文章编号:1000－2367(2019)01－0017－09 **DOI**:10.16366/j.cnki.1000－2367.2019.01.003

NTRU 密码算法的安全性分析

李超[a,b],杨智超[a]

(国防科技大学 a.计算机学院;b.文理学院,长沙 410073)

摘 要:随着量子计算的快速发展,目前主流的公钥密码体制如 RSA、ECC 等均已找到多项式时间复杂度的量子求解算法.NTRU 密码算法由于至今未找到有效的量子求解算法,被认为具有抗量子计算攻击的能力,加之其具有加解密速度快、内存需求小等特点,已经在公钥密码领域受到了广泛关注.首先介绍 NTRU 密码算法的加解密流程以及算法的改进方案,然后从格攻击和非格攻击两方面分析 NTRU 密码算法的安全性,重点介绍格攻击在子域上的最新进展,以及解密错误攻击的提出和改进.

关键词:NTRU;密码分析;格;格算法

中图分类号:TP918 **文献标志码**:A

量子计算的迅速发展给传统公钥密码体制带来了巨大挑战,因此密码学家越来越关注密码算法的抗量子攻击能力.NTRU[1]是 1996 年由 Brown 大学三位数学家 Silverman、Hoffstein 和 Pipher 提出的公钥密码算法,由于该算法至今未找到量子求解方法,被广泛地认为具有抵抗量子计算攻击能力.又因为已知 NTRU 公钥求解私钥的问题可规约到相应格中求解最短向量问题,所以除了利用传统方法对 NTRU 密码安全性进行分析,也可以通过求解格中最短向量恢复 NTRU 密钥.随着 NTRU 算法的不断完善和改进,其应用也受到越来越广泛的关注,2003 年日本索尼公司与 NTRU 公司合作,将基于 NTRU 的数字签名算法 NTRU-Sign 应用于嵌入式设备和 IC 卡等领域.2008 年恩智浦半导体公司与 NTRU 公司合作,推出了首款用于通用型 ARM7 微控制器的基于软件的加密解决方案,同年基于 NTRU 的加密算法和签名算法的标准 IEEE p1361.1 正式通过.

1 预备知识

格理论的研究源于 1611 年开普勒提出的球堆积猜想:在一个容器中堆放半径相等的小球所能达到的最大密度是 $\pi/\sqrt{18}$.自 19 世纪以来许多领域都对格的相关性质进行了广泛而深入的研究.为解决该问题,高斯引进了格的概念并指出:在三维空间中,当所有的球心构成一个格,则球堆积可达到最大密度值 $\pi/\sqrt{18}$. 目前基于格的密码是一类备受关注的抗量子计算攻击的公钥密码体制,格密码理论的研究涉及的密码学问题众多,学科交叉特色明显,研究方法趋于多元化[2－3].

1.1 格

设 B 是定义在实数域 $\mathbf{R}$ 上的行满秩矩阵,其行向量分别为 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m \in \mathbf{R}^n$,称集合 $\mathcal{L}=\{x_1\boldsymbol{b}_1+x_2\boldsymbol{b}_2+\cdots+x_m\boldsymbol{b}_m \mid x_i \in \mathbf{Z}(1\leq i\leq m)\}$ 为向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 在 $\mathbf{R}^n$ 中张成的格,记为 $L(\boldsymbol{B})$.$\boldsymbol{B}$ 称为格基矩阵,其行向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 为格 L 的一组格基.格 $L(\boldsymbol{B})$ 的维数 $\dim(L(\boldsymbol{B}))=\mathrm{rank}(\boldsymbol{B})$,即为 m.如果 $m=n$,则称 $L(\boldsymbol{B})$ 为满秩格.

收稿日期:2018-02-02;**修回日期**:2018-11-21.

基金项目:国家自然科学基金(11531002;61672530)

作者简介:李超(1966－),男,湖南汨罗人,国防科技大学教授,博士生导师,主要研究领域为密码学,E-mail:lichao_nudt@sina.com.

通信作者:杨智超,E-mail:yzc_nudt@qq.com.

