $\mathrm{RLWE}_{q,n,2,\sigma}$ 问题。

**证明**　假设 B 被给定判定性 $\mathrm{RLWE}_{q,n,2,\sigma}$ 问题实例 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$，它们都服从 $\mathfrak{R}_q\times\mathfrak{R}_q$ 上的随机均匀分布，或者满足 $\boldsymbol{t}_1=\boldsymbol{a}_1\boldsymbol{x}+\boldsymbol{e}_{1R}$ 且 $\boldsymbol{t}_2=\boldsymbol{a}_2\boldsymbol{x}+\boldsymbol{e}_{2R}$（环上 LWE 分布 $A_{x,\chi}$），其中 $\boldsymbol{x},\boldsymbol{e}_{1R},\boldsymbol{e}_{2R}\leftarrow D_\sigma^n$。本文将敌手 B 作为 RLWE-SC 方案的挑战者来模拟 CCA2 攻击游戏，下面描述 B 如何利用 A 的知识构造一个判定性 $\mathrm{RLWE}_{q,n,2,\sigma}$ 问题的区分器。

准备公钥。对于上述给定的分布 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$，模拟者将（$\boldsymbol{a}_1,\boldsymbol{a}_2$）作为方案的公开参数，随后模拟者输出公钥 $\mathrm{pk}_R^*=\{\boldsymbol{t}_{1R}^*=\boldsymbol{t}_1,\boldsymbol{t}_{2R}^*=\boldsymbol{t}_2\}$，并发送给敌手 A。

第一阶段哈希询问与解签密询问。对 $(p_1,p_2,m,\mathrm{pk}_S,\mathrm{sk}_S)$ 的 $H_1$ 询问模拟。当收到 $H_1$ 的哈希询问时，模拟者查看多元组 $(p_1,p_2,m,\mathrm{pk}_S,\mathrm{pk}_R^*,\boldsymbol{z},b')$ 是否在 $L_1$ 中已经存在，如果存在，返回 $b'$，否则模拟者随机选择 $\boldsymbol{z}\leftarrow\mathfrak{R}_{q,[B-U]}$ 和 $b'\in\{0,1\}^k$，计算 $\boldsymbol{b}=F(b')$，$\boldsymbol{w}_1=\boldsymbol{a}_1\boldsymbol{z}-\boldsymbol{t}_{1S}\boldsymbol{b}$，$\boldsymbol{w}_2=\boldsymbol{a}_2\boldsymbol{z}-\boldsymbol{t}_{2S}\boldsymbol{b}$。接下来，检查对于所有的 $j\in(1,2,\cdots,n)$，是否满足 $[\boldsymbol{w}_{1j}]_{2^d}<2^d-L$ 和 $[\boldsymbol{w}_{2j}]_{2^d}<2^d-L$，如果不满足则重复上述过程。由拒绝抽样的性质可以得出，对于 $i=1,2$ 满足 $\lfloor\boldsymbol{w}_i\rceil_{d,q}=\lfloor\boldsymbol{a}_i\boldsymbol{y}\rceil_{d,q}$（详见文献[7]），然后模拟者将多元组 $(p_1,p_2,m,\mathrm{pk}_S,\mathrm{sk}_S,\mathrm{pk}_R^*,\boldsymbol{z},b')$ 插入 $L_1$，并返回 $b'$。

对 $\boldsymbol{\tau}$ 的 $H_2$ 询问模拟。当收到 $H_2$ 的哈希询问时，模拟者查看多元组 $(\boldsymbol{\tau},H_{2\boldsymbol{\tau}})$ 是否在 $L_2$ 中已经存在，如果存在，返回 $H_{2\boldsymbol{\tau}}$，否则模拟者随机选择 $H_{2\boldsymbol{\tau}}\leftarrow\mathrm{keysp}(\lambda)$，将元组 $(\boldsymbol{\tau},H_{2\boldsymbol{\tau}})$ 插入 $L_2$ 中，并返回 $H_{2\boldsymbol{\tau}}$。

对 $(\boldsymbol{\tau},\mu)$ 的 $H_3$ 询问模拟。当收到 $H_3$ 的哈希询

问时，模拟者查看多元组 $(\boldsymbol{\tau},\mu,H_{3\boldsymbol{\tau},\mu})$ 是否在 $L_3$ 中已经存在，如果存在，返回 $H_{3\boldsymbol{\tau},\mu}$，否则模拟者随机选择 $H_{3\boldsymbol{\tau},\mu}\leftarrow\prod$，将元组 $(\boldsymbol{\tau},\mu,H_{3\boldsymbol{\tau},\mu})$ 插入 $L_3$ 中，并返回 $H_{3\boldsymbol{\tau},\mu}$。

对 $(m,\mathrm{pk}_R,\mathrm{pk}_S,\mathrm{sk}_S)$ 的签密询问模拟。当收到对 $(m,\mathrm{pk}_R,\mathrm{pk}_S,\mathrm{sk}_S)$ 的签密询问时，模拟者选择 $\boldsymbol{y}\leftarrow_{\$}\mathfrak{R}_{q,[\mathrm{B}]}$，模拟 $\left(\lfloor\boldsymbol{a}_1\boldsymbol{y}\rceil_{d,q},\lfloor\boldsymbol{a}_2\boldsymbol{y}\rceil_{d,q},m,\mathrm{pk}_S,\mathrm{sk}_S\right)$ 的 $H_1$ 询问，获得 $(\boldsymbol{z},b')$。然后选取随机数 $\boldsymbol{\tau}\in\{0,1\}^n$，模拟对 $\boldsymbol{\tau}$ 的 $H_2$ 询问获得 $(\boldsymbol{\tau},H_{2\boldsymbol{\tau}})$，计算 $\mu=E_{H_2(\boldsymbol{\tau})}(m,\boldsymbol{z},b')$。进一步地，模拟对 $(\boldsymbol{\tau},\mu)$ 的 $H_3$ 询问获得 $(\boldsymbol{\tau},\mu,h_{3\boldsymbol{\tau},\mu})$，令 $\theta=H_3(\boldsymbol{\tau},\mu)$，由 $\theta$ 的随机性选取错误向量 $\boldsymbol{e}_1,\boldsymbol{e}_2\leftarrow D_\sigma^n$，随机选取 $\boldsymbol{e}_3\leftarrow D_\sigma^n$，计算 $\boldsymbol{v}_1=\boldsymbol{a}_1\boldsymbol{e}_1+\boldsymbol{e}_2(\mathrm{mod}\,q)$，$\boldsymbol{v}_2=\boldsymbol{t}_{1R}\boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{\tau}\left\lfloor\frac{q}{2}\right\rfloor(\mathrm{mod}\,q)$，返回 $c\leftarrow(\boldsymbol{v}_1,\boldsymbol{v}_2,\mu)$。

