一种基于环上LWE的广义签密方案

刘 镇,吴立强,韩益亮,杨晓元,柳曙光
(武警工程大学武警部队网络与信息安全保密重点实验室,陕西西安 710086)

摘 要: 广义签密可以灵活地工作在签密、签名和加密三种模式,具有很强的实用性.本文结合基于格的签名方案和密钥交换协议,构造了一个无陷门的广义签密方案.方案构造中引入了区分函数,根据输入的发送方与接收方密钥情况来自动识别加密、签名和签密三种模式,保障了算法在这三种工作模式下的优美对称性.基于环上判定性LWE问题,并借鉴FO13的方法,证明了该方案满足自适用抗选择密文攻击不可区分性安全性(IND-CCA2)和自适用抗选择消息攻击强不可伪造性安全性(SUF-CMA).该方案是基于Fiat-Shamir的中止(abort)框架,没有用到复杂的原像抽样和陷门生成算法,具有较高的计算效率.

关键词: 广义签密;环上的带错学习问题;无陷门格基签密;区分函数;抗量子攻击
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2021) 07-1314-09
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20190978

A Generalized Signcryption Scheme Based on LWE over Rings

LIU Zhen, WU Li-qiang, HAN Yi-liang, YANG Xiao-yuan, LIU Shu-guang
(*Key Laboratory of Network and Information Security, Engineering University of Chinese Armed Police Force, Xi'an, Shaanxi* 710086, *China*)

Abstract: Generalized signcryption can run flexibly in three modes: signcryption, signature and encryption, and has strong practicability.This paper combines lattice-based signature scheme and key exchange protocol to construct a trapdoor-free generalized signcryption scheme.In the construction, a distinguishing function is introduced, which automatically identifies the three modes of encryption, signature and signcryption according to the key conditions of the sender and the receiver. This ensures the excellent symmetry of the algorithm in these three modes.Finally, based on the deterministic learning with errors (LWE) problem on the ring, itused the method of FO13 toprove that the scheme satisfies the indistinguishability against adaptive chosen ciphertext attack (IND-CCA2) security and the strong unforgeability against choosing message attack (SUF-CMA) security.It is based on Fiat-Shamir with abort framework which does not use complex preimage sample algorithmand trapdoor generation algorithm, so it has high computational efficiency.

Key words: generalized signcryption;learning with errors on rings;trapdoor-free lattice-based signcryption;discernibility function;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一步.同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.随后签密成为了一个研究热点,大量的签密方案相继提出.尽管如此,但是有些场合往往有时只需要保障机密性或认证性中的某一个.Zheng建议此时可以分别采用加密或者签名算法来解决,也就是说实际应用中需要同时包含三个密码学原语:加密、签名和签密.在许多资源受限的场景中,例如嵌入式系统和传感器网络等,这种方法显然会大大增加系统开销,是不可行的.

2006年,韩等人提出了一个新的密码学原语,广义签密[2],它可以根据应用需求,分别工作在签密、签名和加密三种模式.随后出现了许多广义签密相关研究成果[3-6].然而这些方案都是基于耗时的双线配性对来实现的,其

收稿日期:2019-09-27;修回日期:2020-08-12;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61572521,No.U1636114,No.61772550);武警工程大学创新团队科学基金(No.KYTD201805);陕西省自然科学基础研究计划(No.2021JM-252);武警工程大学基础研究基金(No.WJY2019014)

安全性都可以归结到离散对数和大整数因子分解问题.

随着量子计算的不断发展,传统的基于离散对数和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,引起了学界广泛兴趣.它具有计算效率高,构造功能灵活等诸多优点,更是抗量子攻击密码最重要的成员之一.近些年来基于格的加密[7]和签名[8,9]相关成果不断涌现,然而基于格的签密研究成果并不丰富,WHW12[10]首次采用混合签密的思路构造了一个格签密方案,随后YWWY13[11]、LWJ14[12]和SS18[13]分别构造了标准模型下的格签密方案,但效率较低.LTT19[14]结合NTRU密钥封装机制与NTRU的签名方案,构造了一个基于NTRU的签密方案,提高了格签密方案的效率,LWWD16[15]构造了一个无陷门的格签密方案,避免了使用复杂的陷门产生和原像抽样运算,该方案具有较高的效率.然而到目前还未见基于格的广义签密相关成果.

结合ABB16[8]的ring-TESLA签名方案和ADP16[7]的密钥交换协议,并借鉴FO13[16]的转换方法,基于环上LWE问题,我们首次构造了一个无陷门的广义签密方案.方案构造中,我们引入了区分函数,根据输入的发送方与接收方密钥情况来自动识别加密、签名和签密三种模式,保障了算法在这三种工作模式下的优美对称性.最后基于环上判定性LWE问题,我们证明了该方案满足选择密文攻击不可区分性安全性(IND-CCA2)和选择消息攻击强不可伪造性安全性(SUF-CMA).本文的方案是基于Fiat-Shamir的中止(abort)框架,没有用到复杂的带陷门的原像抽样和求逆运算,具有很高的计算效率.

2　相关基础知识

2.1　符号说明

设$\mathbb{R},\mathbb{Z},\mathbb{N}$分别表示实数集、自然数集和整数集,对于$k\in\mathbb{N}$,我们定义$n=2^k\in\mathbb{N}$,素数$q\in\mathbb{N}$,满足$q=1(\mathrm{mod}2n)$.所有的对数运算都是以2为底数,$\mathbb{Z}_q$表示有限域$\mathbb{Z}/q\mathbb{Z}$.定义环$\mathcal{R}=\mathbb{Z}[x]/x^n+1$,有单位元的环用$\mathcal{R}^\times$表示,环$\mathcal{R}_q=\mathbb{Z}_q[x]/x^n+1,\mathcal{R}_{q,B}=\left\{\sum_{i=0}^{n-1}a_ix^i\in\mathcal{R}_q|i\in[0,n-1],a_i\in[-B,B]\right\}$,其中$B\in[0,q/2]$,定义$\mathcal{B}_{n,\omega}=\{v\in\{0,1\}^n|\|v\|^2=\omega\}$.我们用小写字母来表示多项式,用黑体小写字母来表示向量,用黑体大写字母来表示矩阵.对于向量$\boldsymbol{x}$,用$||\boldsymbol{x}||$来表示向量的欧氏范数.用$O(\cdot)$来表示复杂度函数.

设$\mathcal{A}$是一个随机算法,$y\leftarrow\mathcal{A}(x)$表示算法$\mathcal{A}$输入$x$,输出$y$.设$\mathcal{O}$是一个随机预言机,$\mathcal{A}^{\mathcal{O}}$表示算法$\mathcal{A}$可以访问$\mathcal{O}$.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,我们把抽样一个多项式$a\in\mathcal{R}$的所有系数也用$a\leftarrow D_\sigma^n$来表示.对于一个有限集合$S$,用$s\leftarrow\mathcal{U}(S)$或者简式$s\leftarrow{}_\$S$来表示随机均匀从$S$中抽样一个元素$s$.