在空间 $\mathbf{R}^n$ 中记 $\boldsymbol{G}(\boldsymbol{B})=[(\boldsymbol{b}_i,\boldsymbol{b}_j)]_{1\leq i,j\leq m}$ 为格 L 在 $\mathbf{R}$ 中的 Gram 矩阵,其中 $(\boldsymbol{b}_i,\boldsymbol{b}_j)$ 表示向量 $\boldsymbol{b}_i$ 与 $\boldsymbol{b}_j$ 的内积,易知 $\boldsymbol{G}$ 为对称的正定矩阵.格 $\mathscr{L}$ 的体积定义为 $\mathrm{vol}(L)=\sqrt{\det(\boldsymbol{G}(\boldsymbol{B}))}$,若格 L 为满秩格,则 $\mathrm{vol}(L)=|\det(\boldsymbol{B})|$,即体积为格基矩阵 $\boldsymbol{B}$ 行列式的绝对值.

1.2 格中困难问题

在格的研究中,最著名的两个问题是最短向量问题(SVP)和最近向量问题(CVP).

最短向量问题(SVP)给定一个格基矩阵 $\boldsymbol{B}$,找到一个非零向量 $\boldsymbol{v}\in L(\boldsymbol{B})$,使之成为格 $L(\boldsymbol{B})$ 中最短的非零向量.

最近向量问题(CVP)给定一个格基矩阵 $\boldsymbol{B}$ 以及向量 $\boldsymbol{u}\in\mathbf{R}^n$,找到一个向量 $\boldsymbol{v}\in L(\boldsymbol{B})$,使之成为格 $L(\boldsymbol{B})$ 中离 $\boldsymbol{u}$ 最近的向量.

SVP 和 CVP 都属于非常困难的问题[4-6],尤其随着格维数增大求解相应问题的时间复杂度会呈指数增加,最终导致不可解.然而即使是求解 SVP 和 CVP 近似问题,在理论和工程方面都发挥着巨大作用.如今普遍认为最近向量问题(CVP)是 NP-Hard 问题,而最短向量问题(SVP)在"随机归约假设"下也被认为是 NP-Hard 问题.但在实际应用中,一般认为 CVP 问题要稍难于 SVP 问题[7],因为 CVP 问题常常能转化为更高维度的 SVP 问题.例如在背包问题中,一个 $N+1$ 维 SVP 问题可以很容易转化为 N 维 CVP 问题.而且,SVP 问题和 CVP 问题在不同范数选取下难度也不同,如 SVP 和 CVP 问题在 $\mathscr{L}_\infty$ 范数下就要比在欧氏范数下更难.

1.3 格基约化算法

格 $\mathscr{L}$ 中存在无数组格基,格基约化目的在于寻找到一组性质良好的格基,使得在这组格基下能高效求解 SVP 或 CVP 问题.因此,格基约化算法在求解 CVP 和 SVP 问题中扮演着非常重要的角色,格基约化算法强度直接决定了基于格上困难问题的密码体制的安全性.与向量空间不一样,格中可能不存在正交基,格基约化实际上是寻找一组尽可能接近正交的格基.另一方面,由于格的行列式固定,也就是格的体积固定,从而格基正交性好也就意味着基向量长度尽可能短.

枚举算法 枚举算法是求解 SVP 问题最直接的算法,也是到目前为止研究最为广泛的求解算法之一.给定一组格基 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$,枚举算法旨在遍历这组基下长度在某个界中的所有整系数线性组合 $x_1\boldsymbol{b}_1+x_2\boldsymbol{b}_2+\cdots+x_m\boldsymbol{b}_m$,从而输出最短向量并终止程序.但实际求解过程中随着维数的增大,枚举算法的时间复杂度也随之成指数增加,因而不能在有效的时间内求出格中短向量.

剪枝是提高枚举算法效率的一个重要策略,通过剪去存在短向量概率较小的空间,可降低算法时间复杂度.但如果裁剪空间选取不合理,很可能在剩下的遍历空间中不存在短向量,因此 Nguyen 等人在文献[8]中提出了极限裁剪枚举算法,并通过大量的实验[9]说明,当合理选取裁剪参数时,极限裁剪枚举算法能以较高的概率输出格中最短向量.但如何选取裁剪参数是极限裁剪枚举算法的核心问题.为有效的解决极限裁剪枚举算法中的参数选取问题,Aono 和 Nguyen 在 EUROCRYPT2017[10] 上提出了离散裁剪枚举算法,该算法避免了极限裁剪枚举算法的参数选取问题,可以自动高效的对搜索空间进行裁剪,与之前的极限裁剪枚举算法相比,在维数较大的情况下改进效果更为明显.

