计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200100024

基于 MLWE 的双向可否认加密方案

郑嘉彤[1,2]　吴文渊[1]
1 中国科学院重庆绿色智能技术研究院自动推理与认知重庆市重点实验室　重庆 400714
2 中国科学院大学　北京 101408
(940188085@qq.com)

摘　要　传统的加密方案没有考虑到敌手窃听密文后胁迫发送方或接收方交代加密时使用的公钥、随机数、明文或解密密钥的情况,因此可否认加密的概念在1997年被提出,以解决胁迫问题所带来的信息泄露。目前国内外学者仅提出了几种可否认加密方案,但是普遍存在加密效率过低和膨胀率过高的问题,因此并不实用。文中通过构造"模糊集"的方式来构造一种可抵抗量子攻击的实用双向可否认加密方案。该方案基于多项式环上的模容错学习(Module Learning With Errors,MLWE)困难问题来构造两个敌手无法进行区分的密文分布,并通过卡方统计实验验证了两个密文分布的不可区分性,其安全性可规约到格上的最短独立向量问题(Shortest Independent Vectors Problem,SIVP)。文中对方案的正确性、安全性、可否认性、膨胀率和复杂度等进行了分析,并且通过C++实现的实验结果与理论分析相一致。实验结果表明,该可否认加密方案的误码率约为1×10^{-23},密文膨胀率为5.0,加密速度约为670KB/s,因此该方案在电子选举和电子竞标等场景具有实用价值。

关键词:可否认加密;抗量子攻击;格密码;对称加密;模糊集
中图法分类号　TP309

Practical Bi-deniable Encryption Scheme Based on MLWE

ZHENG Jia-tong[1,2] and WU Wen-yuan[1]
1 Chongqing Key Lab. of Auotomated Resoning & Cognition,Chongqing Inst. of Green Intelligent Technol.,Chinese Academy of Sciences,Chongqing 400714,China
2 University of Chinese Academy of Sciences,Beijing 101408,China

Abstract　The traditional encryption scheme does not take into account the situation in which the adversary eavesdrops on the ciphertext to force the sender or receiver to hand over the public key,random number,plaintext,or secret key used in the encryption. Therefore,the concept of deniable encryption was proposed in 1997 to solve the information leakage caused by the coercion problem. At present,only several complete deniable encryption schemes have been proposed and implemented. However,the schemes are not practical due to the problems of low encryption efficiency and high expansion rate. By constructing a "translucent set",a practical bi-deniable anti-quantum encryption scheme is proposed in this paper. The scheme uses the difficult problem of Module Learning With Errors (MLWE) based on polynomial ring to construct two ciphertext distributions that adversaries can't distinguish. The indistinguishability of two ciphertext distributions is verified by chi-square statistical experiments. The schemes' security can be reduced to the Shortest Independent Vectors Problem (SIVP). Meanwhile,the correctness,security,deniable,expansion rate and complexity of the scheme are theoretically analyzed. And the experimental results obtained through C++ are consistent with the theoretical analysis. Experimental results show that the bit error rate is about 1×10^{-23},the ciphertext expansion rate 5.0,and the encryption efficiency is about 670KB/s. Therefore,it has practical application prospects in many scenarios,such as electronic election and electronic bidding.

Keywords　Deniable encryption,Anti-quantum attack,Lattice encryption,Symmetric encryption,Translucent set

到稿日期:2020-01-03　返修日期:2020-11-09　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:重庆市科委项目(cstc2018jcyj-yszxX0002,cstc2019yszx-jcyjX0003,cstc2017zdcy-yszxX0011);中科院前沿科学重点项目(QYZDB-SSW-SYS026);贵州省科技计划项目([2020]4Y056)
This work was supported by the Chongqing Science and Technology Program (cstc2018jcyj-yszxX0002,cstc2019yszx-jcyjX0003,cstc2017zdcy-yszxX0011),Key Research Program of Frontier Sciences of Chinese Academy of Sciences (QYZDB-SSW-SYS026) and Guizhou Science and Technology Program ([2020]4Y056).
通信作者:吴文渊(wuwenyuan@cigit.ac.cn)

1 引言

如果窃听者在截获密文后对密文的发送者或接收者进行主动胁迫，使其交代加密时所用的本地随机数、明文或解密密钥，那么传统的加密方案将无法保证数据的安全。

考虑这样一种情况：窃听者强迫消息的发送方或接收方交代产生密文的真实参数或用于解密的密钥。为了应对窃听者的胁迫攻击，发送方可以将真实的明文 m 加密生成密文，并使之看起来像是假明文 m' 加密得来的，然后用 m' 对胁迫者进行欺骗。胁迫者在对给出的 m' 进行验证后无法察觉到欺骗的存在，最终仅获取了假明文 。传统的加密方案并不具备这样的功能，而可否认加密体制具有对明文的可否认性。

可否认加密最早由 Canetti 等[1]提出的。文献[1]介绍了可否认加密的基本概念，并描述了如何通过一个“模糊集”、核心断言和陷门置换函数构造一个可否认加密方案；同时其根据可否认的对象将可否认加密划分为发送方、接收方和双向可否认加密，并描述了如何通过简单的技巧使某些发送方可否认加密转换为接收方可否认加密。另外，文献[1]按加密前发收双方有无分享信息将可否认加密分为标准的公钥可否认加密和密钥分享可否认加密。