舍入运算:对于$d\in\mathbb{N},c\in\mathbb{Z}$,用$[c]_{2^d}$来表示$c\mathrm{mod}\,2^d$在区间$(-2^{d-1},2^{d-1}]$中的唯一值,我们定义舍入运算$\lfloor\cdot\rceil_d:\mathbb{Z}\to\mathbb{Z},c\mapsto\left(c-[c]_{2^d}\right)/2^d$.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$v\left(\mathrm{mod}q\right)_d$的缩写成$v_{d,q}$.

2.2　环上的LWE问题

定义1(环上LWE分布)　设n,q为正整数,$s\in\mathcal{R}_q$,χ是环$\mathcal{R}$上的某个分布,均匀随机选取$a\leftarrow\mathcal{R}_q$,选取$e\leftarrow\chi$,则称$A_{s,\chi}=(a,t=as+e)$为环$\mathcal{R}_q\times\mathcal{R}_q$上的LWE分布.

定义2(环上的判定性LWE问题)　设n,q,k为正整数,$q=2^k$,χ是环$\mathcal{R}$上的某个分布,$\mathcal{O}_\chi$是一个随机预言机,当输入$s\in\mathcal{R}_q$,它返回一个抽样$A_{s,\chi}$.我们称一个判定性环上带差错学习问题R-LWE$_{q,n,m,\chi}$是(t,ε)困难的,如果对于任意概率多项式时间(PPT)算法$\mathcal{A}$,运行时间为t,最多进行m次预言机$\mathcal{O}_\chi$询问,下面等式成立:

$$Adv_{n,q,\chi}^{\mathrm{R-LWE}}(\mathcal{A})=\left|\Pr\left[\mathcal{A}^{\mathcal{O}_\chi(s)}=1\right]-\Pr\left[\mathcal{A}^{\mathcal{U}\left(\mathcal{Z}_q^n\times\mathcal{Z}_q\right)}=1\right]\right|\leqslant\varepsilon$$

其中$s\leftarrow\mathcal{U}\left(\mathcal{R}_q\right)$是一次选取的,$A_{s,\chi}$是随机选取的.

ACP09[17]证明了即使秘密分布s同错误分布χ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χ为标准差为σ的离散高斯分布,我们用R-LWE$_{q,n,m,\sigma}$来表示.

3　基于环上LWE问题的广义签密(RLWE-GSC)

设λ为安全参数,parm$=\{n,\omega,d,B,q,U,L,k\}$为公开参数,其中$n\in\mathbb{N}$满足$n>k>\lambda$.$D_\sigma$表示标准差为$\sigma$的高斯分布,$H:\{0,1\}^*\to\{0,1\}^k$为哈希函数,$G:\{0,1\}^*\to\{0,1\}^k$为随机预言机.$f:\{0,1\}^*\to\{0,1\}$为区分函数,满足

$$f(x)=\begin{cases}0, & x=0\\ 1, & x\neq 0\end{cases}$$

$F:\{0,1\}^k\to\mathcal{B}_{n,\omega}$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ω长度为n的向量,更多编码函数的描述可见文献[9].进一步地,设$a_1,a_2\in\mathcal{R}_q^\times$是环上两个随机均匀抽样,它们为方案公开的全局常

量. CheckE为拒绝抽样(rejection sampling)条件检测函数:对多项式e_S,设函数$\max_k\left(e_S\right)$返回e_S第k个最大系数值(第k大系数值),如果$\sum_{k=1}^{\omega}\max_k\left(e_S\right)>L$,$\mathrm{CheckE}\left(e_S\right)$返回1,否则返回0. 设定参数$L$满足$\left(1-2L/2^d\right)^{2n}\geqslant 0.4$,其描述详见ABB16. 本文借鉴了ADP16的方法来实现密钥封装,他们定义了一对调和函数HelpRec和Rec来计算k比特的调和信息用于密钥交换,关于调和函数HelpRec和Rec的构造详见ADP16.

发送方S将消息m签密后发送给接收方R,接收方R解密获得消息m,用$\varnothing$表示空集,签密算法具体如下.

3.1 密钥生成算法

$\left(\mathrm{pk}_S,\mathrm{sk}_S\right)\leftarrow\mathrm{KeyGen}\left(S,\mathrm{parm}\right)$:

如果$S\in\varnothing$,则$x_S\leftarrow 0,e_{S1}\leftarrow 0,e_{S2}\leftarrow 0$,否则随机选取$x_S,e_{S1},e_{S2}\leftarrow D_\sigma^n$,满足$\mathrm{CheckE}\left(e_{S1}\right)\neq 0\vee\mathrm{CheckE}\left(e_{S2}\right)\neq 0$;

计算$t_{S1}=a_1x_S+e_{S1}\left(\mathrm{mod}q\right)$和$t_{S2}=a_2x_S+e_{S2}\left(\mathrm{mod}q\right)$;

令$\mathrm{sk}_S\leftarrow\left\{x_S,e_{S1},e_{S2}\right\}$,$\mathrm{pk}_S\leftarrow\left\{t_{S1},t_{S2}\right\}$;

返回$(\mathrm{pk}_S,\mathrm{sk}_S)$.

$(\mathrm{pk}_S,\mathrm{sk}_S)\leftarrow\mathrm{KeyGen}\left(R,\mathrm{parm}\right)$:

如果$R\in\varnothing$,则$x_R\leftarrow 0,e_{R1}\leftarrow 0,e_{R2}\leftarrow 0$,否则随机选取$x_R,e_{R1},e_{R2}\leftarrow D_\sigma^n$,满足$\mathrm{CheckE}\left(e_{R1}\right)\neq 0\vee\mathrm{CheckE}\left(e_{R2}\right)\neq 0$;

计算$t_{R1}=a_1x_R+e_{R1}\left(\mathrm{mod}q\right)$和$t_{R2}=a_2x_R+e_{R2}\left(\mathrm{mod}q\right)$;

令$\mathrm{sk}_R\leftarrow\left\{x_R,e_{R1},e_{R2}\right\}$,$\mathrm{pk}_R\leftarrow\{t_{R1},t_{R2}\}$;

返回$(\mathrm{pk}_R,\mathrm{sk}_R)$.

3.2 签密算法

$C\leftarrow\mathrm{GSC}\left(m,\mathrm{pk}_R,\mathrm{sk}_S\right)$:

随机选择$y\leftarrow_{\$}\mathcal{R}_{q,[B]}$,$y',y''\leftarrow D_\sigma^n$,计算$c'\leftarrow H\left(a_1y_{d,q},a_2y_{d,q},m,\mathrm{pk}_S,\mathrm{pk}_R\right)$,编码$c=F(c')$,计算$z\leftarrow\left(x_Sc+y\right)\cdot f\left(\mathrm{sk}_S\right)$,$w_1\leftarrow a_1z-e_{s1}c$和$w_2\leftarrow a_2z-e_{s2}c$,如果$z\neq 0$,验证$\left[w_1\right]_{2^d},\left[w_2\right]_{2^d}\in\mathcal{R}_{q,2^d-L}\vee z\in\mathcal{R}_{q,[B-U]}$是否满足,不满足则重选随机数$y$并重复以上步骤;

计算$v_1\leftarrow a_1y+y',v_2\leftarrow t_{R1}y+y'',u\leftarrow\mathrm{HelpRec}\left(v_2\right)$;

然后计算

$$K\leftarrow G\left(v_1,u,\mathrm{Rec}\left(v_2,u\right),\mathrm{pk}_S,\mathrm{pk}_R\right)\cdot f\left(\mathrm{pk}_R\right)$$

和$\mathcal{E}\leftarrow\left(m||z||c'\right)\oplus K$,

返回$C\leftarrow\left(v_1,u,\mathcal{E}\right)$.