对 $(\boldsymbol{v}_1,\boldsymbol{v}_2,\mu,\mathrm{pk}_S,\mathrm{sk}_S)$ 的解签密询问模拟。当收到对 $(\boldsymbol{v}_1,\boldsymbol{v}_2,\mu,\mathrm{pk}_S,\mathrm{sk}_S)$ 的解签密询问时，模拟者遍历 $L_1$、$L_2$ 和 $L_3$，查看是否存在这样的元组 $(p_1,p_2,m,pk_S,sk_S,\mathrm{pk}_R^*,\boldsymbol{z},b')$、$(\boldsymbol{\tau},H_{2\boldsymbol{\tau}})$ 和 $(\boldsymbol{\tau},\mu,H_{3\boldsymbol{\tau},\mu})$，满足编码 $\boldsymbol{b}=F(b')$，$\mu=E_{H_2(\boldsymbol{\tau})}(m,\boldsymbol{z},\boldsymbol{b})$；令 $\theta=H_3(\boldsymbol{\tau},\mu)$，由 $\theta$ 的随机性选择错误向量 $\boldsymbol{e}_1,\boldsymbol{e}_2\leftarrow D_\sigma^n$ 和 $\boldsymbol{e}_3\leftarrow D_\sigma^n$，计算 $\boldsymbol{v}_1=\boldsymbol{a}_1\boldsymbol{e}_1+\boldsymbol{e}_2(\mathrm{mod}\,q)$，$\boldsymbol{v}_2=t_{1R}^*\boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{\tau}\left\lfloor\frac{q}{2}\right\rfloor(\mathrm{mod}\,q)$。如果这样的元组存在，返回消息 $m$，否则返回 $\perp$。

准备挑战签密文。第一阶段完成后，A 在消息空间中选择 2 个等长消息 $(m_0,m_1)$，连同任意发送者的公私钥对 $(\mathrm{pk}_S^*,\mathrm{sk}_S^*)$ 一起发送给挑战者 B，要求挑战者 B 以接收方公钥 $\mathrm{pk}_R^*=\{\boldsymbol{t}_{1R}^*,\boldsymbol{t}_{2R}^*\}$ 生成挑战密文。随后挑战者 B 随机选择一个比特 $\mathrm{bt}\in\{0,1\}$，做如下运算。

首先选择 $\boldsymbol{y}\leftarrow_{\$}\mathfrak{R}_{q,[\mathrm{B}]}$，计算 $b'^*=H_1(\lfloor\boldsymbol{a}_1\boldsymbol{y}\rceil_{d,q},\lfloor\boldsymbol{a}_2\boldsymbol{y}\rceil_{d,q},m_{\mathrm{bt}},\mathrm{pk}_S^*,\mathrm{pk}_R^*)$，编码 $\boldsymbol{b}^*=F(b'^*)$，计算 $\boldsymbol{z}^*=\boldsymbol{x}_S^*\boldsymbol{b}^*+\boldsymbol{y}^*$、$\boldsymbol{w}_1^*=\boldsymbol{a}_1\boldsymbol{y}^*-\boldsymbol{e}_{1S}^*\boldsymbol{b}^*$ 和 $\boldsymbol{w}_2^*=\boldsymbol{a}_2\boldsymbol{y}^*-\boldsymbol{e}_{2S}^*\boldsymbol{b}^*$。验证 $[\boldsymbol{w}_1^*]_{2^d},[\boldsymbol{w}_2^*]_{2^d}\in\mathfrak{R}_{q,[2^d-L]}$ 且 $\boldsymbol{z}^*\leftarrow\mathfrak{R}_{q,[\mathrm{B}-U]}$ 是否成立，如果不成立则重新开始并重复上述过程。

然后选取随机数 $\boldsymbol{\tau}^*\in\{0,1\}^n$，计算 $\mu^*=E_{H_2(\boldsymbol{\tau}^*)}(m_{\mathrm{bt}},\boldsymbol{z}^*,b'^*)$。

令 $\theta^*=H_3(\boldsymbol{\tau}^*,\mu^*)$，由 $\theta^*$ 的随机性选取错误向量 $\boldsymbol{e}_1^*,\boldsymbol{e}_2^*\leftarrow D_\sigma^n$ 和 $\boldsymbol{e}_3^*\leftarrow D_\sigma^n$，计算 $\boldsymbol{v}_1^*=\boldsymbol{a}_1\boldsymbol{e}_1^*+\boldsymbol{e}_2^*(\mathrm{mod}\,q)$，$\boldsymbol{v}_2^*=\boldsymbol{t}_{1R}^*\boldsymbol{e}_1^*+\boldsymbol{e}_3^*+\boldsymbol{\tau}^*\left\lfloor\frac{q}{2}\right\rfloor(\mathrm{mod}\,q)$。