由于可否认加密区别于传统的加密，具有可否认的功能，其加密效率和密文膨胀率会有所牺牲，因此提出的许多可否认方案虽然具有可否认的功能，但在实际应用中并不实用。Canetti 等[1]提出了一种可否认公钥加密方案。该方案需要对多比特信息进行多次加密，并且为了构造充分小概率 ε 可被攻破的可否认方案，将生成超多项式长度 $\frac{1}{\varepsilon}$ 的密文，因此其可否认性是不够的。Ibrahim[2]提出了一种基于二次剩余的发送方可否认加密方案，但其不能够从有效明文空间中任意选取用于欺骗的明文。后来，Jaydeep[3]改进了这一缺陷，但其加密效率仍然很低，且密文膨胀率达到约 1∶20000，因此并不实用。同时 Ibrahim 在文献[4]的基础上提出了一种基于 MPKI(mediated RSA PKI)的可否认公钥加密方案[5]，使用不经意传输(Oblivious Transfer，OT)协议，并且需要使用一个可信第三方。其在进行多比特可否认加密时重复执行不经意传输协议，效率很低。Klonowski 等[6]对文献[1]的方案进行了改进，并基于 Elgamal 构造了一个接收方可否认加密方案，明文的可否认性有所提高，但密文膨胀率却没有较大改变。2010 年，Meng 等[7]对 Klonowski 等的方案进行了改进，并基于 Elgamal 改进了可否认加密的效率，但其仍无法抵御量子计算机的攻击。以上方案未见有完整的性能分析和实验结果，且普遍存在无法抗量子、加密效率过低、膨胀率过高的问题。

因此，本文通过构造“模糊集”的方式来构造一个双向可否认的抗量子加密方案。该方案基于多项式环上的模容错学习(MLWE)困难问题，不需要任何物理假设，加密效率及膨胀率都十分优越，是实用的可否认加密方案。

在电子选举和电子拍卖等场景中，选民和拍卖者的信息是公开的，那么很有可能存在胁迫投票、买票，以及胁迫交代竞标价格等行为。可否认加密可以杜绝上述行为的发生，文献[8-9]介绍了其在电子选举中的应用。本文所提方案不仅在电子选举和电子拍卖等场景中有着非常好的应用前景，而且在已知信道被窃听的情况下，还可以故意使敌手窃听到假密钥，令其在解密后仅获取假明文信息。

2 相关工作

1997 年 Canetti 首次提出了可否认加密方案的概念，并提出了一种发送方可否认公钥加密方案。该方案逐比特进行加密，发送方在受胁迫时可将明文比特 1 否认为比特 0，而不能将比特 0 否认为比特 1。而后 Canetti 利用了奇偶性的技巧解决了这一问题，但其可否认性仍然不够。

2008 年，Klonowski 等[6]提出一种基于 Elgamal 的接收方可否认公钥加密方案。经分析此方案存在缺陷：胁迫者通过胁迫接收方可以得到私钥和假明文，然后胁迫方会计算哈希值并得到明文。于是，2010 年 Mengt 等在此基础上进行了改进，并利用 BCP 承诺方案得到了一种接收方可否认加密方案，使效率上也得到了提高。

2009 年，Jaydeep[3]首先对基于二次剩余的发送方单比特可否认公钥加密方案进行了分析。基于二次剩余的方案在加密时随机生成 k 个比特，对于每个比特 1 和 0 分别从二次剩余集合上和非二次剩余集合上选 t 个元素组成矩阵，接收者需要通过私钥重复计算雅各比符号并进行 k 次异或得到正确明文。但该方案效率很低。受胁迫的发送方可谎称 k 个比特中的某一个比特 1 是 0，以完成对单比特的欺骗。随后，Jaydeep 对其方案稍加改进并提出了对多比特的可否认加密方案，但是其 1∶20000 的密文膨胀率并不实用。

2009 年 Regev[10]提出了容错学习(Learning With Error，LWE)问题，成为之后大部分基于格的密码体制的基础，但是其本身的计算效率较低，且密文膨胀率较大。为了提升基于 LWE 问题加密方案的加密效率，2010 年 Lyubashevsky 等[11]提出了环上的容错学习(Ring Learning With Error，RLWE)问题，但其安全性只能规约到理想格上的困难问题，因此环的维数要取比较大的整数，导致加密效率不够高。2015 年 Langlois 等[12]提出了模容错学习(MLWE)问题，将 MLWE 问题规约到模格上的困难问题，并证明了 MLWE 问题中两个分布的不可区分性。2017 年 Bos 等[13]基于 MLWE 问题构建了 Kyber 密钥交换算法，该方法成为后量子密码备选方案之一。2017 年 Ke 等[14]在 Kyber 算法的基础上将明文空间扩大，使得加密效率和膨胀率得到了进一步优化。本文提出的实用可否认加密方案基于 MLWE 格困难问题，与以往提出的方案相比，还具有可有效抵御量子计算机攻击的优势。

3 预备知识

3.1 基础记号

令 $R_q = Z_q[x]/f(x)$ 表示模 q 上的多项式环，$f(x) = x^n + 1$。其中 mod q 表示模 q，mod q 的取值范围在 $[-(q-1)/2, (q-1)/2]$，$\text{mod}^+ q$ 的取值范围在 $[0, q-1]$。对于 R_q 上的多项式 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$，$f(x)$ 的无穷范数表示为 $\| f(x) \|_\infty = \max\{|a_j|\}$，多个多项式 $(u_1, u_2, \cdots, u_n) \leftarrow R_q^n$ 构成的多项式向量 $\boldsymbol{u}$ 的无穷范数表示为 $\| \boldsymbol{u} \|_\infty = \max\{|u_j|\}$。

