NTRU 全同态掩码防御方案

杨亚涛[1),3)] 刘博雅[1)] 孙亚飞[3)] 李子臣[2)]

[1)](北京电子科技学院电子与通信工程系 北京 100070)

[2)](北京印刷学院信息工程学院 北京 102600)

[3)](西安电子科技大学通信工程学院 西安 710071)

摘 要 为了抵抗量子计算机的攻击,相关的后量子密码算法被先后提出. NTRU(Number Theory Research Unit)密码算法是基于格理论的典型算法之一,在 NTRU 密码方案的硬件设计及实现过程中,主要会面临格攻击、简单能量攻击、差分能量攻击及相关能量攻击等风险. 为了解决 NTRU 算法在实现过程中的侧信道攻击安全隐患,提出一种新的全同态掩码防御方案,并给出电路设计参考模型,所提出方案能够对 NTRU 算法所有系数执行掩码操作并防范能量攻击. 本方案的密钥生成部分采用高斯抽样算法,解密部分采用同态加密实现密文间的全同态运算. 设计的全同态掩码方案电路模型中,根据算法功能分为数据采样区、存储区及运算区. 本方案通过高斯取样生成密钥,能防范格攻击;通过密文之间的同态运算,可以实现多项式所有系数同时掩码;通过分析算法的同态性,验证了本方案的正确性;通过分析方案的实现过程,论证了该方案能够有效防御选择密文攻击、差分能量攻击、零值攻击及相关能量攻击.

关键词 NTRU;能量攻击;选择密文攻击;掩码;同态加密

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2019.02742

Fully Homomorphic Masking Defense Scheme Based on NTRU

YANG Ya-Tao[1),3)] LIU Bo-Ya[1)] SUN Ya-Fei[3)] LI Zi-Chen[2)]

[1)](*Department of Electronic and Communication Engineering, Beijing Electronic Science & Technology Institute, Beijing* 100070)

[2)](*College of Information Engineering, Beijng Institute of Graphic Communication, Beijing* 102600)

[3)](*School of Telecommunication Engineering, Xidian University, Xi'an* 710071)

Abstract In order to resist the attack from quantum computer, the algorithms and protocols based on post quantum cryptography (PQC) had been proposed one by one, generally speaking, post quantum cryptography mainly contained lattice based cryptosystem (LBC), Hash based cryptosystem (HBC), multivariate public key cryptosystem (MPKC), coding theory based cryptosystem (CBC), LBC has been widely researched for its better mathematical properties and security. However, even if the cryptographic algorithm itself is secure, it is also probable to suffer various attacks during its implementation process inevitably. Among them, side channel attack has brought more and more threats to this kind of post quantum cryptographic algorithm. NTRU (Number Theory Research Unit) cryptosystem is one of the typical LBC algorithms; the security of this scheme is based on the shortest vector problem (SVP), it has been the IEEE P1363 standard and finance service industrial standard in USA. During the hardware design and implementation process of NTRU cryptography, there are many potential risks such as Lattice Attack, Simple Power Attack, Differential Power Attack and Related Power Attack and so on.

收稿日期:2018-04-13;在线出版日期:2019-03-20. 本课题得到"十三五"国家密码发展基金(MMJJ20170110)资助.**杨亚涛**,博士,副教授,硕士生导师,主要研究领域为密码学与通信安全. E-mail: yy2008@163.com. **刘博雅**(通信作者),硕士研究生,主要研究方向为密码协议、网络安全. E-mail: lby330613263@163.com. **孙亚飞**(通信作者),硕士研究生,主要研究方向为密码学、网络信息安全. E-mail: yfsun0112@163.com. **李子臣**,博士,教授,博士生导师,主要研究领域为密码学、信息安全、后量子密码、数字水印等.

Lee et al. has implemented the Power Attacks for NTRU cryptosystem in 2010; Wang et al. has implemented the attack through combining Chosen Ciphertext Attack and Power Attack in NTRU-Based wireless body area networks in 2013. Up to now, there is still no any research achievement or paper about defense scheme based on Homomorphic Masking technology to resist side channel attack of NTRU cryptosystem. Masking technology is one of common countermeasures to resist side channel attack. By masking the intermediate values and variables, the calculating operations are executed under the masked state, which can effectively guarantee the security of data. The masking technology contains Boolean Masking and Arithmetic Masking. As an important property of public key cryptosystem, homomorphic computation algorithm can operate ciphertext, and can achieve Arithmetic Masking between ciphertext. In order to solve the problems of side channel attack in the implementation process of NTRU, a novel Fully Homomorphic Masking (FHM) defense scheme is proposed and its circuit design model is given. Our scheme can effectively implement the mask for all the polynomial coefficients and resist the Power Attack. In this scheme, the key generation uses Gaussian abstraction algorithm, and the decryption part applies the homomorphic encryption to realize fully homomorphic calculation between ciphertexts. In the circuit model of fully homomorphic masking scheme we constructed, data sampling area, storage area, and operation area are divided according to the algorithm function. By analysis, it is obvious that lattice attack can be avoided as if the key of NTRU is generated by Gaussian abstraction, and that all the coefficients of polynomials can be masked by the homomorphic calculation between the ciphertext. Because of double mask, it can effectively resist the Zero Value Attack. With the analysis of the algorithm homomorphism, the correctness of our scheme has been verified; it shows that Chosen Ciphertext Attack, Differential Power Attack, Zero Value Attack and Correlation Power Attack all can be resisted effectively in the implementation process of this scheme.

Keywords　number theory research unit; power attack; chosen ciphertext attack; masking; homomorphic encryption

1　引　言

后量子密码体系主要包括四个分支：基于格理论的后量子密码、基于 Hash 的后量子密码、基于多变量的后量子密码以及基于编码理论的后量子密码，其中基于格理论的后量子密码体制由于其良好的数学性质而受到广泛的研究. 然而，即使算法本身的设计是安全的，在其实现过程中也难免会遭受各种各样的攻击，其中，侧信道攻击给后量子密码体制带来了越来越大的安全威胁.

1998 年，美国布朗大学的 Hoffstein、Pipher 和 Silverman 三位数学教授发明的一种公钥密码体制 NTRU(Number Theory Research Unit)[1]. 相比较于基于椭圆曲线上的离散对数问题[2]和基于大数分解问题[3]的公钥密码体制而言，NTRU 的安全性依赖于格上的最短向量问题[4]，具备抗量子计算机攻击的能力. NTRU 自从被提出以来就备受关注，目前已正式成为 IEEEP1363 标准及美国金融服务行业标准[5].

由 Kochor 提出的侧信道攻击[6-7]，主要是根据密码算法在执行过程中的消耗信息进行破译. 此后，侧信道攻击与防御技术的研究成为密码学的一个重要分支，受到了广泛关注. 能量攻击是最重要、最有效的侧信道攻击形式之一，尤其对智能卡等设备的实际安全性造成严重的威胁. 而 NTRU 算法特别适合用于智能卡、无线保密网及认证系统等业务[8]，也就是说 NTRU 的算法面临着侧信道攻击的风险.