返回 $c^*\leftarrow(\boldsymbol{v}_1^*,\boldsymbol{v}_2^*,\mu^*)$ 给敌手 A。

第二阶段解签密询问。敌手 A 重复第一阶段的询问过程，但是要求不能以公私钥对 $(\mathrm{pk}_S^*,\mathrm{sk}_S^*)$ 对挑战签密文 $c^*=(\boldsymbol{v}_1^*,\boldsymbol{v}_2^*,\mu^*)$ 进行询问，模拟者同第一阶段那样应答询问。

猜测阶段。敌手 A 输出 $\mathrm{bt}'\in\{0,1\}$ 作为对 bt 的猜测。

可以看出，上述模拟是完善的。当给定模拟者 B 的分布 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$ 恰好是来自分布 $A_{x,\chi}$，从敌手 A 视角看到的模拟过程与 bt 的分布，同真实的攻击是一致的，但是如果分布 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$ 都是 $\mathfrak{R}_q\times\mathfrak{R}_q$ 上的均匀随机分布，bt 的分布与敌手 A 的视角看到的分布在信息论上是独立的，于是模拟者完成了对判定性 $\mathrm{RLWE}_{q,n,2,\sigma}$ 问题的区分算法的构造。

如果 $\mathrm{bt}'=\mathrm{bt}$，B 获知分布 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$ 来自分布 $A_{x,\chi}$，否则分布 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$ 都是 $\mathfrak{R}_q\times\mathfrak{R}_q$ 上的均匀随机分布，判定性 $\mathrm{RLWE}_{q,n,2,\sigma}$ 问题得解。

上述过程中会使模拟不完善的唯一事件是合法签密文在解签密询问时被拒绝，它是由于对哈希询问 $(H_1,H_2,H_3)$ 的模拟不完善导致的。对于 $H_1$ 的询问模拟，该概率不超过 $\frac{q_{H_1}}{2^k}$；对于 $H_2$ 的询问模拟，该概率不超过 $\frac{q_{H_2}}{2^{f_2}}$；对于 $H_3$ 的询问模拟，该概率不超过 $\frac{q_{H_3}}{2^{f_3}}$。因此 B 攻破判定性 $\mathrm{RLWE}_{q,n,2,\sigma}$ 问题的优势为 $\varepsilon_{\mathrm{B}}\geqslant\varepsilon_{\mathrm{A}}\left[1-q_{\mathrm{DSC}}\left(\frac{q_{H_1}}{2^k}+\frac{q_{H_2}}{2^{f_2}}+\frac{q_{H_3}}{2^{f_3}}\right)\right]$。

下面，计算 B 的运行时间，由于 B 将 A 作为一个子过程使用，因此有 $t_{\mathrm{B}}>t_{\mathrm{A}}$。B 多出的运行时间是由于 B 要为 A 模拟 IND-CCA2 游戏。它主要包括 2 个获得挑战分布 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$ 询问的时间，以及模拟哈希询问、签密询问和解签密询问的时间。由于 B 模拟的签密文分布与真实签密算法的签密文分布是统计接近的，因此 B 拒绝一对签密文 $(\boldsymbol{v}_1,\boldsymbol{v}_2,\mu)$ 的概率和运行签密算法时拒绝的概率是

相同的。进一步地，忽略获得挑战的时间（非常小），以及高效的加法运算时间，签密与解签密的模拟过程可以看作由几次多项式乘法运算组成，多项式乘法运算时间复杂度为 $O(n^2)$，即签密与解签密平均每次询问的时间复杂度为 $O(n^2)$，由于询问次数的上界 $(q_{\mathrm{SC}},q_{\mathrm{DSC}},q_{H_1},q_{H_2},q_{H_3})$ 都是 $n$ 的多项式，因此可以得出近似的边界值 $t_{\mathrm{B}}\approx t_{\mathrm{A}}+O((q_{\mathrm{SC}}+q_{\mathrm{DSC}})n^2+q_{H_1}+q_{H_2}+q_{H_3})$。

证毕。

**定理 2**　认证性。在随机预言机模型下，如果存在着 SUF-CMA 敌手 A 在多项式时间 $t_{\mathrm{A}}$ 内，进行不多于 $q_{\mathrm{SC}}$ 次签密询问，不多于 $q_{\mathrm{DSC}}$ 次解签密询问，不多于 $q_{H_1}$ 次哈希预言机 $H_1$ 询问，$q_{H_2}$ 次哈希预言机 $H_2$ 询问，$q_{H_3}$ 次哈希预言机 $H_3$ 询问，以不可忽略的优势 $\varepsilon_{\mathrm{A}}$ 对 RLWE-SC 方案伪造一个合法的签密，那么存在着一个模拟者 D 在多项式时间 $t_{\mathrm{D}}\approx t_{\mathrm{A}}+O((q_{\mathrm{SC}}+q_{\mathrm{DSC}})n^2+q_{H_1}+q_{H_2}+q_{H_3})$ 内，攻破判定性 $\mathrm{RLWE}_{q,n,2,\sigma}$ 问题，其优势 $\varepsilon_{\mathrm{D}}\geqslant\varepsilon_{\mathrm{A}}\left(1-\dfrac{2^{2n(d+1)}q_{\mathrm{SC}}(q_{H_1}+q_{H_2})}{(2B+1)^n q^n}\right)-\dfrac{2^{2nd}(q_{H_1}+q_{H_2})(2B-2U+1)^n+(28\sigma+1)^{3n}}{q^{2n}}$。