3.2 MLWE 困难问题

设安全参数为 2 的 n 次幂，$f(x)=x^n+1$，模数 q 为大于 2 的素数，模 q 的多项式环 $R_q^n=Z_q[x]/f(x)$，令 k 为多项式矩阵的维数。文献[12]给出了基于 MLWE 困难问题的加密算法在 k 取 2 时能够抵御敌手 2^{100} 次的攻击，当 k 取 3 时，能够抵御敌手 2^{160} 次的攻击。该文中将解决 MLWE 困难问题的优势定义如下：

$$Adv_{n,k,\eta}^{mlwe}(\mathcal{A})=|\Pr[b'=1:\boldsymbol{A}\leftarrow R_q^{n\times k};(\boldsymbol{s},\boldsymbol{e})\leftarrow\beta_\eta^k\times\beta_\eta^n;\boldsymbol{b}=\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e};\boldsymbol{b}'\leftarrow\mathcal{A}(\boldsymbol{A},\boldsymbol{b})]-\Pr[b'=1:\boldsymbol{A}\leftarrow R_q^{n\times k};\boldsymbol{b}\leftarrow R_q^n;\boldsymbol{b}'\leftarrow\mathcal{A}(\boldsymbol{A},\boldsymbol{b})]|$$

我们以 $k=2$ 的情况为例，简单来说，判定型 MLWE 问题即区分下述两个分布：

(1) $\left(\begin{bmatrix}\boldsymbol{a}_{11}&\boldsymbol{a}_{12}\\\boldsymbol{a}_{21}&\boldsymbol{a}_{22}\end{bmatrix},\begin{bmatrix}\boldsymbol{b}_1\\\boldsymbol{b}_2\end{bmatrix}\right)$。其中均匀随机选取多项式 $\boldsymbol{a}_{ij}\leftarrow R_q^n(1\leqslant i\leqslant k,1\leqslant j\leqslant k)$ 和 $b_j\leftarrow R_q^n(1\leqslant j\leqslant k)$。

(2) $\left(\begin{bmatrix}\boldsymbol{a}_{11}&\boldsymbol{a}_{21}\\\boldsymbol{a}_{21}&\boldsymbol{a}_{22}\end{bmatrix},\begin{bmatrix}\boldsymbol{b}_1\\\boldsymbol{b}_2\end{bmatrix}=\begin{bmatrix}\boldsymbol{a}_{11}&\boldsymbol{a}_{12}\\\boldsymbol{a}_{21}&\boldsymbol{a}_{22}\end{bmatrix}\cdot\begin{bmatrix}\boldsymbol{s}_1\\\boldsymbol{s}_2\end{bmatrix}+\begin{bmatrix}\boldsymbol{e}_1\\\boldsymbol{e}_2\end{bmatrix}\right)$。其中，均匀随机选取 $\boldsymbol{a}_{ij}\leftarrow R_q^n(1\leqslant i\leqslant k,1\leqslant j\leqslant k)$，$\boldsymbol{s}_i\leftarrow R_q^n(1\leqslant i\leqslant k)$，$\boldsymbol{e}_i\leftarrow\chi(1\leqslant i\leqslant k)$。

3.3 压缩与解压缩技术

为了尽可能地减小密钥和密文大小，本文所提方案将采取 Kyber 算法中的压缩与解压缩技术。但压缩技术的引入会带来一定的误差，须选择合理的参数对正确率和密文膨胀率进行平衡。下文将阐述压缩与解压缩对解密带来的误差影响。

定义压缩函数 $Compress_q(x,d)$：输入 $x\in Z_q$，$d<\lceil\log q\rceil$，输出 $y=round((2^d/q)\cdot x)\bmod^+2^d$。

定义解压缩函数 $Decompress_q(y,d)$：输入 $y=Compress_q(x,d)$，输出 $x'=round((q/2^d)\cdot y)$。

对于 $x\in Z_q$，在 *Compress* 和 *Decompress* 函数压缩和解压缩后会产生误差：$|x-x'|\leqslant round(q/2^{d+1})$。

4 实用的双向可否认加密方案

4.1 双向可否认加密方案

考虑这样一种电子投票应用场景：计票者、投票者的信息以及候选者的身份信息公开。投票者用指定的加密方式向候选者投票，敌手在得知计票者和投票者身份后威胁投票人给指定候选人投票，并在得到密文后胁迫投票者或计票者向其出示投票结果。

对于胁迫方，我们假设其具有可以窃听到密文的能力，并可以接近发送方和接收双方，强迫他们对密文进行解密，并出示加密时所用的密钥和相关参数，而双方不可以借口相关参数丢失来欺骗胁迫者。

针对上述情景，我们提出了一种分享密钥类[15]的双向可否认加密方案，密文的发送方和接收方均可以通过欺骗胁迫者来抵抗胁迫攻击。收发双方在受到胁迫时均可以向胁迫者出示假的密钥 $\boldsymbol{s\_fake}$，用假明文 m' 来欺骗胁迫者，胁迫者却无法发觉被欺骗。而收发双方具有的真密钥 $\boldsymbol{s}$ 可以解密得到正确的明文 m。

本文方案为对称加密方案，共分为 3 部分：密钥生成 *Keygen*、不进行抵赖时的加密 *Enc* 或进行抵赖时的加密 *Enc_fake*、解密 *Dec*。

Keygen(k)：

1)设安全参数为 λ，多项式次数 $n=n(\lambda)$，n 为 2 的幂次。多项式矩阵的维数 $k=k(\lambda)$，模数 q 为素数，环 $R_q^n=Z_q[x]/f(x)$，近似高斯噪声分布 χ[16]。