能量攻击通过利用密码设备的能量消耗特征来获取秘密信息，是一种非接触式的攻击方法. 差分能量攻击通过分析芯片运行过程中的能量消耗，能够实现对密钥的恢复，是一种高效的密码分析方式. 针对基于 NTRU 算法的密码系统，Atici 等人[9]首次给出能量攻击方式，Lee 等人[10]给出了简单能量攻击、差分能量攻击的方法并针对所提攻击方法给出

三种不同的防御措施. Wang 等人[11]对基于 NTRU 的无线体域网进行能量分析并提出相应的防御措施，通过结合选择密文攻击对 Lee 等人提出的防御措施进行攻击，取得良好的攻击效果. 目前关于 NTRU 算法的分析得到了广泛的研究[12-15].

在 NTRU 算法的实现过程中，密钥生成过程存在格攻击的安全问题[16]，且存在选择密文攻击及能量攻击等问题. 同态是公钥密码算法的一种常见性质，同态算法可以对密文进行操作，并能实现密文间的掩码. 掩码技术包含布尔掩码和算术掩码，通过掩码技术，可以掩盖算法执行过程中的中间变量和中间数值，运算操作中的数据在被掩盖状态下运行，进而可以防范侧信道攻击，保障数据安全. 截止目前，还没有看到基于同态掩码来防范侧信道攻击方案.

本文通过对 NTRU 算法进行分析，在密钥生成部分，通过采用格上的高斯抽样算法生成密钥对，从而避免格攻击，并且不改变密钥的分布. 为了防御选择密文攻击，利用算法的同态特性对密文进行改造，对所处理密文进行随机化，同时该方法能有效的抵抗零值攻击、二阶差分能量攻击.

2 NTRU 算法介绍

NTRU 算法是在多项式环 $Z[x]/(x^N-1)$ 的基础上实现的，环上的多项式 f 可以表示成一个多项式或者向量的形式：

$$f=\sum_{i=0}^{N-1} f_i x^i=[f_0,f_1,\cdots,f_{N-1}].$$

环上的乘法运算 $*$ 是卷积乘，假设：

$$f=[f_0,f_1,\cdots,f_{N-1}],$$
$$g=[g_0,g_1,\cdots,g_{N-1}],$$
$$h=[h_0,h_1,\cdots,h_{N-1}],$$

则多项式 f 和 g 的卷积 h 定义如下：

$$h=f*g,$$

其中，

$$h_k=\sum_{i=0}^{k} f_i g_{k-i}+\sum_{i=k+1}^{N-1} f_i g_{N+k-1}$$
$$=\sum_{i+j\equiv k \bmod N} f_i g_j (0\le k\le N-1).$$

因为 NTRU 算法只涉及多项式环上的乘法和求模运算，与传统公钥密码算法的模幂运算相对比，其运算速度有大幅度提高. 同时，NTRU 的密钥产生算法相对简单，使得它有着十分广阔的应用范围及应用场景. NTRU 算法由密钥生成、加密算法及解密算法三部分组成，如下所述：

(1) 密钥产生 $KeyGen$：

NTRU 算法涉及到三个公开参数 (N,p,q)，其中，一般选取 $p=3$，$q=2^k$，$N-1$ 是多项式的最高次数. 该算法构建在商环 $Z[x]/(x^N-1)$ 上；$L(a,b)$ 表示环中满足 a 个系数为 1，b 个系数为 -1，其他系数均为 0 的所有整系数多项式.

首先，随机提取两个多项式 $f\in L(d_f+1,d_f)$ 和 $g\in L(d_g,d_g)$，其中 $d_f,d_g\in Z$ 且需要保证 f 存在逆元 f_p 和 f_q，使得 $f*f_p=1(\bmod p)$，$f*f_q=1(\bmod q)$；然后，计算 $h(x)=pf_q*g(\bmod q)$；最后，根据参数生成 NTRU 的公钥为 (N,p,q,h)，私钥为 f 和 f_p，且私钥可以表示为 $f=1+pf'$ 的形式.

(2) 加密算法 Enc：

首先，将明文消息 m 编码为对应的多项式 $m(x)$；然后，用户选取随机多项式 $r\in L(d_r,d_r)$，$r\in Z$；最后，计算：$c=[pr*h+m(x)](\bmod q)$，则 c 即为所求密文.

(3) 解密算法 Dec：

首先，解密者得到密文 $c=[pr*h+m(x)](\bmod q)$；然后，利用私钥 f 计算 $a(x)\equiv c*f(\bmod q)$；其次，计算 $m'(x)=a(x)*f_p$；最后，计算明文：$m(x)\equiv m'(x)(\bmod p)$.

3 NTRU 算法分析

NTRU 密码算法自被提出以来，受到了广泛的研究和分析，针对其攻击分为理论上的攻击如格攻击，实现上的攻击如简单能量攻击、差分能量攻击等. 下面分类对其进行分析.

3.1 格攻击

文献[16]指出由 $h'=f_q*g(\bmod q)$ 可得 $f*h'=g+q*a'$，$a'\in Z_q[x]/(x^N-1)$，那么向量集：$L=\{(u,v):u*h'=v(\bmod q),u,v\in Z^N\}\in Z^{2N}$ 中肯定包含向量 (f,g)，为使解密能够成功，需要 $\|f\|=2d_f-1$ 和 $\|g\|=2d_g$ 都远小于 N，因此，如果能够从 L 中找出最短向量，就有可能恢复出 (f,g). 利用 LLL 算法可以提高找到最短向量的概率.

3.2 简单能量攻击

在 NTRU 算法的解密过程中，其核心运算为

$$f*c(\bmod q)=(1+pf')*c(\bmod q)$$
$$=c+pf'*c(\bmod q).$$

因此，只要知道 f' 的值，就可以实现对算法的破解，因此对算法的破解转化为求解 $t=f'*c$. 假设

$N=8$，$f'=[10011010]$，则卷积运算过程如图 1 所示，其中 Add 表示多项式系数取模相加.

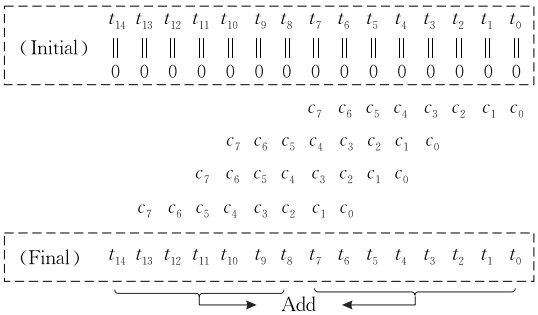

图 1　卷积运算过程

在简单能量攻击(Simple Power Attack，SPA)过程中不需要使用任何的统计分析方法，攻击者只要观察目标操作运算执行过程中的能量消耗即可实现对算法的破译. 假设在 SPA 过程中，对于非零整数 a 和 b，计算 $a+b$ 和 $a+0$ 的能量消耗是不同的. 因此，攻击者能够选取系数都非零的密文多项式对算法进行攻击，根据能量消耗的变化确定相应的值. 在上述的卷积运算过程中，对于第 2 行而言，下面的每一行与前面的行相加都是两个非零值相加，而第一行与初始化的内存单元值相加则是零值与非零值相加，因此攻击者能够根据能量的消耗情况确定出第一行的值，同理，逐行递推，最后利用穷搜的方法就能得到整个 f' 的值.