**证明**　假设模拟者被给定 2 个 $\mathrm{RLWE}_{q,n,2,\sigma}$ 挑战对 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$，它以等概率服从 $\mathfrak{R}_q\times\mathfrak{R}_q$ 上的随机均匀分布，或者满足 $\boldsymbol{t}_1=\boldsymbol{a}_1\boldsymbol{x}+\boldsymbol{e}_{1R}$ 且 $\boldsymbol{t}_2=\boldsymbol{a}_2\boldsymbol{x}+\boldsymbol{e}_{2R}$（环上 LWE 分布 $A_{x,\chi}$），其中 $\boldsymbol{x},\boldsymbol{e}_{1R},\boldsymbol{e}_{2R}\leftarrow D_\sigma^n$，$\chi$ 表示 $\mathfrak{R}_q$ 上的高斯分布 $D_\sigma^n$。下面，描述模拟者 D 如何利用敌手 A 的信息为判定性 $\mathrm{RLWE}_{q,n,2,\sigma}$ 问题来构造一个区分算法，

准备公钥阶段。对于上述给定的参数和 2 个 $\mathrm{RLWE}_{q,n,2,\sigma}$ 挑战对 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$，D 设置 $(\boldsymbol{a}_1,\boldsymbol{a}_2)$ 作为方案的公开参数，并发送 $\mathrm{pk}_S^*=\{\boldsymbol{t}_{1S}^*=\boldsymbol{t}_1,\boldsymbol{t}_{2S}^*=\boldsymbol{t}_2\}$ 给 A。

哈希询问、签密询问与解签密询问同定理 1。

伪造阶段。询问阶段结束后，攻击者 A 输出了一对公私钥 $(\mathrm{pk}_R^*,\mathrm{sk}_R^*)$ 和伪造的签密文 $c^*=(\boldsymbol{v}_1^*,\boldsymbol{v}_2^*,\mu^*)$，并且要求 $c^*$ 没有进行过解签密询问。然后 D 验证伪造的签密文是否有效，如果解签密算法 $\mathrm{DSC}(c^*,\mathrm{pk}_S^*,\mathrm{sk}_R^*)$ 返回 $m$，D 输出 1，否则 D 输出 0。模拟者 D 完成了对 $\mathrm{RLWE}_{q,n,2,\sigma}$ 挑战区分器的构造。

可以看出，如果 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$ 来自分布 $A_{x,\chi}$，则 D 对哈希询问、签密及解签密询问模拟的应答同真实的随机预言机、签密与解签密预言机的应答是不可区分的；如果分布 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$ 都是 $\mathfrak{R}_q\times\mathfrak{R}_q$ 上的均匀随机分布，则敌手 D 的模拟同真实的攻击是信息论独立的（除模拟可能会终止外）。下面本文证明两点：模拟签密过程中随机选择的 $z$ 的分布同真实签密算法中 $\boldsymbol{z}$ 的分布是统计接近的；模拟终止的概率可以忽略。下面，分别给出具体描述。

1) 由文献[8]引理 1 容易得出，签密算法计算出的分布 $\boldsymbol{z}\in\mathfrak{R}_{q,[\mathrm{B}-U]}$ 同 $\mathfrak{R}_{q,[\mathrm{B}-U]}$ 上的均匀分布是统计上接近的，并且文献[8]定理 1 给出了详细证明过程，这里不再详述。

2) 假设签密模拟过程中在 $\mathfrak{R}_{q,[\mathrm{B}]}$ 上随机均匀地选择 $\boldsymbol{y}$，那么不仅有 $b'=H_1(\lfloor\boldsymbol{w}_1\rceil_{d,q},\lfloor\boldsymbol{w}_2\rceil_{d,q},m,\mathrm{pk}_S^*,\mathrm{pk}_R)$，而且满足 $b'=H_1(\lfloor\boldsymbol{a}_1\boldsymbol{y}\rceil_{d,q},\lfloor\boldsymbol{a}_2\boldsymbol{y}\rceil_{d,q},m,\mathrm{pk}_S^*,\mathrm{pk}_R)$。显然，模拟签密过程中终止的概率上界源于上述签密模拟过程中对真实签密的改变，它同发现一个冲突的概率是相同的。文献[8]定理 1 证明中给出了模拟终止的概率上界为 $\dfrac{2^{2n(d+1)}q_{\mathrm{SC}}(q_{H_1}+q_{H_2})}{(2B+1)^n q^n}$，并且进一步利用 RLWE 游戏中伪造者的优势，给出了模拟者区分给定挑战分布的下界为 $\varepsilon_{\mathrm{D}}\geqslant\varepsilon_{\mathrm{A}}\left(1-\dfrac{2^{2n(d+1)}q_{\mathrm{SC}}(q_{H_1}+q_{H_2})}{(2B+1)^n q^n}\right)-\dfrac{2^{2nd}(q_{H_1}+q_{H_2})(2B-2U+1)^n+(28\sigma+1)^{3n}}{q^{2n}}$，这里不再详述。

最后分析运行时间，方案中的运算都是高效的线性运算，可以看出敌手 A 的运行时间 $t_{\mathrm{A}}$ 同模拟者 D 的运行时间 $t_{\mathrm{D}}$ 是接近的。由于模拟者 D 将 A 作为一个子过程调用，因此 $t_{\mathrm{D}}\geqslant t_{\mathrm{A}}$。进一步地，D 所需要的额外时间主要是用于为 A 模拟不可伪造游戏，例如获得挑战元组 $(\boldsymbol{a}_1,\boldsymbol{t}_1)$ 和 $(\boldsymbol{a}_2,\boldsymbol{t}_2)$ 的时间，加上回答哈希询问、签密和解签密询问所需的时间。其中 D 模拟签密过程中拒绝一个对 $(\boldsymbol{v}_1,\boldsymbol{v}_2,\mu)$ 的概率与运行 SC 算法时的概率是相同的。进一步地，忽略高效的加法和数乘运算时间，以及获得挑战的时间，模拟签密与解签密过程由几个多项式乘法运