2)在模 q 上均匀随机选取多项式矩阵 $\boldsymbol{A}\leftarrow R_q^{k\times k}$。

3)从近似高斯分布上随机生成密钥 $\boldsymbol{s}$、假密钥 $\boldsymbol{s\_fake}$，以及噪声 $\boldsymbol{e}$，$(\boldsymbol{s},\boldsymbol{s\_fake},\boldsymbol{e})\leftarrow\chi^k\times\chi^k\times\chi^k$。

4)输出 $\boldsymbol{s},\boldsymbol{s\_fake}$。

Enc($\boldsymbol{s},m$)：

1)输入对称密钥 $\boldsymbol{s}$，密文压缩参数 du 和 dv，明文空间压缩参数 dp，明文 $m\in\{0,1\}^{dp\times n}$，此时明文 m 为每项含 dp 位明文比特的 n 项多项式，通过引入 dp[13]可以同时加密 $dp\times n$ 个明文比特，从而减小密文膨胀率。

2)随机生成服从高斯分布的多项式向量 $\boldsymbol{r}$，及高斯噪声 $\boldsymbol{e}_1,e_2$。$(\boldsymbol{r},\boldsymbol{e}_1,e_2)\leftarrow\chi^k\times\chi^k\times\chi$。

3)计算多项式向量：

$$\boldsymbol{b}=\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}\tag{1}$$

4)生成密文 $\boldsymbol{C}_1$：

$$\boldsymbol{C}_1=Compress_q(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{r}+\boldsymbol{e}_1,du)\tag{2}$$

5)生成密文 C_2：

$$C_2=Compress_q(\boldsymbol{b}^{\mathrm{T}}\boldsymbol{r}+e_2+round(\frac{q}{2^{dp}})\cdot m,dv)\tag{3}$$

其中，dp 是为了扩大明文空间引入的变量。

6)生成密文 C_3：

$$C_3=Compress_q(u,dv)\tag{4}$$

其中，u 是模 q 均匀选取的多项式 $u\leftarrow R_q^k$。

7)输出密文 $\boldsymbol{C}=(\boldsymbol{C}_1,C_2,C_3)$。

Enc_fake($\boldsymbol{s},\boldsymbol{s\_fake},m,m'$)：

1)输入对称密钥 $\boldsymbol{s}$ 和 $\boldsymbol{s\_fake}$，密文压缩参数 du 和 dv，明文空间的压缩参数 dp，明文 $m\in\{0,1\}^{dp\times n}$，假明文 $m'\in\{0,1\}^{dp\times n}$。

2)随机生成服从高斯分布的多项式向量 $\boldsymbol{r}$，及高斯噪声 $\boldsymbol{e},\boldsymbol{e}_1,e_2,e_3,e_4$。

3)计算多项式向量：

$\boldsymbol{b}_1=\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}$，$\boldsymbol{b}_2=\boldsymbol{A}\cdot\boldsymbol{s\_fake}+\boldsymbol{e}_1$

4)生成密文 $\boldsymbol{C}_1$：

$\boldsymbol{C}_1=Compress(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{r}+\boldsymbol{e}_2,du)$

5)生成密文 C_2：

$C_2=Compress_q(\boldsymbol{b}_1^{\mathrm{T}}\boldsymbol{r}+e_3+round(\frac{q}{2^{dp}})\cdot m,dv)$

6)生成密文 C_3：

$C_3=\mathrm{Compress}_q(\boldsymbol{b}_2^{\mathrm{T}}\boldsymbol{r}+e_4+round(\frac{q}{2^{dp}})\cdot m',dv)$

7)输出密文 $\boldsymbol{C}=(\boldsymbol{C}_1,C_2,C_3)$。

Dec($\boldsymbol{s},\boldsymbol{C}$)：

1)输入密钥 $\boldsymbol{s}$，密文 $\boldsymbol{C}=(\boldsymbol{C}_1,C_2,C_3)$，密文压缩参数 du 和 dv。

2)解压缩得到 $\boldsymbol{C}_1'=Decompress_q(\boldsymbol{C}_1,du)$。

3)解压缩得到 $C_2'=Decompress_q(C_2,dv)$。

4)解压缩得到 $C_3'=Decompress_q(C_3,dv)$。

5)输出明文 $m=Compress_q(C_2'-\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}_1)$。

在使用 *Enc* 加密时,发送方以随机的发送顺序将 C_2,C_3 发送给接收方,接收方通过下述方式区分密文 C_2,C_3:通过 $m=Compress_q(C_2'-\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}_1)$ 对 C_2 进行解密时得到多项式 m 的每项系数在区间$[0,dp)$中,而对 C_3 进行解密时得到多项式 m 的每项系数在区间$[0,p)$中,因此接收方可以正确地区分 C_2,C_3,对 C_2 解密后得到明文 m。

同理,在使用 *Enc_fake* 加密时,接收方使用秘钥 $\boldsymbol{s}$ 对 C_2,C_3 进行区分后,通过 $m=Compress_q(C_2'-\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}_1)$对 C_2 进行解密得到明文 m。通过 $m'=Compress_q(\boldsymbol{C}_3'-\boldsymbol{s\_fake}^{\mathrm{T}}\boldsymbol{C}_1)$ 对 C_3 进行解密得到假明文 m',用于欺骗敌手。