3.3　相关能量攻击

相关能量攻击(Correlation Power Attack，CPA)是比 SPA 更加有效的一种方式. 在 CPA 攻击中，攻击者首先使用同一密钥进行多次解密运算，采集其能量曲线并求平均；然后，计算能量迹与多项式系数之间的关系. 由图 1 可知，若第一行中的 c_5 被加到某一个寄存器上，则当第二行中的 c_2 也被加到该寄存器上时，因为能量消耗与寄存器值的变化相关，因此，在收集大量的能量迹之后，可根据计算所得的相关系数对密钥进行破译.

3.4　差分能量攻击

在一般的差分能量攻击过程中，攻击者首先使用同一密钥进行多次解密运算，采集其能量曲线并求平均；然后，使用猜测的密钥对同一密文进行多次计算并采集能量求平均；最后，根据能量迹的差值进行判断，若出现峰值，则说明相应的比特位值猜测正确，反之，则说明猜测错误. 如此反复进行猜测实验，最终可以实现对密钥的破译.

选择密文攻击是指攻击者能够伪造合法数据，结合算法具体运算过程，利用运算过程中泄露的中间值信息，实现对算法的攻击. 下面结合选择密文与差分能量攻击的思想，给出一种针对 NTRU 算法更加有效的分析方法：

假设用户选择密文 $c=[0,0,\cdots,0]$ 并进行多次运算，求得其平均曲线，用 T_1 表示；然后，用户再选择一个密文 $c=[a,0,\cdots,0]$ 进行多次运算，求得其平均曲线，用 T_2 表示；最后，对 T_1，T_2 做差得 $\Delta T=T_1-T_2$，值不同的位置便会出现峰值. 其中值为 a 的位置能够被有效的恢复出来. 计算过程如图 2 所示.

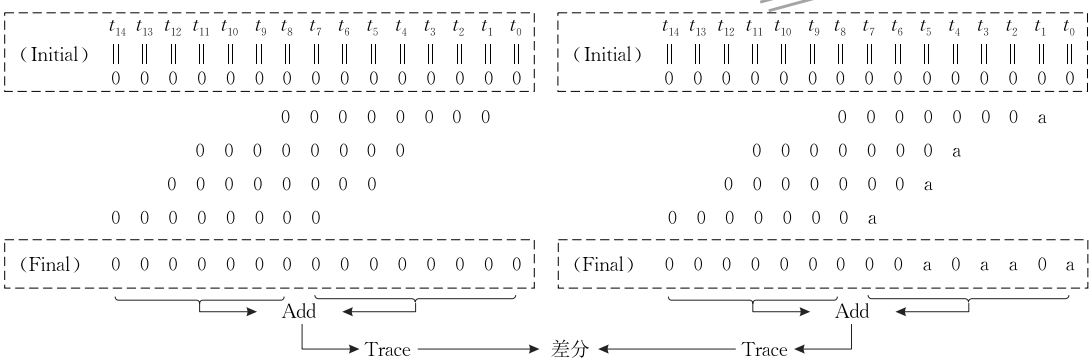

图 2　针对 NTRU 算法的差分攻击过程

4　基于NTRU算法的全同态掩码方案

Lee 等人[10]在提出对NTRU算法的攻击的同时，还提出针对侧信道攻击的防御策略. 分为如下 3 种：

(1)随机化初始寄存器. 在简单能量攻击中，假设寄存器的初始值都是零，因此可以根据计算 $a+b$ 和 $a+0$ 的能量消耗的不同来实现破译. 为了抵抗简单能量攻击，在算法开始前对每个寄存器都进行随机赋值，在算法执行完后再把随机数从对应的寄存器中减去，使得整个算法的执行过程中没有 $a+0$ 的操作，从而使得 SPA 无效.

(2)随机盲化密文多项式.通过引入随机整数 r,计算 $c_i+r(i=0,1\cdots,N-1)$.在解密的最后将每个寄存器中的值减去 $dr \bmod q$ 即可恢复原始值.

(3)随机化存储密钥.密钥是固定的,因此针对密钥的计算,每比特都是固定的,为了抵抗其攻击,将密钥的比特存储进行随机化,使得每次运算中取值顺序是不固定的,因此攻击者无法利用统计方法恢复密钥值.

Lee 等人的方法二是通过引入一个随机数,然后对某一比特进行掩码运算,如果需要同时对所有比特位均实施掩码,则会导致需要生成大量的随机数,增加资源存储开销,降低方案的性能.本节在此方法的基础上,通过改变密钥的生成方式来抵抗格攻击[17],利用 NTRU 密码算法本身的同态特性[18-23]对密文进行随机化处理,对多项式所有系数进行多重掩码,能够有效的防御选择密文攻击、差分能量攻击、零值攻击及相关能量攻击.

4.1 基于 NTRU 的实现方案

新的方案基于原有的 NTRU 方案,并在此基础上引入 R-LWE 思想,设计一种全同态掩码防御方案.其中生成的密文可参考文献[19]提出的 BitDecomp 技术转换为 $l\times l$ 的密文矩阵,具体改进如下:

(1)密钥生成 $KeyGen$

①选择标准差 σ,生成密钥 f 且可以表示为:$f=pf'+1$,其中 f'是从离散高斯分布中取样而来的多项式.

②从离散高斯分布中取样 g,使其满足 $g \bmod q \in R_q$.

③输出私钥 $s_k=f$,公钥 $p_k=h=pgf^{-1}$.

(2)加密算法 Enc

加密运算为:$c=hs+pe+m$.对于明文消息 m,首先将其映射为环上的元素;其次,随机抽样选取多项式 s,e;然后,根据加密运算步骤实现对消息 0 的加密,即 $c^*=hs+pe$;最后,计算密文 $c=Flatten(\text{BitDecomp}(I_{l\times l}\cdot m+c'))$.

其中,Flatten 函数是用于将矩阵转化为 0/1 矩阵.其详细用法参考文献[19].

(3)解密算法 Dec

首先,随机生成消息 m_1,m_2,根据加密算法对其进行加密运算得密文 c_1,c_2,由于不是所有的随机消息都是可用的,也不是所有的随机消息都是可靠的,通常情况下,要确保生成的密文系数是随机的、非空的.

其次,对密文进行运算得 $C=(c+c_1)\cdot c_2$;然后,计算 fC,如下:

$$\begin{aligned} fC &= f((c+c_1)\cdot c_2)\\ &= f(2hs+2pe+m+m_1)(hs+pe+m_2)\\ &= 2fhshs+4fhspe+2fhsm_2+2fpepe+\\ &\quad 2fpem_2+hfs(m+m_1)+\\ &\quad fpe(m+m_1)+f(m+m_1)m_2\\ &= f(m+m_1)m_2 \pmod p\\ &= (m+m_1)m_2. \end{aligned}$$

最后,根据随机消息 m_1,m_2,求出消息 m.

4.2 全同态掩码方案电路设计

针对上述所提方案,设计一种可实现的加解密电路.

加密电路

在上述新的方案中,加密运算为 $c=hs+pe+m$,其中 s,e 为高斯抽样随机多项式,h 为公钥,p 为整数,m 为待加密消息.整个加密电路主要分为采样区、数据区、控制运算区.具体实现电路如图 3 所示.