算组成，多项式乘法运算渐进时间复杂度为$O(n^2)$，即签密与解签密平均每次询问的时间复杂度为$O(n^2)$，因此总的运行时间近似为$t_{\mathrm{D}} \approx t_{\mathrm{A}} + O((q_{\mathrm{SC}} + q_{\mathrm{DSC}})n^2 + q_{H_1} + q_{H_2} + q_{H_3})$。

证毕。

### 4.4 效率分析

下面，分析本文方案与相关基于格的签密方案的效率对比，其中$l_{\mathrm{me}}$表示消息长度，$l_{\mathrm{ID}}$表示身份的比特长度，模数$q = \mathrm{poly}(k)$，$S_D$表示高斯采样运算，$S_T$表示带陷门的原像抽样，$l_r$表示LBK13中安全随机数$r$的比特长度，$M_v$表示矩阵向量乘法运算，$M_R$表示多项式环乘法运算。在运算量描述中，本文忽略了向量和多项式加法运算、哈希函数运算，以及环元素抽样等高效的运算。

YWWY13构造了一个同时满足IND-CCA2和SUF-CMA安全的格基签密方案，取参数$m = 2n\log q$（方案对$m$要求的下限值），方案公钥尺寸为$2n^2\log^2 q$，私钥尺寸为$\frac{1}{2}n^2\log q\log(\log n)$，密文量为$l_{\mathrm{me}} + 5n\log^2 q + 5n\log q$，签密需要$S_T + 5S_D + 3M_v$运算，解签密需要$6M_v$运算。

LBK13同YWWY13方案具有类似性质，但效率有较大的提高。具体地，取参数$m = 5n\log q$（方案对$m$要求的下限值），方案公钥尺寸为$5n^2\log^2 q$，私钥尺寸为$25n^2\log^2 q$，密文量为$l_{\mathrm{me}} + 5n\log^2 q + l_r$（其中$l_r$表示选取的随机数的比特长度，比$m$小得多，近似地也可以忽略），签密需要$S_T + M_v$运算，解签密需要$3M_v$运算。

SS18进一步提高了标准模型下满足IND-CCA2和SUF-CMA安全的格基签密方案的效率，但公私钥与密文的尺寸仍然较大。具体来说，取参数$m = 3n\log q$（SS18的方案分析中给定的$m$取值），方案公钥尺寸为$3n^2\log q$，私钥尺寸为$6n^3\log q\log n$，密文量达到$12n^2\log^2 q\log n + 3n\log q$，忽略一些效率较高的函数计算，签密需要$S_T + 5S_D + 6M_v$运算，解签密需要$S_T + 5M_v$运算（由于陷门的求逆运算至少需要两次矩阵乘法运算，这里用两次矩阵乘法运算来近似表示陷门求逆运算）。

LTT19改进了SS18的效率，但仍然是一个基于陷门的构造，密文量及运算量仍然较大。具体来说，公钥尺寸为$n\log q$，发送方私钥尺寸为$2n\left(1+\left\lfloor \log\left(7.02\sqrt{\frac{q}{2n}}\right)\right\rfloor\right)$，接收方私钥尺寸为$n\log q$，密文量为$l_{\mathrm{me}} + 5n\log q$，签密需要$S_T + 5S_D + 2M_v$运算，解签密需要$3M_v$运算。

LWWD16构造了一个无陷门的格基签密方案，取参数$m = 2n$（见方案描述），方案公钥尺寸为$2n^2\log q$，私钥尺寸为$n^2\log q$，密文量为$l_{\mathrm{me}} + 4n\log q$，签密需要$4S_D + 6M_v$运算，解签密需要$3M_v$运算。

FK18以密钥交换（KEX）的方式和密钥封装（KEM）的方式构造了2个无陷门的格基签密方案，它们都是在环上构造的，具有较高的效率。具体来说，2种方案公私钥尺寸、签密和解签密运算量相同，公钥尺寸为$2n\log q$，私钥尺寸为$3n\log q$，签密运算量主要为$8M_R$（忽略了环元素抽样运算），解签密运算量主要为$5M_R$。KEX构造的密文量为$l_{\mathrm{me}} + 2n\log q + l_{\mathrm{HR}}$，其中$l_{\mathrm{HR}}$表示调和函数HelpRec的输出；KEM构造的密文量为$l_{\mathrm{me}} + 3n\log q$。方案在随机预言机模型下认证性上达到了SUF-CMA安全，然而在机密性上只达到了IND-CPA安全。

LHY19改进了FK18的构造，将方案的机密性提高到IND-CCA2安全，但在密文量和计算量上都做出了较大牺牲。具体来说，公钥尺寸为$2n\log q$，私钥尺寸为$3n\log q$，密文量为$l_{\mathrm{me}} + 5n\log q$，签密需要$3S_D + 12M_R$运算，解签密需要$5M_R$运算。

本文基于环上困难问题构造了一个无陷门的格基签密方案，其公私钥尺寸与FK18相同，密文量为$l_{\mathrm{me}} + 5n\log q$，签密运算量主要为$3S_D + 7M_R$（忽略了环元素抽样运算），解签密运算量主要为$5M_R$。本文方案在随机预言机模型下机密性和认证性分别达到了IND-CCA2和SUF-CMA安全性。

相关基于格的标准签密方案的效率对比如表1所示。典型地，本文取$n = 1\,024$，$q = 2^{24}$，$l_{\mathrm{me}} = 10^5$，相关基于格的标准签密方案的公私钥尺寸及密文量对比如表2所示。