3.3 解签密算法

$m\leftarrow\mathrm{GDSC}\left(C,\mathrm{pk}_S,\mathrm{sk}_R\right)$:

计算

$$K\leftarrow G\left(v_1,u,\mathrm{Rec}\left(x_Rv_1,u\right),\mathrm{pk}_S,\mathrm{pk}_R\right)\cdot f\left(\mathrm{pk}_R\right),$$

计算$m||z||c'\leftarrow\mathcal{E}\oplus K$,

如果$z=0$,返回m;

否则编码$c=F(c')$,计算$w_1\leftarrow a_1z-t_{s1}c$和$w_2\leftarrow a_2z-t_{s2}c$,然后验证$c'=H\left(w_{1\,d,q},w_{2\,d,q},m,\mathrm{pk}_S,\mathrm{pk}_R\right)$和$z\in\mathcal{R}_{q,[B-U]}$是否成立,如果成立返回$m$,否则返回$\perp$.

3.4 公开可验证性

本方案是一个标准模型下可验证签密方案,从而可信的第三方可以解决发送方抵赖问题,即发送方某个由他生成的签密文. 当签名(z,c')公布后,可信第三方做如下运算:

编码$c=F(c')$,计算$w_1\leftarrow a_1z-t_{s1}c$和$w_2\leftarrow a_2z-t_{s2}c$,然后验证$c'=H\left(w_{1\,d,q},w_{2\,d,q},m,\mathrm{pk}_S,\mathrm{pk}_R\right)$和$z\in\mathcal{R}_{q,[B-U]}$是否成立,如果成立返回$m$,否则返回$\perp$.

3.5 签名模式和加密模式

当接收方$R\in\varnothing$,则$\mathrm{pk}_R=\{0,0\}$,于是有$f\left(\mathrm{pk}_R\right)=0$,该签密方案退化成ring-TESLA[8]签名方案,$m||z||c'\leftarrow\mathrm{GSC}\left(m,\mathrm{pk}_\phi,\mathrm{sk}_S\right)$;

当发送方$S\in\varnothing$,则$\mathrm{sk}_S\leftarrow\{0,0,0\}$,于是有$f\left(\mathrm{sk}_S\right)=0$,该签密方案退化成加密方案,$\left(v_1,u,\mathcal{E}\right)\leftarrow\mathrm{GSC}\left(m,\mathrm{pk}_R,\mathrm{sk}_\phi\right)$.

3.6 参数选择

结合ABB16及ADP16我们给出方案参数的取值范围. 选取参数ω使得不等式$2^k\geqslant\left|\mathcal{B}_{n,\omega}\right|=2^\omega\binom{k}{\omega}\geqslant 128$成立,令$U=14\sigma\sqrt{\omega},B\geqslant 14\sigma(n-1)\sqrt{\omega},M=\left(\frac{2(B-U)+1}{2B+1}\right)^n$.

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$1\leqslant\alpha\leqslant 1$,模数$q\geqslant\left(\frac{2^{k+2n(d+1)}}{(2B)^n}\right)^{1/n}$且$q\geqslant 4B$,令$\sigma=\alpha q$.

4 方案分析

4.1 正确性

(1) 签密模式

当$\mathrm{S},R\notin\varnothing$时,那么$f\left(\mathrm{pk}_R\right)=1$且$f\left(\mathrm{sk}_S\right)=1$. 如果$C=\left(v_1,u,\mathcal{E}\right)$是一个有效的密文,那么根据调和函数定义可知$\mathrm{Rec}\left(x_Rv_1,u\right)=\mathrm{Rec}\left(v_2,u\right)$,于是有

$$\begin{aligned}&G\left(v_1,u,\mathrm{Rec}\left(x_Rv_1,u\right),\mathrm{pk}_S,\mathrm{pk}_R\right)\cdot f\left(\mathrm{pk}_R\right)\\&=G\left(v_1,u,\mathrm{Rec}\left(v_2,u\right),\mathrm{pk}_S,\mathrm{pk}_R\right)\cdot f\left(\mathrm{pk}_R\right)\\&=K\end{aligned}$$

从而可以计算$\mathcal{E}\oplus K=m||z||c'$得到消息及签名.接下来验证$z\in\mathcal{R}_{q,[B-U]}$是否成立,如果成立则编码$c=F(c')$,计算

$$\begin{aligned}a_1z-t_{s1}c&=a_1z-a_1x_Sc-e_{S1}c\\&=a_1x_Sc+a_1y-a_1x_Sc-e_{S1}c\\&=a_1y-e_{S1}c\\&=w_1\end{aligned},$$

$$\begin{aligned}a_2z-t_{s2}c&=a_2x_Sc+a_2y-a_2x_Sc-e_{S2}c\\&=a_2y-e_{S2}c\\&=w_2\end{aligned}$$

最后可以通过验证等式$c'=H\left(w_{1\,d,q},w_{2\,d,q},m,\mathrm{pk}_S,\mathrm{pk}_R\right)$是否成立来验证签名的正确性,并输出消息$m$.

(2) 签名模式

当$S\notin\varnothing,R\in\varnothing$时,那么$f\left(\mathrm{pk}_R\right)=0$且$f\left(\mathrm{sk}_S\right)=1$,于是有$K=0$,$\left(m||z||c'\right)\oplus K=m||z||c'$. 忽略掉所有的空操作,方案退化成了ring-TESLA签名方案,由ring-TESLA签名方案[8]的正确性可得该模式下方案是正确的.

(3) 加密模式

当$R\notin\varnothing,S\in\varnothing$时,那么$f\left(\mathrm{pk}_R\right)=1$且$f\left(\mathrm{sk}_S\right)=0$,于是有$z=0$. 如果$C=\left(v_1,u,\mathcal{E}\right)$是一个有效的密文,那么根据调和函数定义可知$\mathrm{Rec}\left(x_Rv_1,u\right)=\mathrm{Rec}\left(v_2,u\right)$(详见文献[7]),于是有

$$\begin{aligned}&G\left(v_1,u,\mathrm{Rec}\left(x_Rv_1,u\right),\mathrm{pk}_S,\mathrm{pk}_R\right)\cdot f\left(\mathrm{pk}_R\right)\\&=G\left(v_1,u,\mathrm{Rec}\left(v_2,u\right),\mathrm{pk}_S,\mathrm{pk}_R\right)\cdot f\left(\mathrm{pk}_R\right)\\&=K\end{aligned}$$

从而可以计算$\mathcal{E}\oplus K=m||0||c'$得到并返回消息$m$.