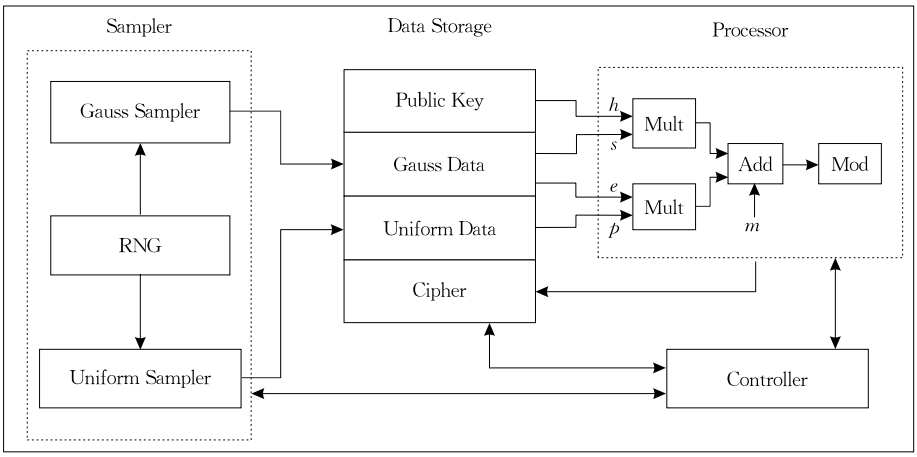

图 3 改进的 NTRU 加密电路设计

其中，各部分对应的功能如下：

(1) 采样区

Uniform Sampler：产生多项式最高次数 $N-1$，模数 p. 这些参数在每次加密过程中保持不变，可以在生成之后直接存储至 ROM 中，因此在实际实现的时候可以将此部分忽略.

RNG：产生随机数，可以采用 $\log_2 N$ bits 的 LFSR 实现.

Gauss Sampler：满足离散高斯分布的序列，组成加密过程中要用到的多项式 s，e. 其中高斯采样过程中需要引入随机数.

(2) 数据区

Public Key：只读存储器 ROM，用于实现对公钥的存储；

Uniform Data：只读存储器 ROM，存储模数；

Gauss Data：读写存储器 RAM，用于在每次运算时进行高斯多项式的读写操作；

Cipher：读写存储器 RAM，用于存储加密结果.

(3) 控制运算区：

Mult：乘法器，用于实现卷积运算；

Add：加法器，对两个乘法器结果进行求和运算；

Mod：对运算结果进行取模运算；

Controller：对电路的各个模块进行控制. 包括采样及数据的读写等.

解密电路

在新的方案中，通过引入随机数的方式实现了对数据的掩码，从而保证了算法的安全性. 在设计电路的时候需要一个单独的寄存器用于存储生成的随机数，以便在解密之后对数据进行去掩码操作. 解密电路如图 4 所示.

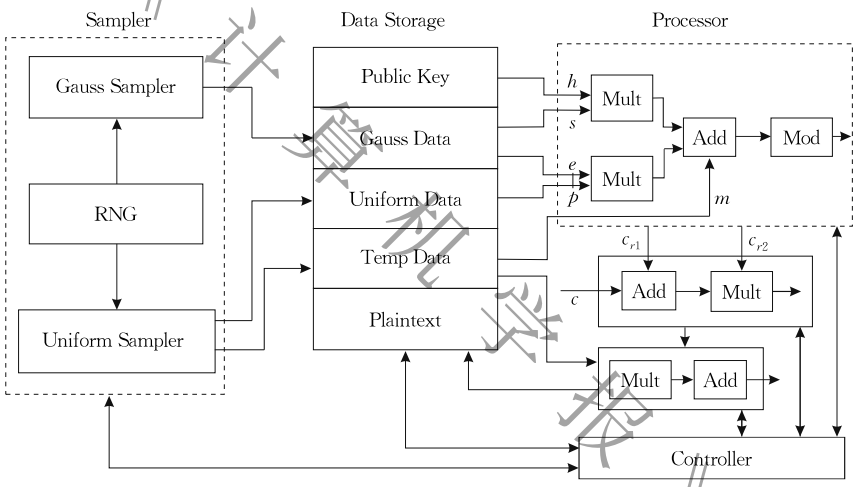

图 4　改进的 NTRU 解密电路设计

其中，取样区与加密电路一致，数据存储区增加一个随机数的寄存器 Temp Data 及存储明文信息的寄存器 Plaintext，两者均采用读写存储器 RAM，不同的地方为数据处理区. 下面详细介绍其处理过程：

首先，采样区生成随机数并将其读写在 Temp Data 区域；

然后，对随机产生的消息进行加密运算，其加密过程与加密电路保持一致；

其次，将需解密的密文与随机生成的密文进行同态运算，对运算后的密文解密；

最后，使用随机数寄存器中的数据进行去掩码操作，获得有效的明文.

5　基于 NTRU 算法的全同态掩码方案分析

在上述设计的方案中，我们改变了其密钥生成方式以防范格攻击，改变密文的计算流程以防范选择密文攻击及差分能量攻击，其中，为了实现对密文的改进，使用了方案本身的同态特性，下面分析该方案的同态正确性及安全性[20].

5.1　正确性分析

在解密过程中，使用到同态加和同态乘的运算，下面分别从加法同态特性和乘法同态特性两个方面进行验证，说明方案的正确性.

(1)加法同态特性:

首先,对于每个密文都可以表示如下形式:将对0加密所得的密文表示成比特形式:

$$c^*=\begin{pmatrix} c_{(l-1,l-1)} & c_{(l-1,l-2)} & \cdots & c_{(l-1,0)} \\ c_{(l-2,l-1)} & c_{(l-2,l-2)} & \cdots & c_{(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{(0,l-1)} & c_{(0,l-2)} & \cdots & c_{(0,0)} \end{pmatrix},$$

其中,$c_{(l,l)}$表示密文的比特位.

然后,计算:

$$\begin{aligned} c&=I_l\cdot m+c^* \\ &=\begin{pmatrix} m & 0 & \cdots & 0 \\ 0 & m & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & m \end{pmatrix}+\begin{pmatrix} c_{(l-1,l-1)} & c_{(l-1,l-2)} & \cdots & c_{(l-1,0)} \\ c_{(l-2,l-1)} & c_{(l-2,l-2)} & \cdots & c_{(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{(0,l-1)} & c_{(0,l-2)} & \cdots & c_{(0,0)} \end{pmatrix} \\ &=\begin{pmatrix} c_{(l-1,l-1)}+m & c_{(l-1,l-2)} & \cdots & c_{(l-1,0)} \\ c_{(l-2,l-1)} & c_{(l-2,l-2)}+m & \cdots & c_{(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{(0,l-1)} & c_{(0,l-2)} & \cdots & c_{(0,0)}+m \end{pmatrix}. \end{aligned}$$