在进行 *Compress* 和 *Decompress* 时会产生误差:$\boldsymbol{C}_1'-\boldsymbol{C}_1=\varepsilon_u$ 以及 $C_2'-C_2=\varepsilon_v$。由于在解密时经过解压缩会得到:

$$\boldsymbol{C}_1'=Decompress(\boldsymbol{C}_1,du)=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{r}+\boldsymbol{e}_1+\varepsilon_u$$

$$C_2'=Decompress(C_2,dv)=(\boldsymbol{As}+\boldsymbol{e})^{\mathrm{T}}\boldsymbol{r}+e_2+round(\frac{q}{2^{dp}})\cdot m+\varepsilon_v$$

$$C_2'-\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}_1'=\boldsymbol{e}^{\mathrm{T}}r+e_2+round(\frac{q}{2^{dp}})\cdot m+\varepsilon_v-s^{\mathrm{T}}\boldsymbol{e}_1+\boldsymbol{s}^{\mathrm{T}}\varepsilon_u$$

$$=\varepsilon+round(\frac{q}{2^{dp}})\cdot m$$

因此使用 *Enc* 加密时会产生噪声:

$$\varepsilon=\boldsymbol{e}^{\mathrm{T}}\boldsymbol{r}+e_2+\varepsilon_v-\boldsymbol{s}^{\mathrm{T}}\boldsymbol{e}_1+\boldsymbol{s}^{\mathrm{T}}\varepsilon_u \tag{5}$$

同理,使用 *Enc_fake* 加密时会产生噪声:

$$\varepsilon=\boldsymbol{e}_{0\text{ or }1}^{\mathrm{T}}\boldsymbol{r}+e_{3\text{or}4}+\varepsilon_v-\boldsymbol{s}^{\mathrm{T}}\boldsymbol{e}_2+\boldsymbol{s}^{\mathrm{T}}\varepsilon_u$$

两个噪声 ε 服从同样的分布,当噪声的范数 $\|\varepsilon\|$ 与模数 q 和压缩参数 dp 满足以下关系时,解密可以得到正确的明文[13]:

$$\Pr(\|\varepsilon\|<round(\frac{q}{2^{dp+1}}))>1-negl \tag{6}$$

若需要将明文否认成更多的假明文,则可以生成并通信多个 $\boldsymbol{s\_fake}$,在加密时计算生成更多的密文。在交代不同的 $\boldsymbol{s\_fake}$ 时可以解密获得不同的假明文,敌手同样无法发觉欺骗的存在。同时密文的膨胀率随着需要欺骗的假明文个数线性增加。

4.2 性能分析

本节将对 4.1 节中双向可否认加密方案的密文膨胀率、正确性以及如何进行否认进行分析。该方案在 Module-SIVP 问题是困难的情况下是 IND-CPA 安全的,选取合适的参数平衡后得到的误码率约为 10^{-23},膨胀率为 5.0。

4.2.1 密文膨胀率

对 4.1 节的方案进行分析,设密文膨胀率为 ρ,密文 $\boldsymbol{C}_1$ 的压缩参数为 du,密文 C_2 和 C_3 的压缩参数为 dv,明文空间的压缩参数为 dp。由于最后的密文为二维多项式向量 $\boldsymbol{C}_1$ 和多项式 C_2,C_3,则密文膨胀率为 $\rho=\frac{2du+dv\cdot 2}{dp}$。为了保证密文膨胀率 ρ 尽可能小,且误码率可以达到 6σ(约 10^{-23}),我们得到平衡后的参数:$du=23$,$dv=17$,$dp=16$,此时的密文膨胀率为 $\frac{2du+dv\cdot 2}{dp}=5.0$。

4.2.2 正确性分析

整个方案在进行多项式计算时均是在环 $R_q^n=Z_q[x]/f(x)$ 中进行,具体为:令多项式 $W=w_0+w_1x+\cdots+w_{n-1}x^{n-1}$,多项式 $U=u_0+u_1x+\cdots+u_{n-1}x^{n-1}$,则环 R_q 上的多项式乘法为:

$$Y=W\cdot U=y_0+y_1x+\cdots+y_{n-1}x^{n-1}$$

$$=(y_0,\cdots y_{n-1})$$

$$=(w_0,\cdots,w_{n-1})\cdot\begin{bmatrix}u_0 & u_1 & u_2 & \cdots & u_{n-1}\\ -u_{n-1} & u_0 & u_1 & \cdots & u_{n-2}\\ -u_{n-2} & -u_{n-1} & u_0 & \cdots & u_{n-3}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ -u_1 & -u_2 & -u_3 & \cdots & u_0\end{bmatrix}$$

本方案中离散整数型随机变量噪声 $\boldsymbol{e}$ 是根据 Bai[16] 的方案生成的,其分布 χ 近似于 $N(0,\eta/2)$,分布在$[-\eta/2,\eta/2]$之间。

考虑 ε_u 近似是期望为 0,方差为 $\frac{[2\times round(\frac{q}{2^{du+1}})]^2}{12}$ 的离散均匀分布。而变量 $\varepsilon_u-\boldsymbol{e}_1$ 可以近似考虑为分布在$[-round(\frac{q}{2^{du+1}})-\eta,round(\frac{q}{2^{du+1}})+\eta]$上的近似离散均匀分布。其期望为 0,方差为 $\frac{[2\times round(\frac{q}{2^{du+1}})+\eta]^2}{12}$。

由于变量 $\boldsymbol{s}$ 与 e_2 的期望为 0,方差为 $\frac{\eta}{2}$,且与 $\varepsilon_u-\boldsymbol{e}_1$ 相互独立,根据环上的多项式乘法知多项式 $\boldsymbol{s}^{\mathrm{T}}(\varepsilon_u-\boldsymbol{e}_1)$ 中的每个系数均为 $2n$ 个相互独立同分布的变量之和,根据中心极限定理可知,其分布近似于 $N(0,2n\cdot\frac{\eta}{2}\cdot\frac{[round(\frac{q}{2^{du+1}})+\eta]^2}{3})$。