4.2　安全性

本文的方案是基于ADP16的密钥交换协议和ABB16的ring-TESLA签名方案构造的,方案的IND-CCA2安全性可以借鉴FO13及ADP16的方法来证明,方案的SUF-CMA安全性可以借鉴ABB16的方法来证明,下面我们给出安全性规约.

定理1(机密性)　当$R\notin\varnothing$时,设$n,d,q,\omega,\sigma,B,U,L,k,l$是满足上述RLWE-GSC方案要求的任意参数,在随机预言机模型下,如果存在着敌手A在多项式时间t_{A}内,进行不多于q_{SC}次签密询问,不多于q_{DSC}次解签密询问,以不可忽略的优势ϵ攻击RLWE-GSC方案的IND-CCA2安全性,那么存在着一个敌手B在多项式时间$t_{\mathrm{B}}\approx t_{\mathrm{A}}+\mathcal{O}\left(q_{\mathrm{GSC}}k^2+q_H+q_G\right)$内,以优势$\varepsilon'>\varepsilon\left(1-q_{\mathrm{DSC}}\left(\frac{q_H}{2^n}+\frac{q_G}{2^l}\right)\right)$攻击判定性R-LWE$_{q,n,2,\sigma}$问题.

证明　当$R\notin\varnothing$时,那么$f\left(\mathrm{pk}_R\right)=1$,方案运行在加密或者签密模式下.假定模拟者被给定判定性R-LWE$_{q,n,2,\sigma}$问题实例$\left(a_1,t_1\right)$和$\left(a_2,t_2\right)$,它们都服从$\mathcal{R}_q\times\mathcal{R}_q$上的随机均匀分布,或者满足$t_1=a_1x+e_1\left(\mathrm{mod}\,q\right)$且$t_2=a_2x+e_2(\mathrm{mod}q))$,其中$x,e_1,e_2\leftarrow\mathbb{D}_\sigma^n$. 下面我们描述模拟者如何利用敌手A的信息为判定性R-LWE$_{q,n,2,\sigma}$问题来构造一个区分算法B.

准备公钥:对于上述给定的参数和分布$\left(a_1,t_1\right)$和$\left(a_2,t_2\right)$,模拟者将a_1,a_2作为方案的公开参数,并输出公钥$\mathrm{pk}_R^*=\left\{t_{R1}^*=t_1,t_{R2}^*=t_2\right\}$,并发送给敌手A.

第1阶段哈希询问与解签密询问

对$\left(p_1,p_2,m,\mathrm{pk}_S,\mathrm{sk}_S\right)$的$H$询问模拟. 当收到对$H$的哈希询问时,模拟者查看是否多元组$\left(p_1,p_2,m,\mathrm{pk}_S,\mathrm{sk}_S,\mathrm{pk}_R^*,z,c'\right)$在$\mathrm{L}_1$中已经存在,如果存在,返回$c'$,否则模拟者随机选择$z\leftarrow\mathcal{R}_{q,[B-U]}$和$c'\in\{0,1\}^k$,计算$c=F(c')$,$w_1=a_1z-t_{s1}c$,$w_2=a_2z-t_{s2}c$. 接下来检查是否对于所有的$j\in(1,2,\cdots,n)$,满足$\left[w_{1j}\right]_{2^d}<2^d-L$和$\left[w_{2j}\right]_{2^d}<2^d-L$,如果不满足重复上述过程. 由拒绝抽样的性质可以得出,对于$i=1,2$满足$w_{i\,d,q}=a_iy_{d,q}$(详见文献[7]),然后模拟者将多元组$\left(p_1,p_2,m,\mathrm{pk}_S,\mathrm{sk}_S,\mathrm{pk}_R^*,z,c'\right)$插入$\mathrm{L}_1$,并返回$c'$.

对$\left(v_1,u,\mathrm{pk}_S,\mathrm{sk}_S\right)$的$G$询问模拟. 当收到对$G$的哈希询问时,模拟者查看是否多元组$\left(v_1,u,\mathrm{pk}_S,\mathrm{sk}_S,\mathrm{pk}_R^*,K\right)$在$\mathrm{L}_2$中已经存在,如果存在,返回$K$,否则模拟者随机选择$x\in D_\sigma^n$,计算$K=G\left(v_1,u,\mathrm{Rec}\left(xv_1,u\right),\mathrm{pk}_S,\mathrm{pk}_R^*\right)$,将元组$\left(v_1,u,\mathrm{pk}_S,\mathrm{sk}_S,\mathrm{pk}_R^*,K\right)$插入$\mathrm{L}_2$中,并返回$K$.

对$\left(m,\mathrm{pk}_R^*,\mathrm{pk}_S,\mathrm{sk}_S\right)$的签密询问模拟. 当收到对$\left(m,\mathrm{pk}_R^*,\mathrm{pk}_S,\mathrm{sk}_S\right)$的签密询问时,模拟者像运行签密算法那样计算签密,但是其中H和G的哈希运算按照上述方法进行模拟.

对$\left(v_1,u,\mathcal{E},\mathrm{pk}_S,\mathrm{sk}_S\right)$的解签密询问模拟. 当收到对$\left(v_1,u,\mathcal{E},\mathrm{pk}_S,\mathrm{sk}_S\right)$的解签密询问时,模拟者遍历$\mathrm{L}_1$和$\mathrm{L}_2$,查看是否存在这样的元组$\left(m,\mathrm{pk}_S,\mathrm{sk}_S,\mathrm{pk}_R^*,z,c'\right)$和$\left(v_1,u,\mathrm{pk}_S,\mathrm{sk}_S,\mathrm{pk}_R^*,K\right)$,满足$\mathcal{E}\leftarrow K\oplus\left(m\,\|\,z\,\|\,c'\right)$,如果存在返回$m$,否则返回$\perp$.

准备挑战签密文:第一阶段完成后,A在消息空间中选择两个等长消息(m_0,m_1),连同任意发送者的公私钥对$\left(\mathrm{pk}_S^*,\mathrm{sk}_S^*\right)$一起发送给挑战者,要求挑战者以接收方公钥$\mathrm{pk}_R^*=\left\{t_{R1}^*,t_{R2}^*\right\}$生成挑战密文. 随后挑战者随机选择$b\in\{0,1\}$,做如下运算.

选择 $y \leftarrow {}_{\$}\mathcal{R}_{q,[B]}$, $y', y'' \leftarrow D_{\sigma}^{n}$, 然后计算 $c'^{*} = H\left(a_1 y_{d,q}, a_2 y_{d,q}, m_b, \mathrm{pk}_S^*, \mathrm{pk}_R^*\right)$,编码 $c^* = F\left(c'^{*}\right)$,计算 $z^* = \left(x_S^* c + y^*\right) \cdot f\left(\mathrm{sk}_S^*\right)$, $w_1^* = ay^* - e_{s1}^* c$ 和 $w_2^* = a'ay^* - e_{s2}^* c$. 如果 $z^* \neq 0$,验证 $\left[w_1^*\right]_{2^d}, \left[w_2^*\right]_{2^d} \in \mathcal{R}_{q,\left[2^d - L\right]}$ 且 $z^* \in \mathcal{R}_{q,[B-U]}$ 是否成立,如果不成立则重新开始并重复上述过程.