其中,矩阵的对角线表示密文比特位与明文相加.对于生成的两个最终密文c_1,c_2进行同态验证:

$$\begin{aligned} c_1+c_2&=\begin{pmatrix} c_{1(l-1,l-1)}+m_1 & c_{1(l-1,l-2)} & \cdots & c_{1(l-1,0)} \\ c_{1(l-2,l-1)} & c_{1(l-2,l-2)}+m_1 & \cdots & c_{1(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(0,l-1)} & c_{1(0,l-2)} & \cdots & c_{1(0,0)}+m_1 \end{pmatrix}+\begin{pmatrix} c_{2(l-1,l-1)}+m_2 & c_{2(l-1,l-2)} & \cdots & c_{2(l-1,0)} \\ c_{2(l-2,l-1)} & c_{2(l-2,l-2)}+m_2 & \cdots & c_{2(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{2(0,l-1)} & c_{2(0,l-2)} & \cdots & c_{2(0,0)}+m_2 \end{pmatrix} \\ &=\begin{pmatrix} c_{1(l-1,l-1)}+m_1+c_{2(l-1,l-1)}+m_2 & c_{1(l-1,l-2)}+c_{2(l-1,l-2)} & \cdots & c_{1(l-1,0)}+c_{2(l-1,0)} \\ c_{1(l-2,l-1)}+c_{2(l-2,l-1)} & c_{1(l-2,l-2)}+m_1+c_{2(l-2,l-2)}+m_2 & \cdots & c_{1(l-2,0)}+c_{2(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(0,l-1)}+c_{2(0,l-1)} & c_{1(0,l-2)}+c_{2(0,l-2)} & \cdots & c_{1(0,0)}+m_1+c_{2(0,0)}+m_2 \end{pmatrix}. \end{aligned}$$

在解密时,任取密文矩阵中的某一行,例如取最后一行进行如下计算:

$$\begin{aligned} &c_{1(0,l-1)}+c_{2(0,l-1)},\cdots,c_{1(0,0)}+m_1+c_{2(0,0)}+m_2 \\ &=m_1+m_2+\sum_{i=0}^{l-1}2^i(c_{1(0,i)}+c_{2(0,i)}) \\ &=m_1+m_2+c_{1(0)}+c_{2(0)} \\ &=c', \end{aligned}$$

其中,

$$c_{1(0)}=hs_{1(0)}+pe_{1(0)},\ c_{2(0)}=hs_{2(0)}+pe_{2(0)}.$$

然后,计算:

$$\begin{aligned} &\lfloor c'f\rceil \bmod p \\ &=(m_1+m_2+hs_{1(0)}+pe_{1(0)}+hs_{2(0)}+pe_{2(0)})f \bmod p \\ &=(m_1+m_2+pgf^{-1}s_{1(0)}+pe_{1(0)}+ \\ &\quad pgf^{-1}s_{2(0)}+pe_{2(0)})f \bmod p \\ &=m_1+m_2. \end{aligned}$$

由上述可知,加法同态成立.

(2)乘法同态特性:

首先,对密文进行乘法操作运算:

$$c_1\cdot c_2=\begin{pmatrix} c_{1(l-1,l-1)}+m_1 & c_{1(l-1,l-2)} & \cdots & c_{1(l-1,0)} \\ c_{1(l-2,l-1)} & c_{1(l-2,l-2)}+m_1 & \cdots & c_{1(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(0,l-1)} & c_{1(0,l-2)} & \cdots & c_{1(0,0)}+m_1 \end{pmatrix}\cdot\begin{pmatrix} c_{2(l-1,l-1)}+m_2 & c_{2(l-1,l-2)} & \cdots & c_{2(l-1,0)} \\ c_{2(l-2,l-1)} & c_{2(l-2,l-2)}+m_2 & \cdots & c_{2(l-2,0)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{2(0,l-1)} & c_{2(0,l-2)} & \cdots & c_{2(0,0)}+m_2 \end{pmatrix}.$$

上述乘法所得矩阵的最后一行的元素为

$$c_{1(0,l-1)}\cdot[c_{2(l-1,l-1)}+m_2]+c_{1(0,l-2)}\cdot c_{2(l-2,l-1)}+\cdots+[c_{1(0,0)}+m_1]\cdot c_{2(0,l-1)}$$

$$c_{1(0,l-1)}\cdot c_{2(l-1,l-2)}+c_{1(0,l-2)}\cdot[c_{2(l-2,l-2)}+m_2]+\cdots+[c_{1(0,0)}+m_1]\cdot c_{2(0,l-2)}$$

$$\vdots$$

$$c_{1(0,l-1)}\cdot c_{2(l-1,0)}+c_{1(0,l-2)}\cdot c_{2(l-2,0)}+\cdots+[c_{1(0,0)}+m_1]\cdot[c_{2(0,0)}+m_2].$$

将其进行比特串与二进制转换可得:

$$\begin{aligned} &2^{l-1}c_{1(0,l-1)}\cdot c_{2(l-1,l-1)}+2^{l-1}c_{1(0,l-2)}\cdot c_{2(l-2,l-1)}+\cdots+ \\ &2^{l-1}c_{1(0,0)}\cdot c_{2(0,l-1)}+2^{l-2}c_{1(0,l-1)}\cdot c_{2(l-1,l-2)}+ \\ &2^{l-2}c_{1(0,l-2)}\cdot c_{2(l-2,l-2)}+\cdots+2^{l-2}c_{1(0,0)}\cdot c_{2(0,l-2)}+\cdots+ \\ &c_{1(0,l-1)}\cdot c_{2(l-1,0)}+c_{1(0,l-2)}\cdot c_{2(l-2,0)}+\cdots+ \\ &c_{1(0,0)}\cdot c_{2(0,0)}+2^{l-1}c_{1(0,l-1)}\cdot m_2+2^{l-1}c_{2(0,l-1)}\cdot m_1+ \\ &2^{l-2}c_{1(0,l-2)}\cdot m_2+2^{l-2}c_{2(0,l-2)}\cdot m_1+\cdots+ \\ &c_{1(0,0)}\cdot m_2+c_{2(0,0)}\cdot m_1+m_1\cdot m_2 \\ &=\sum_{i=0}^{l-1}2^ic_{1(0,l-1)}\cdot c_{2(l-1,i)}+\sum_{i=1}^{l-1}2^ic_{1(0,l-2)}\cdot c_{2(l-2,i)}+\cdots+ \\ &\quad\sum_{i=0}^{l-1}2^ic_{1(0,0)}\cdot c_{2(0,i)}+\sum_{i=0}^{l-1}2^ic_{1(0,i)}\cdot m_2+ \end{aligned}$$

$$\sum_{i=0}^{l-1}2^i c_{2(0,i)}\cdot m_1+m_1\cdot m_2$$
$$=c_{1(0,l-1)}\cdot c_{2(l-1)}+c_{1(0,l-2)}\cdot c_{2(l-2)}+\cdots+$$
$$c_{1(0,0)}\cdot c_{2(0)}+c_{1(0)}\cdot m_2+c_{2(0)}\cdot m_1+m_1\cdot m_2$$
$$=c'',$$

其中，

$$c_{1(i)}=hs_{1(i)}+pe_{1(i)},\ c_{2(i)}=hs_{2(i)}+pe_{2(i)}.$$

然后，计算：

$$\lfloor c''f\rceil \bmod p$$
$$=\lfloor c_{1(0,l-1)}\cdot c_{2(l-1)}+c_{1(0,l-2)}\cdot c_{2(l-2)}+\cdots+$$
$$c_{1(0,0)}\cdot c_{2(0)}+c_{1(0)}\cdot m_2+c_{2(0)}\cdot m_1+m_1\cdot m_2\rceil f \bmod p$$
$$=m_1\cdot m_2.$$

由上述可知，乘法同态成立.