由于变量 $\boldsymbol{e}^{\mathrm{T}}\boldsymbol{r}$ 中的 $\boldsymbol{e}^{\mathrm{T}}$ 和 $\boldsymbol{r}$ 相互独立,根据环上的多项式乘法可知多项式 $\boldsymbol{e}^{T}\boldsymbol{r}$ 中的每个系数均为 $2n$ 个相互独立同分布的变量之和,根据中心极限定理可知其分布近似于 $N(0,2n\cdot\frac{n^2}{4})$。

为使方案的正确率尽可能达到 a 倍标准差 σ,那么需要保证式(6)成立,即:

$$a(\sqrt{\frac{n\cdot\eta\cdot(\frac{q}{2^{du+1}}+n)^2}{3}}+\sqrt{\frac{n\cdot\eta^2}{2}}+\sqrt{\frac{\eta}{2}})+\frac{q}{2^{dv+1}}<\frac{q}{2^{dp+1}}$$

考虑到解密正确率以及密文膨胀率,二者经平衡后选定 $a=9$,$du=23$,$dv=17$,$dp=16$。此时我们通过 Maple 积分标准正态分布函数得到 9σ 的误码率约为 10^{-23}。

4.2.3 可否认性分析

本文方案可以做到发送方和接收方的双向可否认,双方需要在加密之前预先约定好密钥 $\boldsymbol{s}$ 和 $\boldsymbol{s\_fake}$,或者从可信任的安全信道通信获得 $\boldsymbol{s}$ 和 $\boldsymbol{s\_fake}$。

当发送方使用 *Enc_fake* 进行加密得到密文 $\boldsymbol{C}=(C_1,C_2,C_3)$被敌手胁迫时,发送方可以对其声称密文 C_3 是通过 *Enc* 加密得到的 C_2,密文 C_2 是通过 *Enc* 加密得到的 C_3,而敌手无法正确区分。然后向其交代出加密时所用到的随机数 $\boldsymbol{r}$、假密钥 $\boldsymbol{s\_fake}$,以及假明文 m',并声称密文是通过 *Enc* 生成的。

敌手对 m' 进行 Enc 加密得到 C_3，通过验证，即：

$Enc\_fake(m',\boldsymbol{r},\boldsymbol{s\_fake})\rightarrow C_3=C_2\leftarrow Enc(\boldsymbol{r},\boldsymbol{s\_fake},m')$

$Enc\_fake(m,\boldsymbol{r},\boldsymbol{s})\rightarrow C_2=C_3\leftarrow Enc(\boldsymbol{r},\boldsymbol{s\_fake})$

最终敌手无法发现加密方使用了 Enc_fake 加密而被欺骗。

当接收方被敌手胁迫时，接收方向胁迫者交代假密钥 $\boldsymbol{s\_fake}$，并解密 $C_3-\boldsymbol{s\_fake}\cdot\boldsymbol{C}_1=\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{r}+\boldsymbol{s\_fake}^{\mathrm{T}}\cdot e_2+e_4+m'=\varepsilon+m'$ 得到假明文 m' 用来欺骗胁迫者。

为了验证经过 Enc_fake 加密后得到的密文 C_3 和经过 Enc 加密后得到的密文 C_2 看似服从同一分布，敌手无法正确区分(即 MLWE 困难问题，文献[6]给出了该 MLWE 问题的证明)，我们进行了如下卡方检验实验。

通过 Enc_fake 加密并压缩后得到 2.56×10^9 个密文 C_3，考虑压缩密文 C_3 的取值范围为 $(0,2^{dv})$，将区间 $(0,2^{dv})$ 分为 1000 段，然后通过卡方检验公式计算均匀分布和密文 C_3，在自由度为 1000 时卡方值约为 1970。

通过 Matlab 计算当自由度为 1000、卡方值为 1142 时，有 0.001 的概率可以将密文分布与均匀分布进行区分。当自由度为 1000，卡方值为 1400 时，仅有 10^{-15} 的概率可以区分两个分布。当自由度为 1000，卡方值为 1970 时可以区分两个分布的概率过低，已超出 Matlab 计算精度(显示结果为 0.0)。由此可以推知，在卡方值为 1970 时概率会远低于 10^{-15}，敌手很难正确区分两个密文分布。

4.2.4 安全性分析

本文方案的安全性是基于格上的困难问题 Module-SIVP 的，即敌手无法区分均匀分布与分布 $\boldsymbol{As}+\boldsymbol{e}$，在 Module-SIVP 问题是困难的情况下，该方案是 IND-CPA 安全的，即：$Adv_{CPA}(\mathscr{A})\leqslant Adv_{\mathrm{MLWE}}(\mathscr{A})$。

使用基于 Game 的方法证明：

Game0　挑战者 C 按照 $Keygen$ 产生密钥 $\boldsymbol{s},\boldsymbol{s\_fake}$，敌手 $\mathscr{A}$ 从明文空间中任选两个明文 m_0 和 m_1 交给挑战者 C，挑战者 C 随机选择 $b\in\{0,1\}$，将 m_b 以 1/2 的概率用 Enc 或 Enc_fake 加密，并将加密得到的密文发送给敌手 $\mathscr{A}$，敌手 $\mathscr{A}$ 对密文进行猜测并输出猜测结果 b'。如果 $b'=b$，则敌手 $\mathscr{A}$ 攻击成功，敌手的攻击优势记为：

$$Adv_{CPA}(\mathscr{A})=\left|\Pr(b=b'\ inGame_0-\frac{1}{2})\right|=\frac{1}{2}\left|\Pr(b=b'\ inGame_{0Enc})-\frac{1}{2}\right|+(1-p)\left|\Pr(b=b'\ inGame_{0Enc\_fake})-\frac{1}{2}\right|$$