然后计算

$$v_1^* = a_1 y + y', v_2^* = ty + y'',$$

$$u^* = \mathrm{HelpRec}\left(v_2^*\right),$$

$$K^* = G\left(v_1^*, u^*, \mathrm{Rec}\left(v_2^*, u^*\right), \mathrm{pk}_S^*, \mathrm{pk}_R^*\right),$$

得到 $\mathcal{E}^* = K^* \oplus \left(m_b \| z^* \| c'^{*}\right)$,最后输出 $C^* = \left(v_1^*, u^*, \mathcal{E}^*\right)$ 并发送给敌手 A.

第2阶段解签密询问

敌手重复第1阶段的询问过程,但是要求不能以公私钥对 $\left(\mathrm{pk}_S^*, \mathrm{sk}_S^*\right)$ 对挑战签密文 $C^* = \left(v_1^*, u^*, \mathcal{E}^*\right)$ 进行询问,模拟者同第1阶段那样应答询问.

猜测阶段:敌手A输出 $b' \in \{0, 1\}$ 作为对 b 的猜测.

可以看出,上述模拟是完善的. 当给定模拟者的分布 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$ 恰好是来自分布 $A_{s,\chi}$,从敌手视角看到的模拟过程与 b 的分布,同真实的攻击时是一致的,但是如果分布 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$ 都是 $\mathcal{R}_q \times \mathcal{R}_q$ 上均匀随机分布,bt 的分布与敌A的视角看到的分布是信息论上独立的,于是模拟者完成了对判定性 R-LWE$_{q,n,2,\sigma}$ 问题的区分算法的构造.

如果 $b' = b$,敌手B获知分布 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$ 是来自分布 $A_{s,\chi}$,否则分布 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$ 都是 $\mathcal{R}_q \times \mathcal{R}_q$ 上均匀随机分布,判定性 R-LWE$_{q,n,2,\sigma}$ 问题得解.

上述过程中会使得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 和 G 的模拟不完善导致的. 对于 H 的询问模拟,这个概率不超过 $q_H/2^k$;对于 G 的询问模拟,该概率不超过 $q_G/2^l$. 因此算法B攻破判定性 R-LWE$_{q,n,2,\sigma}$ 问题的优势 $\varepsilon' > \varepsilon\left(1 - q_{\mathrm{DSC}}\left(\frac{q_H}{2^n} + \frac{q_G}{2^l}\right)\right)$.

从上述过程可以看出,算法B的运算都是非常高效的. 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 $\left(v_1, v_2, u_2, \mathcal{E}\right)$ 的概率和运行真实签密算法时拒绝的概率是一样的. 进一步地,忽略高效的加法及哈希运算,签密与解签密的模拟过程包含许多次多项式乘法运算,平均大约每次询问包含 $\mathcal{O}\left((k+l)^2\right)$ 次多项式乘法运算,于是可以得出近似的边界值:

$$t_{\mathrm{B}} \approx t_{\mathrm{A}} + \mathcal{O}\left(\left(q_{SC} + q_{DSC}\right)(k+l)^2 + q_H + q_G\right)$$

定理2(认证性) 当 $S \notin \varnothing$ 时,设 $n, d, q, \omega, \sigma, B, U, L, k, l$ 是满足上述RLWE-GSC方案要求的任意参数,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_{A} 内,进行不多于 q_{SC} 次签密询问,不多于 q_H 次哈希 H 询问,不多于 q_G 次哈希 G 询问,以不可忽略的优势 ε_{A} 对RLWE-GSC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 $t_{\mathrm{D}} \approx t_{\mathrm{A}} + \mathcal{O}\left(q_{SC}(k+l)^2 + q_H + q_G\right)$ 内,攻破判定性 R-LWE$_{q,n,2,\sigma}$ 问题,其优势

$$\varepsilon_{\mathrm{D}} \geqslant \varepsilon_{\mathrm{A}}\left(1 - \frac{\left(q_H + q_G\right) q_{SC} 2^{2n(d+1)}}{(2B+1)^n q^n}\right) - \frac{2^{2dn}\left(q_H + q_G\right)(2B - 2U + 1)^n + (28\sigma + 1)^{3n}}{q^{2n}}$$

证明 当 $S \notin \varnothing$ 时,那么 $f\left(sk_S\right) = 1$,方案运行在签名或签密者模式下. 假定模拟者被给定两个 R-LWE$_{q,n,2,\sigma}$ 挑战对 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$,它以等概率服从 $\mathcal{R}_q \times \mathcal{R}_q$ 上的随机均匀分布,或者都服从 $A_{s,\chi}$ 分布($t_1 = a_1 s + e_1 \left(\mathrm{mod}\, q\right)$, $t_2 = a_2 s + e_2 \left(\mathrm{mod}\, q\right)$,见定义2),其中 χ 表示 $\mathcal{R}_q$ 上的高斯分布 D_{σ}^{n},且 $s \leftarrow D_{\sigma}^{n}$. 下面我们描述模拟者D如何利用敌手A的信息为判定性 R-LWE$_{q,n,2,\sigma}$ 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两个 R-LWE$_{q,n,2,\sigma}$ 挑战对 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$,D设置 a_1, a_2 为公开参数,并发送 $\mathrm{pk}_S^* = \left(t_{S1}^* = t_1, t_{S2}^* = t_2\right)$ 给A.

哈希询问:对 $\left(p_1, p_2, m, \mathrm{pk}_R\right)$ 的 H 询问模拟. 当收到对 H 的哈希询问时,模拟者在 L_1 查询是否存在元组 $\left(p_1, p_2, m, \mathrm{pk}_S^*, \mathrm{pk}_R, c'\right)$,如果存在,返回 c',否则选择一个随机数 $c' \in \{0, 1\}^k$,将元组 $\left(p_1, p_2, m, \mathrm{pk}_S^*, \mathrm{pk}_R, c'\right)$ 插入 L_1 中,并返回 c'.

对 $\left(v_1, u, \mathrm{pk}_R, \mathrm{pk}_S^*\right)$ 的 G 询问模拟. 当收到对 G 的哈希询问时,模拟者查看是否多元组 $\left(v_1, u, \mathrm{pk}_S^*, \mathrm{pk}_R, K\right)$ 在 L_2 中已经存在,如果存在,返回 K,否则计算 $K = G\left(v_1, u, \mathrm{Rec}\left(x_R v_1, u\right), \mathrm{pk}_S^*, \mathrm{pk}_R\right) \cdot f\left(\mathrm{pk}_R\right)$, 将元组 $\left(v_1, u, \mathrm{pk}_S, \mathrm{sk}_S, \mathrm{pk}_R^*, K\right)$ 插入 L_2 中,并返回 K.

签密(签名)询问:对 $\left(m, \mathrm{pk}_R, \mathrm{sk}_R\right)$ 的签密或签名询问模拟. 当收到签密或签名询问时,D按照如下步骤模拟.