为了确保在经过同态掩码之后的密文能够正确解密，需要保证乘法同态掩码时采用的掩码值是可逆的. 因此，在每次选取掩码值时，需要对其进行判断，如果不存在逆元，则应该舍弃并重新选择. 在去掩码的时候，应当按照先去除乘法掩码，然后去除加法掩码，最后再进行取模运算的顺序执行.

对掩码后的密文进行解密可得明文$(m+m_1)\cdot m_2$，由于 m_1，m_2 是由解密电路在本地产生，因此攻击者无法获取该信息. 解密电路首先根据 m_2 求得其逆 $(m_2)^{-1}$，然后计算：

$$((m+m_1)\cdot m_2\cdot (m_2)^{-1})-m_1=m.$$

最终可以实现正确的去掩码，获取真正的明文消息.

5.2　安全性分析

本节设计的掩码方案主要用于防御选择密文攻击和差分能量攻击，下面主要从这两个方面进行安全性分析.

(1) 抗选择密文攻击. 在对 NTRU 算法的分析中指出，攻击者可以利用选择密文的方式实现对算法的破译. 为了防御选择密文攻击，我们结合算法本身的同态特性对密文进行改造，即假设所有的密文都是不可信的，凡是需要解密的消息都应使用同态算法进行计算，从而实现对密文的掩码，破坏特殊密文与密钥之间的关系，从而达到防御选择密文攻击的目的.

在上述的选择密文攻击中，我们选择一组密文 $c=[0,0,\cdots,0]$ 及另外一组密文 $c=[a,0,\cdots,0]$ 进行运算，通过利用密文与密钥之间的关系对算法实现破译. 在我们提出的防御方案中，我们引入了随机密文，改变密文的结构，使得攻击者无法构造密文，消除选择密文攻击的隐患. 假设攻击者提交给解密电路的密文是 c，解密电路检查密文的合法性之后，生成随机密文 c_r，对密文 c 与随机密文 c_r 进行运算得密文(c,c_r)，因为 c_r 对于攻击者来说是随机不确定的且取样范围较大不可预测，所以，攻击者知晓 c_r 的概率可以忽略，也就是说(c,c_r)没有泄露有关中间值的消息，并且在每一次解密运算过程中，该密文都是随机生成，防止攻击者通过重复大量实验获取有效信息. 解密电路对运算后的密文进行解密，得到加掩码后的明文消息，再利用随机消息进行去掩码操作即可获得真正的明文消息.

(2) 抗差分能量攻击. 差分能量攻击是在选择密文的基础上，通过精心构造合法密文，利用数据之间的关系对算法进行破译. 本文提出的防御策略通过同态运算实现对密文的改进，使得差分运算无法正常获取密钥信息.

对于密文 c，第一次解密运算时，随机生成密文 c_{r1} 和 c_{r2}，进行计算得$(c+c_{r1})\cdot c_{r2}$，第二次解密运算时，随机生成密文 c'_{r1} 和 c'_{r2}，计算得$(c+c'_{r1})\cdot c'_{r2}$. 根据上述差分思想，假设攻击者构造出合法密文 c，经计算后，进行差分计算得：

$$(c+c_{r1})\cdot c_{r2}-(c+c'_{r1})\cdot c'_{r2}$$
$$=c\cdot c_{r2}+c_{r1}\cdot c_{r2}-c\cdot c'_{r2}-c'_{r1}\cdot c'_{r2}$$
$$=c\cdot (c_{r2}-c'_{r2})+c_{r1}\cdot c_{r2}-c'_{r1}\cdot c'_{r2}.$$

其中，攻击者已知密文 c，而其他中间值均是不可知的，且在每次计算过程中该中间值是随机变化的. 因此，攻击者无法通过重复大量实验获取能量曲线，进而通过差分能量攻击的方式进行对算法的破译，即该方案能够有效的抵抗 DPA 攻击.

在该方案中对数据进行二重掩码，即同时进行加法掩码和乘法掩码. 为的是能够使数据充分随机化，同时还能避免由于单一掩码带来的安全隐患，如零值攻击.

零值攻击是假设处理数据值 0 所需的能量消耗小于处理其他值的能量消耗. 即如果所需处理的被掩码数据为 0，则无论掩码值是多少，其计算结果均为 0，此时，该过程的能量消耗明显低于其他情况下的能量消耗，同时对应位上的能量迹总是表现为低能量. 例如，对于计算 $m\cdot r$，这里 m 为被掩码数据，r 为掩码值. 则零值模型的形式化定义如下：

$$h=m\cdot r=\begin{cases}0, & m=0\\ 1, & m\neq 0\end{cases}.$$

假设采取乘法同态进行掩码处理，即 $c\cdot c_r$，若 $c=0$，则 $c\cdot c_r$ 恒为 0，而如果 $c\neq 0$，则 $c\cdot c_r$ 不为 0，因此，攻击者可以根据零值模型进行破译. 而通过双重

掩码的方式对数据进行处理，使得即使攻击者根据零值攻击方式获取中间值，该中间值也是经掩码处理的，即 $c+c_r$；

若只采取加法同态掩码对数据进行处理，攻击者也有可能构造出精心的数据来避免该掩码的保护. 在上述 2 节的分析中，我们得到两组数据，密文 $c=[0,0,\cdots,0]$ 及另外一组密文 $c=[a,0,\cdots,0]$，在经过计算之后的解密结果为 $[0,0,0,0,0,0,0,0]$ 及 $[a,0,0,a,a,0,a,0]$. 假设在某次只使用加法同态掩码过程中，得到两组解密结果为

$$[r_1,0,0,r_1,r_1,0,r_1,0],$$
$$[a+r_2,0,0,a+r_2,a+r_2,0,a+r_2,0],$$

则攻击者依然可以根据上述的差分能量攻击方法实现对算法的破译. 即差分结果为

$$\Delta T=[a+r_2-r_1,0,0,a+r_2-r_1,$$
$$a+r_2-r_1,0,a+r_2-r_1,0].$$

在相应的密钥位上依然有可能出现峰值，从而对算法造成威胁. 因此，通过双重掩码可以有效的避免上述两种可能存在的风险，使得方案的实现过程更加安全.

此外，在原始 NTRU 密码方案中，生成的公钥具有较好的分布性质，但是其并不完全服从均匀分布，因此其不满足密码学上的伪随机性，因此，原始密钥生成算法部分有可能存在有效的格攻击，从而对方案的安全性产生威胁. 本文所提方案的密钥生成部分采用文献[17]给出的方法，通过高斯取样，在不改变密钥分布空间的基础上，有效的避免格攻击.

本方案利用算法的同态特性构造了一种全同态的掩码防御方案，一般而言，为了抵抗二阶能量攻击，仅需要执行一次加法和乘法同态运算即可. 若对系统的安全性有更高的要求，可执行多次全同态运算. 由于高阶能量分析存在诸多的受限因素，一般而言，对三阶以上的分析即为困难不可行的，因此，该全同态掩码防御方案在执行两次同态运算之后，即可抵抗上述攻击，且操作次数较少.