从表1和表2的效率比较可以看出，与陷门方案YWWY13、LBK13、SS18和LTT19相比，本文

**表 1**　　**相关基于格的标准签密方案的效率对比**

| 构造 | 方案 | 公钥 | 私钥 | 密文 | 签密运算 | 解签密运算 | 安全性 |
|---|---|---|---|---|---|---|---|
| 陷门 | YWWY13 | $2n^2\log^2 q$ | $\frac{1}{2}n^2\log q\log(\log n)$ | $l_{\text{me}}+5n\log^2 q+5n\log q$ | $S_T+5S_D+3M_v$ | $6M_v$ | IND-CCA2SUF-CMA（标准模型） |
| | LBK13 | $5n^2\log^2 q$ | $25n^2\log^2 q$ | $l_{\text{me}}+5n\log^2 q+l_r$ | $S_T+M_v$ | $3M_v$ | IND-CCA2SUF-CMA（随机预言机模型） |
| | SS18 | $3n^2\log q$ | $6n^3\log q\log n$ | $12n^2\log^2 q\log n+3n\log q$ | $S_T+5S_D+6M_v$ | $S_T+5M_v$ | IND-CCA2SUF-CMA（标准模型） |
| | LTT19 | $n\log q$ | $2n\left(1+\left\lfloor\log\left(7.02\sqrt{\frac{q}{2n}}\right)\right\rfloor\right)$（发送方）<br>$n\log q$（接收方） | $l_{\text{me}}+5n\log q$ | $S_T+5S_D+2M_v$ | $3M_v$ | IND-CCA2SUF-CMA（标准模型） |
| 无陷门 | LWWD16 | $2n^2\log q$ | $n^2\log q$ | $l_{\text{me}}+4n\log q$ | $4S_D+6M_v$ | $3M_v$ | IND-CCA2EUF-CMA（随机预言机模型） |
| | FK18(KEX) | $2n\log q$ | $3n\log q$ | $l_{\text{me}}+2n\log q+l_{\text{HR}}$ | $8M_R$ | $5M_R$ | IND-CPASUF-CMA（随机预言机模型） |
| | FK18(KEM) | $2n\log q$ | $3n\log q$ | $l_{\text{me}}+3n\log q$ | $8M_R$ | $5M_R$ | |
| | LHY19 | $2n\log q$ | $3n\log q$ | $l_{\text{me}}+5n\log q$ | $l_{\text{me}}+5n\log q$ | $5M_R$ | IND-CCA2SUF-CMA（随机预言机模型） |
| | 本文方案 | $2n\log q$ | $3n\log q$ | $l_{\text{me}}+4n\log q$ | $3S_D+7M_R$ | $5M_R$ | IND-CCA2SUF-CMA（随机预言机模型） |

**表 2**　　**相关基于格的标准签密方案的公私钥尺寸及密文量大小对比**

| 构造 | 方案 | 公钥 | 私钥 | 密文 |
|---|---|---|---|---|
| 陷门 | YWWY13 | $1.2\times10^9$ | $4.2\times10^7$ | $3.2\times10^6$ |
| | LBK13 | $3\times10^9$ | $1.5\times10^{10}$ | $3.0\times10^6$ |
| | SS18 | $5\times10^7$ | $1.5\times10^{12}$ | $7.2\times10^{10}$ |
| | LTT19 | $2.5\times10^4$ | $2.5\times10^4$（发送方）<br>$2.0\times10^4$（接收方） | $2.22\times10^5$ |
| 无陷门 | LWWD16 | $5\times10^7$ | $2.5\times10^7$ | $1.98\times10^5$ |
| | FK18(KEX) | $4.9\times10^4$ | $7.3\times10^4$ | $1.49\times10^5$ |
| | FK18(KEM) | $4.9\times10^4$ | $7.3\times10^4$ | $1.73\times10^5$ |
| | LHY19 | $4.9\times10^4$ | $7.3\times10^4$ | $2.22\times10^5$ |
| | 本文方案 | $4.9\times10^4$ | $7.3\times10^4$ | $1.98\times10^5$ |

方案具有更高的计算和通信效率；与无陷门同类方案相比，在计算效率方面，本文方案高于 LHY19，同 LWWD16 相近，略低于 FK18，但由于不包含复杂的陷门产生和原像抽样运算，上述无陷门的签密方案计算效率都较高。在通信效率方面，本文方案要高于 LHY19 和 LWWD16，略低于 FK18。值得注意的是，FK18 在机密性上只实现了 IND-CPA 安全性，而本文方案达到了更高的 IND-CCA2 安全性。

目前，将 IND-CPA 安全的方案转换成 IND-CCA2 安全的方案有 2 种通用方法[26]，一种方法是利用一次签名技术，另一种方法是利用承诺函数和消息认证码。为了效率比较更直观，本文利用基于格的一次签名技术将 FK18 转换成 IND-CCA2 安全的方案，其中强不可伪造的一次签名方案采用经典的 LM08 方案[27]，用 $l_H$ 表示一次签名方案哈希函数的输出长度，转换后的效率对比如表 3 所示。

从表 3 可以看出，FK18 转换成 IND-CCA2 安全的方案后，在计算效率和通信效率方面都显著低于本文方案。综上，本文方案在同等安全强度下具有较高的效率。

### 4.5　实验与性能分析

本文将上述 RLWE-SC 方案进行了编程实现，

**表 3 FK18 转换成 IND-CCA2 安全的方案与本文方案效率对比**

| 方案 | 公钥 | 私钥 | 密文 | 签密运算 | 解签密运算 |
|---|---|---|---|---|---|
| FK18（KEX）+LM08 | $2n\log q$ | $3n\log q$ | $l_{\text{me}}+2n\log q+l_{\text{HR}}+n\lceil\log n\rceil\log q+2l_H\lceil\log n\rceil$ | $8M_R+\lceil\log n\rceil M_R$ | $5M_R+\lceil\log n\rceil M_R$ |
| FK18（KEM）+LM08 | $2n\log q$ | $3n\log q$ | $l_{\text{me}}+3n\log q+n\lceil\log n\rceil\log q+2l_H\lceil\log n\rceil$ | $8M_R+\lceil\log n\rceil M_R$ | $5M_R+\lceil\log n\rceil M_R$ |
| 本文方案 | $2n\log q$ | $3n\log q$ | $l_{\text{me}}+4n\log q$ | $3S_D+7M_R$ | $5M_R$ |