LLL 约化 &BKZ 约化 1982 年文献[11]给出了多项式时间内求得约化基的算法,由于该算法由 Lenstra、Lenstra 和 Lovász 共同提出,因此被称为 LLL 算法.将格 L 的一组基作为输入,通过 LLL 算法可以输出一组 LLL-约化基,其中的第一个基向量即为近似 SVP 的解向量,LLL 算法虽然是关于秩 m(以及格基向量中分量的比特长度)的多项式时间复杂度算法,但输出基的正交性仍然较弱.1994 年 Schnorr[12] 等人对 LLL 算法进行推广,提出了更一般的格基约化算法-BKZ(BlockKorkine-Zolotarev)算法.与 LLL 算法相比,参数为 $\beta(2<\beta<n)$ 的 BKZ 算法首先利用 LLL 算法对格基 $\boldsymbol{B}$ 进行预处理,然后在每个分块 $\boldsymbol{B}_{[j,\min(j+\beta-1,n)]}$ 中不断约化迭代,直到每一块中第一个向量成为该分块中的最短向量,因此 BKZ 算法可输出约化性质更好的格基.由于 BKZ 算法中需要调用枚举算法,因此枚举算法的效率很大程度上决定了 BKZ 算法的运行效率.

Shoup 在 NTL 库中实现了 BKZ 算法以及带有剪枝枚举的 BKZ 算法,方便了格中困难问题的分析和求解.为进一步提高 BKZ 算法的运行效率,Chen 和 Nguyen 在 BKZ 基础上结合极限裁剪枚举算法对 BKZ 算法进行了深度改进,进而提出了新的 BKZ2.0[13] 算法.BKZ2.0 被认为是目前求解格中 SVP 最高效的算法,但

由于其运行代码没有公开,并且其算法效能很大程度上取决于裁剪参数的选取,这在一定程度上限制了其推广.另外 Aono 等人 2016 年提出的 PBKZ 算法[14]也是对经典 BKZ 算法的深度改进,算法在运行过程中会自动调整选择约化策略,因而不需要事先的设置相关参数,提高了算法的运行效率.

本文主要以 NTRU 密码算法的发展和分析为主线,将对 NTRU 算法的攻击分为格攻击和非格攻击两类.剩余内容安排如下:第二节围绕 NTRU 密码的提出、发展和完善,详细介绍了 NTRU 密码存在的问题及其解决方案,并以早期的 NTRU 版本为例,给出了算法加、解密的一般流程.第三节介绍了 NTRU 密码算法的格攻击方案,并重点介绍了针对 NTRU 格攻击的最新结果-子域攻击.在第四节中,依次介绍针对 NTRU 的解密错误攻击、选择密文攻击、中间相遇攻击、混合攻击、多重传输攻击和广播攻击等非格攻击.最后在第五节进行总结.

2　NTRU 密码算法及其发展

NTRU 密码算法是定义在多项式环 $R=\mathbf{Z}[X]/(X^N-1)$ 上的公钥密码算法,是 Hoffstein、Pipher、Silverman 3 位数学家在 CRYPTO1996[1]上提出的公钥密码体制.它正式发表于 1998 年[15],并分别在 2001 年[16]和 2005 年[17]进行了两次较大的改进,从而提高了算法的计算效率、安全性、实用性和可靠性.这里以 NTRU-1998 为例介绍 NTRU 密码算法的加、解密流程.

2.1　NTRU

3 个正整数 (N,p,q) 和 4 个整系数多项式集合 $\mathcal{L}_f$,$\mathcal{L}_g$,$\mathcal{L}_r$ 和 $\mathcal{L}_m$ 共同决定 NTRU 密码系统.正整数 p 和 q 的选取满足 $\gcd(p,q)=1$ 且 q 远大于 p,用 $*$ 表示剩余类环 R 中的乘法.在整个密码系统中,一部分乘法将在模 q 下运算,另一部分将在模 p 下运算.