5.3 实验及效率分析

上述 NTRU 算法的解密核心运算为卷积，为了能够更加直观的说明 NTRU 算法存在的缺陷以及本文所提防御方案的优越性，下面通过图示说明. 首先，选取 NTRU 解密过程中需要的参数 $N=25$，$L=(14,0)$，密钥值设置为

$$f=[0,1,0,0,1,1,0,1,1,1,0,1,1,$$
$$0,0,1,0,1,0,1,0,1,1,0,1].$$

图 2 中表明，在实际的分析中通过采取选择密文与差分能量攻击的方式能够有效地对 NTRU 进行破译，我们能够得到如图 5 所示的能量波形图.

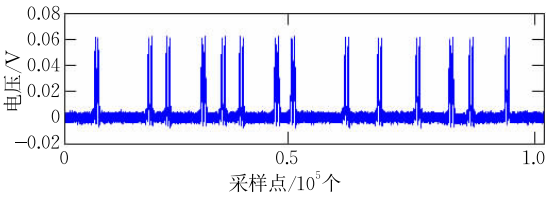

图 5 未受保护的 NTRU 差分能量攻击

由于不同的操作会消耗不同的能量，从图 2 的密文差分结构中可知，当密钥值为 1 时，对应的能量消耗较高，反之能量消耗较少，我们能够从波形上实现对密钥的分析，图 5 中的每个峰值代表密钥位为 1. 针对 Lee 等人提出的防御方案二，对某一比特进行掩码处理，如 c_i+r. 现假设攻击者能够选定两组密文，分别为

$$c^{+}=[a,c_1,\cdots,c_{N-1}],\ c^{++}=[a+r,c_1,\cdots,c_{N-1}],$$

其中，掩码值 r 的选取使得 a 与 $a+r$ 之间的汉明重量尽可能的大，根据图 2 所示差分能量攻击方法对两组密文进行计算. 由于两组密文之间只有一比特存在差异，且其汉明重量相差很大，因此，在排除噪声的干扰之后，依然能够根据能量曲线实现对密钥的破译. 如图 6 所示.

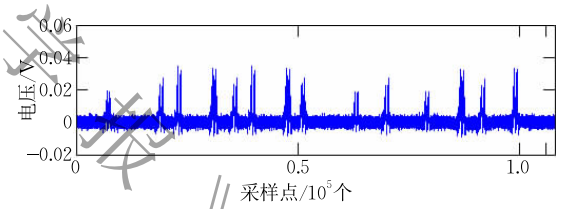

图 6 针对 Lee 的防御策略二的攻击效果

与图 5 对比，由于随机数的掩码参与，使得部分密钥位的能量消耗减少，但是对比其他密钥位的能量信息，密钥有效位的能量消耗依然会有峰值显露. 因此，图 6 表明针对 Lee 的保护方案依然可以有效地实施差分能量攻击. 在本文提出的防御方案中，假设密文表示为 $C=(c+c_1)\cdot c_2$，其中 c_1,c_2 为随机生成的密文，则图 1 中所示比特位表示为相应系数相加. 由于密文之间的运算使得多项式的所有系数都随机化，造成无法实施差分能量攻击. 如图 7 所示.

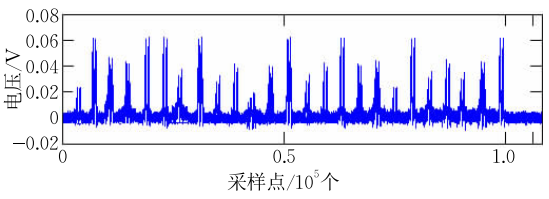

图 7 针对全同态掩码防御方案的攻击效果

从图 7 中可以看出，由于随机数的参与，使得各个密钥位的能量消耗也随机化，能量波形没有明显的峰值，攻击者无法有效的进行密钥位的判别，从而达到防御的目的.

在本文所提出的方案中，通过生成随机的密文，对方案中的原始密文进行加法和乘法的掩码操作，因此，可以实现多比特的掩码处理. 在需要对多比特进行掩码的时候，相比较 Lee 的方案，能够减少随机数的生成，同时减少寄存器的开销.

通过随机生成密文数据，在已知密钥的前提下，根据密文与密钥进行运算，采集计算过程中消耗的能量并根据能量曲线确定攻击点. 猜测密钥的可能值并使用猜测值与密文进行运算求出中间变量的汉明重量. 根据中间变量的汉明重量值与能量消耗之间的相关系数进行密钥的分析，若相关系数较高，则说明猜测的密钥位正确. 为了说明全同态掩码方案中汉明重量与能量消耗之间的相关系数，给出了图 8.

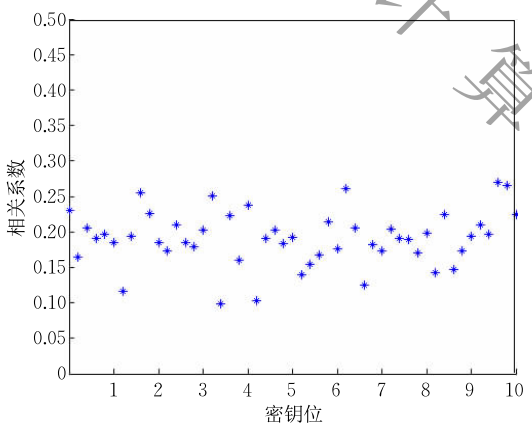

图 8　全同态防御方案 CPA 分析

通过合理选择密文，使得能量曲线与中间变量的汉明重量的相关系数很低，且在一定的范围内浮动，在示例中我们选取的相关系数在 0.2 附近波动，波动范围在 0.08 之间. 因此，只要能够产生合理的掩码数据，该方案就能够有效地防御相关能量攻击.

效率分析：如果在实现过程中采取布尔掩码的方式对数据进行处理，则需要穷举计算所有的掩码值，并且需要构造一个相当庞大的查找表以供去掩码操作，随着查找表所使用的掩码数量的增加，相应的计算规模和存储内存需要也随着增加. 而本文提出的同态掩码方案只需一个存储器对临时变量进行存储即可，在每次运算完成之后，将使用过的数据擦除，下次计算时，再次随机生成掩码值即可. 在 Lee 方案中，若实现对所有系数掩码，则需要生成大量的随机数，增大资源的开销与计算时间；而本方案中生成的密文能够实现对多项式所有系数进行掩码. 同时，采取两重的掩码，可以有效地抵抗二阶分析.

6　总　结

在后量子时代，基于格的公钥密码体制得到了广泛的关注. 密码分析者往往可以绕开 NTRU 算法所基于的数学困难问题，通过提取侧信道信息来降低对密钥的破译难度. 本文根据 NTRU 算法的同态特性，设计了一种全同态掩码防御方案. 在密钥生成部分，改变密钥生成方式，能够有效防御格攻击；在解密部分，通过执行密文之间的操作，可以实现对多项式所有系数同时进行掩码，由于使用了方案本身的加法同态和乘法同态，我们的方案还能有效抵抗零值攻击和二阶差分能量攻击. 抗量子密码算法是目前的研究热点，利用算法本身的同态性质实现掩码，可以减少随机数的生成及存储，有效提高方案的效率及节省资源开销.