实验环境为 1.8GHz 的 4 核 64 位 Intel(R) Core(TM)i7- 8565U 处理器、8GB 固态硬盘、Windows 10 操作系统的笔记本，实验平台为 Visual Studio2017，实验语言为 C 语言。方案的参数取定 $n=1\,024$，$q=343\,576\,577$，$\omega=19$，$B=524\,287$，$\sigma=30$，$L=2\,766$，$d=23$，$U=3\,173$，对称加密算法为 128 位 DES 算法的 CBC 模式，哈希函数为 SHA128 及其变种。

RLWE-SC 方案主要耗时的计算为拒绝抽样函数、多项式乘法运算及对称加密，本文采用了文献[7]提供的库函数对拒绝抽样和多项式乘法运算进行了优化，其中对多项式乘法运算采用了数论转换（NTT, number theoretic transform）和稀疏多项式乘法快速算法，详见文献[7]第 5 节。

实验过程中，本文采用 CPU 时钟周期计数来表示运行时间（精度更高），采取运行算法 5000 次取平均值的方法（减少误差）来获得实验结果，并对消息 $m$ 的长度取不同的值，在 Release 编译模式下得到的实验结果如图 1 所示。

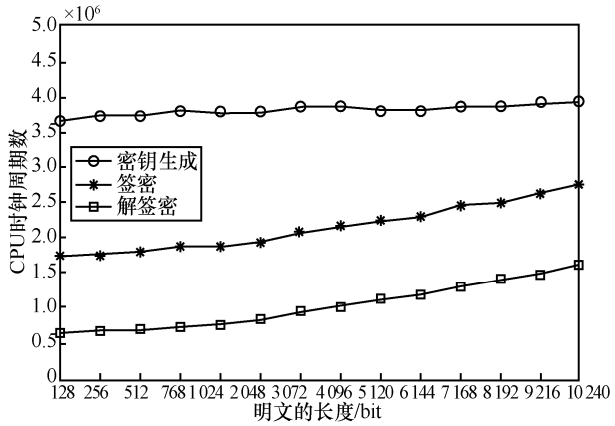



图 1 RLWE-SC 方案 Release 模式下的执行效率

图 1 的实验数据表明，签密算法耗时从某一个初值开始随消息长度增大呈缓慢的增长趋势。由于 RLWE-SC 签密方案耗时的计算可以看成由签名和对称加密 2 个部分组成，签名部分是对消息取固定长度的哈希值后进行签名，因此签名受消息长度影响很少。当消息较短时，对称加密耗时较少，此时签密耗时主要体现签名的时间；当消息长度逐渐增加时，对称加密耗时与消息长度呈线性递增，签名的耗时几乎不变，此时签密耗时逐渐受对称加密影响，同消息长度呈缓慢的线性递增。可以看出，实验结果同理论是一致的。

进一步地，本文将 RLWE-SC 方案与目前较高效的相关环上无陷门签密方案 FK18（包括 KEX 和 KEM 这 2 个构造）以及 LHY19 方案进行比较。由于 RLWE-SC 是 IND-CCA2 安全的，FK18 的 KEX 构造和 KEM 构造都是 IND-CPA 安全的，本文采用环上一次签名方案 LM08 将其转换成 IND-CCA2 安全的方案后进行了编程实现，实验环境同上述 RLWE-SC，实验过程中同样采用了 ABB16 提供的库函数对拒绝抽样和多项式乘法运算进行了优化，取消息 $m$ 的长度为 1024 位，在 Release 编译模式下得到的实验结果如图 2 所示。

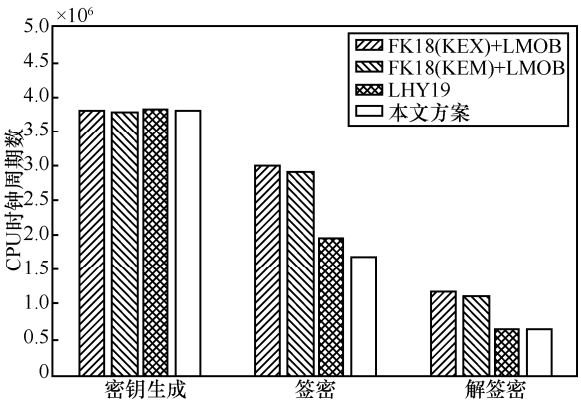



图 2 相关方案 Release 模式下执行效率对比

图 2 的实验数据表明，将 FK18 转换成与本文 RLWE-SC 方案同等安全强度后，本文的 RLWE-SC 方案与 FK18 的 2 种方案相比，密钥生成的耗时相近，签密与解签密耗时显著减少。本文的 RLWE-SC 方案与 LHY19 方案相比，密钥生成和解签密的耗时相近，签密耗时减少。

## 5　结束语

随着量子计算的突飞猛进，抗量子攻击的密码已经成为研究热点，格的功能强大、构造力丰富、计算效率高，是抗量子攻击密码最具影响力的代表。基于格的加密和签名方案成果丰硕，但基于格的签密研究成果并不充分。本文基于环上的判定性 LWE 问题构造了一个标准签密方案，该方案在机密性和认证性方面分别达到了 IND-CCA2 和 SUF-CMA 安全性。效率分析表明，本文方案的构造没有用到复杂的陷门产生及原象抽样运算，与其他基于格的签密方案相比，在同等安全强度下具有较高的效率。

## 参考文献：


[1] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption) <<cost (signature) + cost (encryption)[C]//Annual International Cryptology Conference. Berlin: Springer, 1997: 165-179.