D选择 $y \leftarrow {}_{\$}\mathcal{R}_{q,[B]}, y', y'' \leftarrow D_{\sigma}^{n}$,计算 $v_1 \leftarrow a_1 y + y'$, $v_2 \leftarrow t_{R1} y + y'', u \leftarrow \mathrm{HelpRec}\left(v_2\right)$,然后对 $\left(v_1, u, \mathrm{pk}_R, \mathrm{pk}_S^*\right)$

模拟随机预言机 G 询问，获得秘钥 K，对 $\left(a_1 y_{d,q}, a_2 y_{d,q}, m, \mathrm{pk}_R\right)$ 模拟随机预言机 H 询问，获得 c'，并编码 $c = F(c')$. 接下来随机选择 $z \leftarrow \mathcal{R}_{q,[B-U]}$，计算 $w_1 \leftarrow a_1 z - t_{s1} c$ 和 $w_2 \leftarrow a_2 z - t_{s2} c$，验证 $\left[w_1\right]_{2^d}, \left[w_2\right]_{2^d} \in \mathcal{R}_{q,2^d-L} \vee z \in \mathcal{R}_{q,[B-U]}$ 是否满足，不满足则重选随机数 y 并重复以上步骤. 进一步地，如果在 L_1 中已经存在对 $\left(w_{1\,d,q}, w_{2\,d,q}, m, \mathrm{pk}_S^*, \mathrm{pk}_R\right)$ 哈希询问，D终止模拟，否则计算 $c' \leftarrow H\left(w_{1\,d,q}, w_{2\,d,q}, m, \mathrm{pk}_S^*, \mathrm{pk}_R\right)$，$\mathcal{E} = K \oplus \left(m \parallel z \parallel c'\right)$，并返回 $C \leftarrow \left(v_1, u, \mathcal{E}\right)$.

解签密询问：对 $\left(v_1, u, \mathcal{E}, \mathrm{pk}_S^*, \mathrm{pk}_R, \mathrm{sk}_R\right)$ 的解签密询问模拟. 当收到解签密询问时，D按照如下步骤模拟.

D遍历 L_2，如果 $\left(v_1, u, \mathrm{pk}_R, \mathrm{pk}_S^*\right)$ 不存在，D返回 $\perp$，否则D获得 K，如果 $K \neq 0$，计算 $\left(m \| z \| c''\right) = K \oplus \mathcal{E}$，并返回 m.

伪造阶段：询问阶段结束后，攻击者A输出了一对公私钥 $\left(\mathrm{pk}_R^*, \mathrm{sk}_R^*\right)$ 和伪造的签密文 $C^* = \left(v_1^*, u^*, \mathcal{E}^*\right)$，并且要求 C^* 没有进行过签密询问. 然后D验证伪造的签密文是否有效，如果解签密算法 $\mathrm{GDSC}\left(C^*, \mathrm{pk}_S^*, \mathrm{sk}_R^*\right)$ 返回 m，D输出1，否则D输出0. 模拟者D完成了对 $\mathrm{R\text{-}LWE}_{q,n,2,\sigma}$ 挑战区分器的构造.

可以看出，如果 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$ 是来自分布 $A_{s,\chi}$，D模拟的对哈希询问、签密及解签密询问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 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$ 都是 $\mathcal{R}_q \times \mathcal{R}_q$ 上均匀随机分布的情况下重敌手D的模拟同真实的攻击是信息论独立的，不过模拟可能会终止. 这里的我们还需证明两点：①模拟签密过程中随机选择的 z 的分布同真实签密算法中 z 的分布是统计接近的；②模拟终止的概率可以忽略.

下面我们分别给出具体描述：

(1)由文献[8]引理1容易得出签密算法计算出的分布 $z \in \mathcal{R}_{q,[B-U]}$ 同 $\mathcal{R}_{q,[B-U]}$ 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 $\mathcal{R}_{q,[B]}$ 上随机均匀的选择 y，在环 $\mathcal{R}_q$ 上的离散高斯分布 D_σ^n 中随机选择 y', y'', y'''. 进一步地，如果挑战对 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$ 都服从 $A_{s,\chi}$ 分布，那么模拟过程中不仅满足 $c' = H\left(w_{1\,d,q}, w_{2\,d,q}, m, \mathrm{pk}_S^*, \mathrm{pk}_R\right)$，而且满足 $c' = H\left(a_1 y_{d,q}, a_2 y_{d,q}, m, \mathrm{pk}_S^*, \mathrm{pk}_R\right)$. 显然，原始签密过程中终止的概率上界为上述签密模拟过程中更改的概率，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 $q_{SC}\left(q_H + q_G + q_{SC}\right)\dfrac{2^{2n(d+1)}}{(2B+1)^n q^n}$.

并且进一步利用R-LWE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：

$$\varepsilon_D \geqslant \varepsilon_A\left(1 - \frac{\left(q_H + q_G\right) q_{SC} 2^{2n(d+1)}}{(2B+1)^n q^n}\right) - \frac{2^{2dn}\left(q_H + q_G\right)(2B - 2U + 1)^n + (28\sigma + 1)^{3n}}{q^{2n}}$$

最后我们分析运行时间，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_{A} 同模拟者D的运行时间 t_{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 $\left(a_1, t_1\right)$ 和 $\left(a_2, t_2\right)$ 的两个预言机询问，加上回答哈希询问和签密询问所需的时间. 当模拟签密过程时，D拒绝一个对 $\left(v_1, u, \mathcal{E}\right)$ 的概率同运行GDSC算法时的概率时相同的. 具体来说，忽略一些高效的加法及哈希运算，模拟签密过程由许多乘法多项式运算组成，大约每次询问平均 $\mathcal{O}\left(k^2\right)$ 次，因此总的运行时间近似为 $t_{\mathrm{D}} \approx t_{\mathrm{A}} + \mathcal{O}\left(q_{\mathrm{SC}} k^2 + q_H + q_G\right)$.

4.3　对比分析

现有的广义签密方案都是基于离散对数和双线性对实现的，而本文的方案是基于格上困难问题构造的. 同基于离散对数和双线性对的方案比，在同等安全强度下格密码虽然密文大小上有一定的扩展，但是其运算都是非常高效的线性运算，计算效率普遍要远高于前者，格密码还是抗量子攻击密码最重要的候选者之一，因此这里不将本方案同现有的基于离散对数的同类方案进行详细的效率对比，仅比较相关基于格的签密方案.

根据实际应用环境需求，广义签密可同时实现加密、签名和签密三种功能，但是同传统签密方案比，广义签密方案的构造不应该以显著牺牲效率为代价. 从抗量子攻击的角度出发，结合上述设计原则和无陷门构造的特点，下面我们将本方案同现有无陷门的基于格的加密、签名和签密方案的密文大小进行比较，具体比较结果如表1所示，其中 $|\mathcal{M}|$ 表示明文的比特长度，$S_{\mathbb{D}}$ 表示高斯采样运算，$S_{\mathbb{T}}$ 表示带陷门的原像抽样，$M_{\mathbb{V}}$ 表示矩阵向量乘法运算，$M_{\mathbb{R}}$ 表示多项式环乘法运算，$n = 2^k$，n, q 定义了环 $\mathcal{R}_q$，参数 n, q, k 选择详见2.1节符号说明.