参　考　文　献

[1] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem//Algorithmic Number Theory. Berlin, Germany: Springer, 1998: 267-288

[2] Xu Qiu-Liang, Li Da-Xing. Elliptic curve cryptosystems. Journal of Computer Research and Development, 1999, 36(11): 1281-1288(in Chinese)
(徐秋亮，李大兴. 椭圆曲线密码体制. 计算机研究与发展，1999，36(11)：1281-1288)

[3] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 1978, 21(2): 120-126

[4] Liu Li-Qiang, Yang Ya-Tao, Li Zi-Chen. Analysis and improvement of NTRU decryption failure. Journal of University of Science and Technology of China, 2011, 41(9): 826-830 (in Chinese)
(刘立强，杨亚涛，李子臣. NTRU 密码体制中解密失败的分析与方案改进. 中国科学技术大学学报，2011，41(9)：826-830)

[5] IEEE Std P1363.1-2008. IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems Over Lattices. USA, 2009

[6] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems//Proceedings of the 16th Annual International Cryptology Conference. Santa Barbara, USA, 1996: 104-113

[7] Kocher P, Jaffe J, Jun B. Differential power analysis//Proceedings of the 19th Annual International Cryptology Conference. Santa Barbara, USA, 1999: 388-397

[8] Hu F, Wilhelm K, Schab M, et al. NTRU-based sensor network security: A low-power hardware implementation perspective. Security & Communication Networks, 2009, 2(1): 71-81

[9] Atici A C, Batina L, Gierlichs B, et al. Power analysis on NTRU implementations for RFIDs: First results//Proceedings of the RFIDSec08: Workshop on RFID Security. Budapest, Hungary, 2008: 128-139

[10] Lee M, Song J, Choi D, et al. Countermeasures against power analysis attacks for the NTRU public key cryptosystem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, 93(1): 153-163

[11] Wang A, Zheng X, Wang Z. Power analysis attacks and countermeasures on NTRU-based wireless body area networks. KSII Transactions on Internet & Information Systems, 2013, 7(5): 1094-1107

[12] Xu J, Hu L, Sun S, et al. Cryptanalysis of countermeasures against multiple transmission attacks on NTRU. IET Communications, 2014, 8(12): 2142-2146

[13] Zheng X, Wang A, Wei W. First-order collision attack on protected NTRU cryptosystem. Microprocessors & Microsystems, 2013, 37(6-7): 601-609

[14] Kamal A A, Youssef A M. A scan-based side channel attack on the NTRU encrypt cryptosystem//Proceedings of the 2012 7th International Conference on Availability, Reliability and Security. Prague, Czech Republic, 2012: 402-409.

[15] Kamal A A, Youssef A M. Strengthening hardware implementations of NTRU Encrypt against fault analysis attacks. Journal of Cryptographic Engineering, 2013, 3(4): 227-240

[16] Coppersmith D, Shamir A. Lattice attacks on NTRU//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'97). Konstanz, Germany, 1997: 52-61

[17] Zhang Jian-Hang, He Jian, Hu Yu-Pu. A novel NTRU encryption scheme based on R-LWE problem. Electronic Science and Technology, 2012, 25(5): 76-78(in Chinese)
(张建航，贺健，胡予濮. 基于R-LWE问题的新型NTRU加密方案. 电子科技，2012，25(5)：76-78)

[18] Coron J, Mandal A, Naccache D, et al. Fully homomorphic encryption over the integers with shorter public keys//Proceedings of the Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2011). Santa Barbara, USA, 2011: 487-504

[19] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based//Proceedings of the Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2013). Santa Barbara, USA, 2013: 75-92

[20] Li Zi-Chen, Zhang Juan-Mei, Yang Ya-Tao, Zhang Feng-Juan. A fully homomorphic encryption scheme based on NTRU. Acta Electronica Sinica, 2018, 46(4): 938-944(in Chinese)
(李子臣，张卷美，杨亚涛，张峰娟. 基于NTRU的全同态加密方案. 电子学报，2018，46(4)：938-944)

[21] Rohloff K, Cousins D B. A scalable implementation of fully homomorphic encryption built on NTRU//Proceedings of the International Conference on Financial Cryptography and Data Security (FC 2014). Christ Church, Barbados, 2014: 221-234

[22] Chenal M, Tang Q. Key recovery attacks against NTRU-based somewhat homomorphic encryption schemes//Proceedings of the International Information Security Conference (ISC 2015). Trondheim, Norway, 2015: 397-418

[23] Song Xin-Xia, Chen Zhi-Gang, Zhou Guo-Min. NTRU-type fully homomorphic encryption scheme without key switching. Chinese Journal of Network and Information Security, 2017, 3(1): 39-45(in Chinese)
(宋新霞，陈智罡，周国民. NTRU型无需密钥交换的全同态加密方案. 网络与信息安全学报，2017，3(1)：39-45)

YANG Ya-Tao, Ph. D., associate professor. His current research interests include cryptography and communication security.

LIU Bo-Ya, M. S. candidate. His current research interests include cryptography protocol and cyberspace security.

SUN Ya-Fei, M. S. candidate. His current research interests include cryptography and network information security.

LI Zi-Chen, Ph. D., professor, Ph. D. supervisor. His current research interests include cryptography, information security, post quantum cryptography and digital watermarking.

Background

The lattice based cryptosystem (LBC) is one of the outstanding representatives of post quantum cryptography, it has been widely researched because of its many better secure properties. Generally speaking, the security of LBC scheme is provable, however, the risk of side channel attack is still unavoidable during the implementation process for the

scheme. The side channel attack mainly contains Timing attack, Power attack, Cache attack and Fault attack and so on. At present, many researches show that the unprotected LBC algorithm cannot resist the side channel attack.

NTRU is a typical algorithm of the LBC scheme. It has been widely applied in many cryptosystem to enhance the security of information system; meanwhile, it has been the IEEEP1363 standard and finance service industrial standard in USA. In 2010, Lee et al. proved by experiments that NTRU algorithm could not resist Power Attack; Also, Wang et al. had implemented the side channel attack through combining Chosen Cipher text Attack and Power Attack in 2013.

Masking is a common defense countermeasure to resist Power Attack, by masking the intermediate values, the data operations are under the masked state, which can achieve to resist side channel attack. However, present defense countermeasures in existing scheme can only treat one bit or little bits in masking process, if algorithm needs to achieve multi bits mask and higher security, large resource cost and low efficiency will emerge. A novel NTRU fully homomorphic masking(FHM) defense scheme is proposed in this paper, by designing an fully homomorphic encryption system, we implement the calculation and operation between the cipher texts, all the polynomial coefficients of NTRU algorithm are processed by the masked state.

This is the first defense scheme based on Homomorphic Masking technology to resist side channel attack of NTRU cryptosystem. Compared with other schemes, our defense measure is highly secure and has low resource overhead. Illustrations are given to describe the effectiveness of the scheme, and according to its implementation process, its circuit design model is also given. This scheme can effectively guarantee the security of NTRU algorithm during the hardware implementation, and also provide an useful reference of other cryptosystems during their hardware implementation process.

This work was supported by the "13th Five-Year" National Cryptography Development Foundation (Grant No. MMJJ20170110).