Game1　Game1 改变 Game0 中使用 Enc 加密时 $\boldsymbol{b}=\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}$ 的生成过程，均匀随机选取 $\boldsymbol{b}'\leftarrow R_q^k$，而敌手 $\mathscr{A}$ 区分 $\boldsymbol{b}$ 和 $\boldsymbol{b}'$ 与解决 MLWE 困难问题同样困难，因此 Game1 对 $Game_{0Enc}$ 的优势为：

$$\left|\Pr(b=b'\ inGame_1)-\Pr(b=b'\ inGame_{0Enc})\right|\leqslant Adv_{\mathrm{MLWE}}(\mathscr{A})$$

Game2　Game2 改变 Game0 中使用 $Encrypt\_fake$ 加密时 $\boldsymbol{b}_1=\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}$ 和 $\boldsymbol{b}_2=\boldsymbol{A}\cdot\boldsymbol{s\_fake}+\boldsymbol{e}$ 的生成过程，均匀随机选取 $\boldsymbol{b}_1'\leftarrow R_q^k$ 以及 $\boldsymbol{b}_2'\leftarrow R_q^k$，而敌手 $\mathscr{A}$ 区分 $\boldsymbol{b}_1$ 和 $\boldsymbol{b}_1'$ 以及 $\boldsymbol{b}_2$ 和 $\boldsymbol{b}_2'$ 与解决 MLWE 困难问题同样困难，因此敌手在 Game1 中的优势为：

$$\left|\Pr(b=b'\ inGame_2)-\Pr(b=b'\ inGame_{Enc\_fake})\right|\leqslant Adv_{\mathrm{MLWE}}(\mathscr{A})$$

Game3　Game3 改变 Game1 中生成挑战密文的方式 Enc，使用均匀随机选取的密文 $(\boldsymbol{C}_1',C_2',C_3')\leftarrow R_q^k\times R_q\times R_q$ 替代原密文 $(\boldsymbol{C}_1,C_2,C_3)$，敌手 $\mathscr{A}$ 区分 $(\boldsymbol{C}_1,C_2,C_3)$ 和 $(\boldsymbol{C}_1',C_2',C_3')$ 与解决 MLWE 困难问题同样困难，因此敌手 $\mathscr{A}$ 在 Game3 中的优势为：

$$\left|\Pr(b=b'\ inGame_3)-\Pr(b=b'\ inGame_1)\right|\leqslant Adv_{\mathrm{MLWE}}(\mathscr{A})$$

Game4　Game4 改变 Game2 中生成挑战密文的方式 Enc_fake，使用均匀随机选取的密文 $(\boldsymbol{C}_1',C_2',C_3')\leftarrow R_q^k\times R_q\times R_q$ 替代原密文 $(\boldsymbol{C}_1,C_2,C_3)$，敌手 $\mathscr{A}$ 区分 $(\boldsymbol{C}_1,C_2,C_3)$ 和 $(\boldsymbol{C}_1',C_2',C_3')$ 与解决 MLWE 困难问题同样困难，因此敌手 $\mathscr{A}$ 在 Game3 中的优势为：

$$\left|\Pr(b=b'\ inGame_4)-\Pr(b=b'\ inGame_2)\right|\leqslant Adv_{\mathrm{MLWE}}(\mathscr{A})$$

由于 Game3 和 Game4 中所挑战的密文与明文 b 相互独立，故有：

$$\Pr(b=b'\ inGame_3)=\Pr(b=b'\ inGame_4)=\frac{1}{2}$$

因此：

$$Adv_{CPA}(\mathscr{A})=\frac{1}{2}\left(\left|\Pr(b=b'\ inGame_4-\Pr(b=b'\ inGame_2)\right|\right)+\frac{1}{2}\left(\left|\Pr(b=b'\ inGame_2)-\Pr(b=b'\ inGame_{0Enc\_fake})\right|\right)+\frac{1}{2}\left(\left|\Pr(b=b'\ inGame_3)-\Pr(b=b'\ inGame_1)\right|\right)+\frac{1}{2}\left(\left|\Pr(b=b'\ inGame_1)-\Pr(b=b'\ inGame_{0Enc})\right|\right)\leqslant Adv_{\mathrm{MLWE}}(\mathscr{A})$$

5 效率及方案对比

以往提出的可否认加密方案的效率大都不是很高，而本文提出的方案在效率上有着的明显优势。相比 2009 年 Jaydeep[3] 提出的比较完整的基于二次剩余的方案，本文方案的效率提高了 800 余倍，膨胀率约为其 1/4000。相比基于容错学习 LWE 的方案，本文方案的效率提升了约 4000 倍，膨胀率约为其 1/1000。

考虑这样一个应用场景：一个携带笔记本电脑的人被胁迫方胁迫，胁迫者令其解密电脑中的密文。那么我们通过 MacBookPro2017 (2.3GHz Intel Core i5 8GB 内存)用 C++ 对本文方案进行实现，并分别对多个不同的 100 MB 的文档、图片以及视频文件进行 100 次加密，得到该方案在不同安全参数下的平均消耗时间，如表 1 所列。