表1 相关方案性能比较结果

方案		功能	底层运算结构	安全性	公钥尺寸/bit	密文尺寸/bit	签密运算	解签密运算	运算方法
LWD16		签密	标准格	IND-CCA2 EUF-CMA	$2n^2\log q$	$4n^*\log q+\lvert\mathcal{M}\rvert$	$4S_{\mathbb{D}}+6M_{\mathbb{V}}$	$3M_{\mathbb{V}}$	矩阵运算
FK18	原始KEX构造	签密	理想格	IND-CPA SUF-CMA	$2n\log q$	$4n^*\log q+\lvert\mathcal{M}\rvert$	$8M_{\mathbb{R}}$	$5M_{\mathbb{R}}$	FFT
	原始KEM构造				$2n\log q$	$3n^*\log q+\lvert\mathcal{M}\rvert$	$8M_{\mathbb{R}}$	$5M_{\mathbb{R}}$	FFT
	FK18(KEX)+LM08		理想格+一次签密算法	IND-CCA2 EUF-CMA	$2n\log q$	$2n\log q+l_{HR}+n\log n\log q+2l_H\log n+\lvert\mathcal{M}\rvert$	$8M_{\mathbb{R}}+\log nM_{\mathbb{R}}$	$5M_{\mathbb{R}}+\log nM_{\mathbb{R}}$	FFT
	FK18(KEM)+LM08				$2n\log q$	$3n\log q+n\log n\log q+2l_H\log n+\lvert\mathcal{M}\rvert$	$8M_{\mathbb{R}}+\log nM_{\mathbb{R}}$	$5M_{\mathbb{R}}+\log nM_{\mathbb{R}}$	FFT
本文方案		广义签密	理想格	IND-CCA2 SUF-CMA	$2n\log q$	$3n^*\log q+k+\lvert\mathcal{M}\rvert$	$8M_{\mathbb{R}}$	$5M_{\mathbb{R}}$	FFT

LWWD16构造了一个无陷门的格基签密方案,一般安全参数取$m=2n$,方案公钥尺寸为$2n^2\log q$比特,私钥尺寸为$n^2\log q$比特,密文量为$\lvert\mathcal{M}\rvert+4n\log q$比特,签密需要$4S_{\mathbb{D}}+6M_{\mathbb{V}}$运算,解签密需要$3M_{\mathbb{V}}$运算.

FK18以密钥交换(KEX)的方式和密钥封装(KEM)的方式分别构造了一个格基签密方案,它们都是在环上构造的,具有较高的效率. 具体来说,两种方案公私钥尺寸、签密和解签密运算量相同,公钥尺寸为$2n\log q$比特,私钥为$3n\log q$比特,签密运算量主要为$8M_{\mathbb{R}}$(忽略了环元素抽样运算),解签密运算量主要为$5M_{\mathbb{R}}$. KEX构造的密文量为$\lvert\mathcal{M}\rvert+2n\log q+l_{HR}$比特,其中$l_{HR}$表示调和函数HelpRec的输出;KEM构造的密文量为$\lvert\mathcal{M}\rvert+3n\log q$比特. 在随机预言机模型下,方案认证性上达到了SUF-CMA安全,然而在机密性上只达到了IND-CPA安全.

为了更准确比较效率,可考虑将FK18方案转换为CCA2安全并与新方案进行比较. 将IND-CPA的方案转换成IND-CCA2安全的通用方法是利用一次签名技术,具体比较中采用强不可伪造的一次签名方案采用目前较为高效的LM08[18]方案,用l_H表示一次签名方案哈希函数的输出长度.

本文的广义签密方案同LWD16的签密方案比,密文尺寸小$n^*\log q-k$比特,这主要得益于新方案是基于理想格构造,利用快速傅里叶变换(FFT)可以提高多项式环运算效率,另外在安全性上也提供了更好的认证安全. 同FK18原始的KEM构造相比,密文尺寸只增加了k比特,同FK18原始的KEX构造比,密文尺寸较小了$n^*\log q-k$比特,效率变化不大,但是本文方案提供了更强的保密安全级别,FK18只能达到IND-CPA安全性,而新方案满足IND-CCA2,因而能够抵抗更强的攻击. 同FK18改进的CCA2安全的KEM和KEX构造相比,新方案密文尺寸至少减少了$n\log n\log q+2l_H\log n-k$比特,签密和解签密计算量减少了$\log nM_{\mathbb{R}}$,因此新方案在达到同等CCA2时,效率更高.

另外,LWD16和FK18都只能提供签密功能,而本文方案可以根据实际应用环境需求提供加密、签名、签密三种功能,真正实现了广义签密.

4.4 实验与性能分析

上述GSC方案进行了编程实现,实验环境为1.8GHz四核心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:$n=1024$, $q=343576577$, $\omega=19$, $B=524287$, $\sigma=30$, $L=2766$, $d=23$, $U=3173$,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.

实验过程中,我们采用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,实验结果如图1所示.

实验数据表明,广义签密的密钥生成算法随着明文长度变化其花费时间变化不大. 这主要是因为新方案选择得安全参数是固定的,对于签密、仅加密算法耗时从某一个初值开始随消息长度增大呈缓慢的线性递增,而

仅签名算法对于明文消息长度的变化响应不明显. 原因可能是因为签密方案耗时的计算可以看成由签名和对称加密两部分组成,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. 而加密需要对消息分组并逐组进行加密,耗时与明文消息长度成正比. 另外,将 FK18 转换成 CCA2 安全强度后,新方案同 FK18 的 KEM 和 KEX 构造相比,密钥生成的耗时相近,签密与解签密耗时明显减少.