多项式集合 $\mathcal{L}_f$、$\mathcal{L}_g$、$\mathcal{L}_r$ 和 $\mathcal{L}_m$ 的选取应遵循以下原则:明文 m 所选取的集合 $\mathcal{L}_m$ 是包括所有模 p 的多项式.这里为了方便讨论,假设 p 是奇数,于是有

$$\mathcal{L}_m=\left\{m\in\mathbf{R}:m\text{ 的系数位于}-\frac{1}{2}(p-1)\text{ 和}\frac{1}{2}(p-1)\text{ 之间}\right\}.$$

另外 3 个多项式集合均采用如下形式:

$$\mathcal{L}(d_1,d_2)=\{F\in\mathbf{R}:F\text{ 中有 }d_1\text{ 个系数等于 }1,d_2\text{ 个系数等于 }-1,\text{剩下的均等于 }0\},$$

因此,3 个正整数 d_f,d_g 和 d_r 便可确定参数选取集合:

$$\mathcal{L}_f=\mathcal{L}(d_f,d_f-1),\mathcal{L}_g=\mathcal{L}(d_g,d_g),\mathcal{L}_r=\mathcal{L}(d_r,d_r).$$

由于设计者希望多项式 f 在环 $\mathbf{Z}_p[X]/(X^N-1)$ 和 $\mathbf{Z}_q[X]/(X^N-1)$ 中存在逆元,所以令 $\mathcal{L}_f=\mathcal{L}(d_f,d_f-1)$ 而非 $\mathcal{L}_f=\mathcal{L}(d_f,d_f)$,否则由 $f(1)=0$ 可知 f 不可逆.

密钥生成　首先,随机选取多项式 $f\in\mathcal{L}_f$,$g\in\mathcal{L}_g$ 生成 NTRU 密钥,其中多项式 f 即为私钥,并且在模 p 和 q 下都必须可逆,逆元分别记为 F_p 和 F_q,从而有 $F_p*f\equiv1 \bmod p$,$F_q*f\equiv1 \bmod q$.公钥 h 由 F_q 和 g 生成 $h\equiv F_q*g \bmod q$.实际上,参数 N,p 和 q 都公开,f 为私钥,连同 F_p、F_q 和 g 均需保密.

加密　在得到了公钥 h 后,即可对明文 $m\in\mathcal{L}_m$ 进行加密,随机选取噪声多项式 $r\in\mathcal{L}_r$,对明文 m 操作如下 $e\equiv pr*h+m \bmod q$,得到相应的密文 e.

解密　收到加密信息 e 后,首先将 f 与 e 相乘得到:$a\equiv f*e \bmod q$,在这里算法通过模 q 操作,将 a 的系数控制在区间 $[A,A+q-1]$,其中 A 为合理选取的常数,一般情况下 $A=\left\lfloor\frac{pr(1)\cdot g(1)+f(1)\cdot m(1)}{N}\right\rceil-\frac{q}{2}$,再令 $b\equiv a \bmod p$.最后,明文能由下式计算得到 $F_p*b \bmod p$.

2.2　算法分析

实际上多项式 a 能表示为 $a\equiv f*e=f*pr*h+f*m \bmod q=pr*g+f*m \bmod q$.记 $pr*g+f*m$ 中系数的跨度为系数的最大值减去最小值,由于参数 p 很小且多项式 g,f,r,m 均为小系数多项式,$pr*g+f*m$ 中系数的跨度将以"很高概率"小于 q,所以当参数 A 合理选取时,$pr*g+f*m$ 的系数均落在区间 $[A,A+q-1]$ 中,此时解密正确.若参数 A 选取出现偏差导致 $pr*g+f*m$ 中存在不属于区间 $[A,A+q-1]$ 的系数,此时解密会出现包装失败(wrapfailure).另外当多项式 $pr*g+f*m$ 的系数跨度严

格大于 q 时,不存在 A 使得 $pr*g+f*m$ 的系数均落在区间$[A,A+q-1]$中,此时发生的解密错误称为跨度失败(gapfailure).一般而言,跨度失败发生的概率会高于包装失败的概率.统计数据表明,NTRU-1998 版本平均加密 2^{15} 次时会出现一次解密错误.