表 1　加密和解密效率

Table 1　Encryption and decryption efficiency

k	攻击次数	加密效率/(kB/s)	解密效率/(MB/s)	膨胀率
2	2^{100}	670	1.3	5.0
3	2^{160}	440	1	6.4375

考虑到以往提出的方案要么是发送方可否认加密，要么是接收方可否认加密，或需要可信第三方，或有一定的错误概

率，我们对各方案的功能和效率进行对比，如表 2 和表 3 所列。可以看出，本抗量子的方案还有着双向可否认、出错概率低、加密效率高，以及不需要可信第三方的优势。

表 2 可否认加密方案的功能对比

Table 2 Functional comparison of deniable encryption schemes

	发送方可否认	接收方可否认	出错概率	第三方
文献[1]	可	可	大	需要
文献[4]	可	否	较大	不需要
文献[5]	否	可	小	需要
文献[6]	否	可	小	不需要
文献[7]	否	可	0	不需要
文献[17]	可	否	较大	不需要
文献[18]	可	可	较大	需要
文献[19]	可	可	较大	需要
文献[20]	可	否	较大	不需要
本文方案	可	可	0	不需要

表 3 可否认加密方案的效率对比

Table 3 Efficiency comparison of deniable encryption schemes

	加密效率	密文膨胀率	密钥大小
文献[2]	约 6 B/s	约 1:100000	2 kB
文献[3]	约 80 B/s	约 1:20000	2 kB
基于 LWE	约 160 B/s	约 1:12000	约 20 MB
本文方案	约 670 kB/s	1:5.0	2 kB

结束语 由于以往提出的可否认加密方案普遍存在不实用以及无法抵御量子攻击的问题，本文提出了一种分享密钥类的实用双向可否认加密方案，其安全性可规约到格上的困难问题，即 MLWE 问题。本文通过理论证明和实验印证了所提方案的可行性。在对称加密构造的加密算法基础之上，该方案可以稍作变形改造成公钥可否认加密方案，但只可以对接收方进行否认[20]。因此，如何构造双向可否认公钥加密方案成为未来的研究方向，并且本文利用格困难问题构造后量子双向可否认方案的方式，可应用于其他形式的困难问题来进行相似的构造。

参 考 文 献

[1] CANETTI R, DWORK C, NAOR M, et al. Deniable encryption [C]// Annual International Cryptology Conference. Springer, 1997: 90-104.

[2] IBRAHIM M H. A Method for Obtaining Deniable Public-Key Encryption[J]. International Journal of Network Security, 2009, 8(1): 1-9.

[3] JAYDEEP H D N. Sender-Side Public Key Deniable Encryption Scheme[C]// International Conference on Advances in Recent Technologies in Communication & Computing. IEEE, 2009: 27-28.

[4] MAREK K, PRZEMYALAW K, MIROSLAW K. Practical deniable encryption[C]// Proc. of the 34th Conference on Current Trends in Theory and Practice of Computer Science. Berlin: Springer-Verlag, 2008: 599-609.

[5] IBRAHIM M H. Receiver-deniable Public-Key Encryption[J]. International Journal of Network Security, 2009, 8(2): 159-165.

[6] KLONOWSKI M, KUBIAK P, KUTYŁOWSKI M. Practical Deniable Encryption[J]. Theory and Practice of Computer Science, 2008, 4910: 599-609.

[7] MENG B, WANG J Q. An Efficient Receiver Deniable Encryption Scheme and Its Applications[J]. Journal of Networks, 2010, 5(6): 683-690.

[8] CRAMER R, GENNARO R, SCHOENMAKERS B. A Secure and Optimally Efficient Multi-Authority Election Scheme[C]// International Conference on the Theory & Applications of Cryptographic Techniques. Springer, 1997: 481-490.

[9] HIRT M, SAKO K. Efficient Receipt-Free Voting Based on Homomorphic Encryption[J]. Lecture Notes in Computer Science, 2000, 1807: 539-556.

[10] REGEV O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[J]. Journal of the Acm, 2009, 56(6): 1-40.

[11] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2010: 1-23.

[12] LANGLOIS A, STEHLE D. Worst-case to average-case reductions for module lattices [J]. Designs, Codes and Cryptography, 2015, 75(3): 565-599.

[13] BOS J, DUCAS L, KILTZ E, et al. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM[J]. IACR Cryptology ePrint Archive, 2017: 634-650.

[14] KE C S, WU W Y, FENG Y. Low Expansion Rate Encrption Algorithm Based on MLWE [J]. Computer Science, 2019, 46(4): 145-150.

[15] O'NEIL A, PEIKERT C, WATERS B. Bi-Deniable Public-Key Encryption[C]// Annual International Cryptology Conference. Springer, 2011: 525-542.

[16] BAI S, LANGLOIS A, LEPOINT T, et al. Improved security proofs in lattice-based cryptography: using the Renyi divergence rather than the stastical distance[C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2015: 3-24.

[17] WU W Y, ZHENG J T, FENG Y. Sender-side Public Key Deniable Encryption Scheme Based on LWE[J]. Advanced Engineering Sciences, 2020, 52(2): 1-8.

[18] SUN L, WANG C F. Practical deniable encryption scheme and security proofs[J]. Application Research of Computers, 2010, 27(10): 3862-3865.

[19] SUN L. Deniable Encryption and Deniable Protocol [D]. Lanzhou: Northwest Normal University, 2011.

[20] ZHENG J T. Public Key Deniable Schemes Based on Lattice Problems [D]. Beijing: University of Chinese Academy of Sciences, 2020.

ZHENG Jia-tong, born in 1995, postgraduate. His main research interests include lattice encryption and deniable encryption.

WU Wen-yuan, born in 1976, Ph.D, researcher, Ph.D supervisor. His main research interests include lattice encryption, automatic reasoning and symbolic calculation.