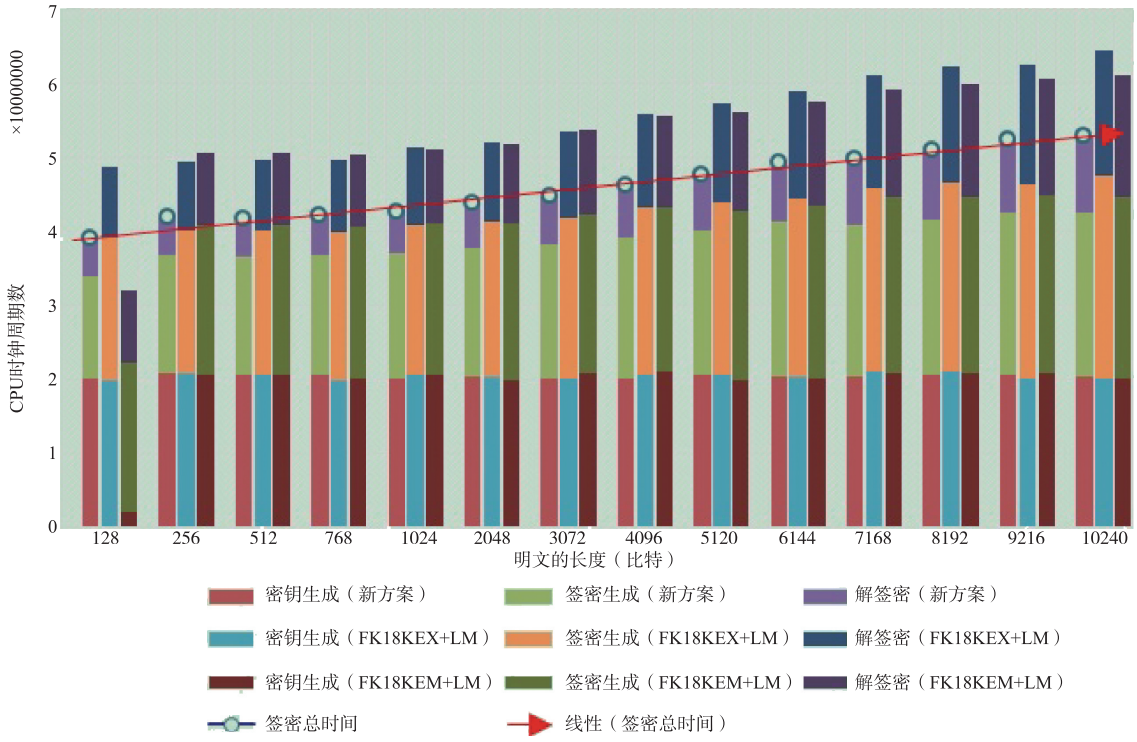


图1　类似GSC方案效率比较

5　总结及展望

广义签密能根据实际应用需求同时提供加密、签名和签密三种功能,具有很强的实用性. 现有的广义签密方案几乎都是基于离散对数困难问题构造的,随着量子计算技术的发展,其安全性越来越受到挑战. 格具有很多优点,更是构造抗量子攻击密码最重要的候选工具,构造基于格上困难问题的广义签密具有重要意义. 本文结合 ABB16 的 ring-TESLA 签名方案和 ADP16 的抗量子攻击的密钥交换协议,并借鉴 FO13 的转换方法,基于环上 LWE 问题,我们首次构造了一个无陷门的广义签密方案. 该方案满足选择密文攻击不可区分性安全性(IND-CCA2)和选择消息攻击强不可伪造性安全性(SUF-CMA),方案没有用到复杂的带陷门的原像抽样和求逆运算,具有很高的计算效率. 同现有相关的无陷门的格基签密方案比,本文方案具有相近的密文尺寸,但是具有更高的安全性,并能同时提供加密、签名和签密三种功能,实用性更强.

参考文献

[1] Zheng Y. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption) [A]. Annual International Cryptology Conference[C]. Berlin, Heidelberg,Germany: Springer, 1997. 165 – 179.

[2] Han Y, Yang X, Wei P, et al. ECGSC: elliptic curve based generalized signcryption [A]. International Conference on Ubiquitous Intelligence and Computing [C]. Berlin, Heidelberg,Germany:Springer, 2006. 956 – 965.

[3] Yu G, Ma X, Shen Y, et al. Provable secure identity based generalized signcryption scheme [J]. Theoretical Computer Science, 2010, 411(40-42): 3614 – 3624.

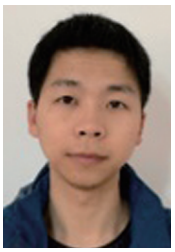
[4] Kushwah P, Lal S. An efficient identity based generalized signcryption scheme [J]. Theoretical Computer Science, 2011, 412(45): 6382 – 6389.

[5] Ji H, Han W, Zhao L. Certificateless generalized signcryption[J]. Physics Procedia, 2012, 33: 962 – 967.

[6] Zhou C, Zhou W, Dong X. Provable certificateless gener-

alized signcryption scheme[J]. Designs, Codes and Cryptography, 2014, 71(2): 331 – 346.
[7] Alkim E, Ducas L, Pöppelmann T, et al. Post-quantum key exchange—a new hope[A]. The 25th Security Symposium (Security 16)[C]. Austin,USA: USENIX, 2016. 327 – 343.
[8] Akleylek S, Bindel N, Buchmann J, et al. An efficient lattice-based signature scheme with provably secure instantiation[A]. International Conference on Cryptology in Africa[C]. Cham,Germany: Springer, 2016. 44 – 60.
[9] Güneysu T, Lyubashevsky V, Pöppelmann T. Practical lattice-based cryptography: A signature scheme for embedded systems[A]. International Workshop on Cryptographic Hardware and Embedded Systems[C]. Berlin, Heidelberg,Germany: Springer, 2012. 530 – 547.
[10] Wang F, Hu Y, Wang C. Post-quantum secure hybrid signcryption from lattice assumption[J]. Applied Mathematics & Information Sciences, 2012, 6(1): 23 – 28.
[11] Yan J, Wang L, Wang L, et al. Efficient lattice-based signcryption in standard model[J]. Mathematical Problems in Engineering, 2013,(2013): ArticleID702539.
[12] 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.
[13] Sato S, Shikata J. Lattice-based signcryption without random oracles[A]. International Conference on Post-Quantum Cryptography (PQCrypto2018)[C]. Cham, Germany: Springer, 2018. 331 – 351.
[14] Liu Z Y, Tso R, Tseng Y F, et al. Signcryption from NTRU lattices without random oracles[A]. The 14th Asia Joint Conference on Information Security (AsiaJCIS2019)[C]. USA: IEEE, 2019. 134 – 141.
[15] 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.
[16] Fujisaki E, Okamoto T. Secure integration ofasymmetric and symmetric encryption schemes[J]. Journal of Cryptology, 2013, 26(1): 80 – 101.
[17] Applebaum B, Cash D, Peikert C, et al. Fast cryptographic primitives and circular-secure encryption based on hard learning problems[A]. Annual International Cryptology Conference[C]. Berlin, Heidelberg, Germany: Springer, 2009. 595 – 618.
[18] An J H, Dodis Y, Rabin T. On the security of joint signature and encryption[A]. International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin, Heidelberg,Germany: Springer, 2002. 83 – 107.

作者简介



刘 镇 男,1985年6月生于湖南省衡南县.现为武警工程大学讲师,主要研究方向为公钥密码算法、可证明安全等.
E-mail: lliuzheng@163.com

吴立强 男,1986年7月出生于陕西省蓝田县.现为武警工程大学密码工程学院讲师,主要研究方向为基于格的密码学和可证明安全理论.
E-mail:latticewj@163.com

韩益亮(通信作者) 男,1977年10月出生于甘肃省会宁县.教授、博士生导师,主要研究方向为信息安全与密码学.
E-mail:hanyil@163.com.

杨晓元 男,1959年11月生于湖南省湘潭市.教授、博士生导师,主要研究领域为网络安全与密码学.
E-mail:yxyangyxyang@163.com

柳曙光 男,1976年生于山东省栖霞市.副教授,主要研究领域为计算机应用、信息安全.
E-mail:18292011695@139.com