另外在运行效率方面,环 R 中多项式 f 存在逆的概率、求逆操作、环中任意多项式的乘法均是影响算法效率的主要因素.为进一步提高算法效率,Silverman 在文献[18]中计算了环 R 中可逆元所占比例,说明了私钥 f 将以很大的概率存在逆元,同时也在文献[19]中给出了计算 R 中多项式乘法的快速算法,进而大大提高了加解密算法的运行效率.在文献[20]中 Silverman 指出当参数 N 为两个素数的乘积产生时,可以利用傅立叶变换高效计算多项式在环中的乘法,从而提高 NTRU 算法的整体运行效率,并给出了一类推荐参数.但实际上这会对 NTRU 密码的安全性产生一定的影响,Gentry 在文献[21]对其安全性进行了分析.

2.3 NTRU-1998 参数集

Silverman 等人[15]给出了 NTRU 不同的参数选取方案,以此来获得不同的安全等级.表 1 给出了参数的取值,在 NTRU 公钥密码的原始方案中[15],$N=107$ 规模的参数对应了中等安全密码系统.

表 1 不同规模下的参数

Fig.1 Parameters in Different Scale

安全等级	N	p	q	d_f	d_g	d_r
中等	107	3	64	15	12	5
标准	167	3	128	61	20	18
最高	503	3	256	216	70	55

2.4 改进版本

NTRU 密码算法提出后由于其具有的抗量子计算攻击的能力,越来越多国际密码学家投入到对 NTRU 密码算法的安全性分析中,各种攻击方法也被相继提出.为应对这些挑战,NTRU 的设计者对算法本身进行了不断的修改和完善,从而提高了算法的安全性和运行效率.

NTRU-2001 2001 年在文献[22-23]提出的 NTRU 标准中,给出了有关 NTRU 的新版本:NTRU-2001,其中明文空间 $\mathscr{L}_m$ 为 R 中系数取自$\{0,1\}$的多项式,参数 q 取为素数.p 被替换为多项式 $x+2$,密钥选择形如 $1+p*F$ 多项式,其中 $F\in$ 这 $\mathscr{B}(d_F)$ 是 R 中具有 d_F 个系数等于 1,其余均为 0 的多项式.其他集合为 $\mathscr{L}_g=\mathscr{B}(d_r)$,$\mathscr{L}_r=\mathscr{B}(d_r)$.此时在模 p 条件下,密钥 f 显然存在逆元,且逆元为 1.所以在解密过程中不需要另外计算多项式逆元 F_p,更不用进行与 F_p 有关的乘积操作,提高了算法运行效率.在这个版本中平均加密次数为 $2^{12}\sim2^{25}$ 时,会出现一次解密错误.

NTRU-2005 另外的一次改进是在 2005 年,Silverman 等人[17]将参数 $p=x+2$ 重新调整为 $p=3$,并且利用了多项式的乘法构造私钥.$\chi(d_f)$ 表示具有形式 $f_1*f_2+f_3$ 的多项式构成的集合,其中 $f_1,f_2,f_3\in\mathscr{B}(d_f)$. 在 NTRU-2005 中,私钥 f 仍然具有 $1+p\cdot F$ 的形式,但 $F\in\chi(d_f)$,其他的集合定义为 $\mathscr{L}_g=\mathscr{B}(N/2)$,$\mathscr{L}_r=\chi(d_r)$,明文空间 $\mathscr{L}_m$ 仍然为 R 中二元多项式组成的集合.特别地,在该版本中若参数 q 为一个素数乘以 2,则 NTRU-2005 在解密过程中可以完全避免解密错误.

StreamlinedNTRUPrime 该版本是 Bernstein 等人在 2016 年[24]提出,对上述经典 NTRU 算法深度改进的密码体制.经典 NTRU 密码算法均定义在多项式环 $R=\mathbf{Z}_q[X]/(X^N-1)$ 上,其中参数 N 为一素数,q 为 2 的方幂.由于多项式环 R 往往同构于某一分圆域的代数整数环,这为攻击者分析 NTRU 密码算法的安全性提供了许多代数工具.为消除多项式环中的特殊代数结构,Bernstein 等人将 NTRU 算法推广到环 $R^*=\mathbf{Z}_q[X]/(X^N-X-1)$ 中,其中 N 仍为素数,进而提出了 Streamlined NTRU Prime 密码算法.与经典的 NTRU 密码算法相比,Streamlined NTRU Prime 算法抵抗了针对 NTRU 的代数攻击,如子域攻击,同时 Bernstein 等人也证明了 Streamlined NTRU Prime 密码算法在自适应性选择密文攻击下是安全的.