[2] ZHENG Y, IMAI H. How to construct efficient signcryption schemes on elliptic curves[J]. Information Processing Letters, 1998, 68(5): 227-233.

[3] STEINFELD R, ZHENG Y. A signcryption scheme based on integer factorization[C]//International Workshop on Information Security. Berlin: Springer, 2000: 308-322.

[4] MICCIANCIO D. Lattice-based cryptography[J]. Encyclopedia of Cryptography and Security, 2011: 713-715.

[5] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM, 2013, 60(6): 43.

[6] LYUBASHEVSKY V. Lattice signatures without trapdoors[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 738-755.

[7] AKLEYLEK S, BINDEL N, BUCHMANN J, et al. An efficient lattice-based signature scheme with provably secure instantiation[C]//International Conference on Cryptology in Africa. Berlin: Springer, 2016: 44-60.

[8] WANG F, HU Y, WANG C. Post-quantum secure hybrid signcryption-from lattice assumption[J]. Applied Mathematics & Information Sciences, 2012, 6(1): 23-28.

[9] FAGEN L, FAHAD T,BIN M, et al. Lattice-based signcryption[J]. Concurrency and Computation: Practice and Experience, 2013, 25(14): 2112-2122.

[10] YAN J, WANG L, WANG L, et al. Efficient lattice-based signcryption in standard model[J]. Mathematical Problems in Engineering, 2013, 2013:1-18.

[11] LU X, WEN Q, JIN Z, et al. A lattice-based signcryption scheme without random oracles[J]. Frontiers of Computer Science, 2014, 8(4): 667-675.

[12] BAI S, GALBRAITH S D. An improved compression technique for signatures based on learning with errors[C]//Cryptographers' Track at the RSA Conference. Berlin: Springer, 2014: 28-47.

[13] LU X, WEN Q, WANG L, et al. A lattice-based signcryption scheme without trapdoors [J]. Journal of Electronics and Information, 2016, 38 (9): 2287-2293.

[14] GERARD F, MERCKX K. Setla: signature and encryption from lattices[C]//International Conference on Cryptology and Network Security. Berlin:Springer, 2018: 299-320.

[15] ALKIM E, DUCAS L, PÖPPELMANN T, et al. Post-quantum key exchange—a new hope[C]//25th USENIX Security Symposium (USENIX Security 2016). Berkeley: USENIX Association, 2016: 327-343.

[16] SATO S, SHIKATA J, Lattice-based signcryption without random oracles[C]//International Conference on Post-Quantum Cryptography(PQCrypto2018). Berlin: Springer, 2018:331-351.

[17] LIU Z Y, TSO R, TSENG Y F, et al. Signcryption from NTRU lattices without random oracles[C]//14th Asia Joint Conference on Information Security (AsiaJCIS2019). Piscataway: IEEE Press, 2019: 134-141.

[18] DEL P R, LYUBASHEVSKY V, POINTCHEVAL D. The whole is less than the sum of its parts: constructing more efficient lattice-based AKEs[C]//International Conference on Security and Cryptography for Networks. Berlin: Springer, 2016: 273-291.

[19] ZHANG Y H, HU Y, XIE J, et al. Efficient ring signature schemes over NTRU lattices[J]. Security and Communication Networks, 2016, 9(18): 5252-5261.

[20] YANG X, CAO H, LI W, et al. Improved lattice-based signcryption in the standard model[J]. IEEE Access, 2019, 7: 155552-155562.

[21] LIU Z, HAN Y L, YANG X Y. A signcryption scheme based learning with errors over rings without trapdoor[C]//National Conference of Theoretical Computer Science. Berlin: Springer, 2019: 168-180.

[22] FUJISAKI E, OKAMOTO T. Secure integration of asymmetric and symmetric encryption schemes[J]. Journal of Cryptology, 2013, 26(1): 80-101.

[23] APPLEBAUM B, CASH D, PEIKERT C, et al. Fast cryptographic primitives and circular-secure encryption based on hard learning problems[C]//Annual International Cryptology Conference. Berlin: Springer, 2009: 595-618.

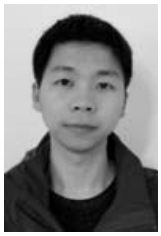
[24] HUANG Q, WONG D S, ZHAO Y. Generic transformation to strongly unforgeable signatures[C]//International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2007: 1-17.

[25] AN J H, DODIS Y, RABIN T. On the security of joint signature and encryption[C]//In Proceedings Advances inCryptology-EUROCRYPT 2002, LNCS 2332. Berlin: Springer, 2002: 83-107.

[26] NANDI M, PANDIT T. Generic conversions from CPA to CCA secure functional encryption[J]. IACR Cryptology ePrint Archive, 2015, 2015: 457.

[27] LYUBASHEVSKY V, MICCIANCIO D. Asymptotically efficient lattice-based digital signatures[C]//Theory of Cryptography Conference. Berlin: Springer, 2008: 37-54.


[作者简介]




**刘镇**（1985– ），男，湖南衡南人，武警工程大学讲师、博士生，主要研究方向为公钥密码算法、可证明安全等。

**韩益亮**（1977– ），男，甘肃会宁人，博士，武警工程大学教授，主要研究方向为密码学、隐私保护、社交网络分析等。

**杨晓元**（1959– ），男，湖南湘潭人，武警工程大学教授，主要研究方向为密码学、信息安全等。

**柳曙光**（1976– ），男，山东栖霞人，武警工程大学副教授，主要研究方向为计算机应用、信息安全等。