3 格攻击

在 NTRU 密码算法中,若给定公钥 h 直接恢复私钥 f 等价于将 h 分解为两个具有特定形式的小系数多

项式的商,该问题的困难性是 NTRU 密码算法安全的基础.由于缺乏高效求解算法,普遍认为在 NTRU 密码算法中利用公钥 h 求解密钥 f 是困难的.1997 年,Coppersmith 和 Shamir[25] 首次将 NTRU 密码算法的安全性与格中求解最短向量问题联系起来,开启了利用格对 NTRU 密码算法分析的大门.

3.1　经典格攻击

Coppersmith 和 Shamir[25] 发现在利用公钥 h 构造的 NTRU-格中,最短向量会以很高概率等于 $(x^i * \lambda f, x^i * g)$,其中 λ 为待定参数(通常取值为 1),i 为一正整数.NTRU-格中部分短向量可以作为弱密钥对密文进行部分解密.设格基矩阵 $\boldsymbol{B}$ 定义如下:

$$\boldsymbol{B}=\begin{bmatrix}\lambda \boldsymbol{I}_{N\times N} & \boldsymbol{H}_{N\times N}\\ \boldsymbol{0}_{N\times N} & q\boldsymbol{I}_{N\times N}\end{bmatrix},$$

$\boldsymbol{H}$ 即为公钥 h 所对应的循环矩阵,此时得到 $\boldsymbol{B}$ 生成的格 $L^{\mathrm{NTRU}}=L(\boldsymbol{B})$ 即为 NTRU-格.

为评估 NTRU-格攻击对 NTRU 密码算法安全性的影响,Silverman 等人在 1999 年[26] 利用 LLL 算法及其改进版本对不同规模的 NTRU 算法进行了大量求解实验,测试了 NTRU 密码算法在格攻击下的安全性.Silverman 发现该方法的运行时间 T 与格的维数 $2N$ 满足关系

$$\lg(T) > A \cdot N + B, \tag{1}$$

A 与 B 是与格基约化算法及其输入格相关的常数,当参数 N 较大时,攻击的时间复杂度远远超过了当时的计算能力.并且在实验过程中格基约化算法往往直接输出原始私钥或求解失败,并未发现文献[25]中提到的弱密钥.因此 Silverman 等人相信即使在 NTRU-格攻击下,NTRU 密码算法仍然是安全的.2012 年 Bi 与 Cheng[27] 利用 Kolmogorov 复杂度理论给出了 NTRU 格中最短向量长度的下界,从另一方面说明了 NTRU 密码的困难性,即穷搜获得 NTRU 密码算法的密钥 f 是不可行的.

3.2　低维格攻击

由公式(1)可知,待约化格的维数很大程度上决定了格攻击的时间复杂度,且在经典的 NTRU-格攻击中,待约化格维数往往很大,结合已有的格基约化算法很难对其中的最短向量进行有效求解,因此如何尽可能地降低待约化格的维数,是提高格攻击效率的关键.

May 在 1999 年提出针对 NTRU 的 Zero-Run 攻击[28].在 Zero-Run 攻击中,May 首先猜测多项式 g 连续 r 个等于 0 的系数,从而在 NTRU-格基础上构造了维数更低的 Zero-Run 格.同年,Silverman[29] 指出在猜测多项式 g 中系数时,并不需要假设所猜测的系数是特定位置连续的 r 个,从而推广 May 的想法提出了关于 NTRU 的 Zero-Force 攻击.在 Zero-Force 攻击及其相应变种中,猜测 g 相关系数的正确率得到极大提高,待约化格维数进一步降低.2001 年 May 和 Silverman 在文献[30]中给出了 NTRU-格更一般的形式:循环模格(CML:Circulant Modular Lattice)和相应的 CML 模式攻击(CML Pattern Method).CML 模式攻击是对 Zero-Force 和 Zero-Run 攻击的一般总结和归纳,文献[30]分析了此类方法的成功概率和难点,对后续的进一步研究有着指导意义.

2002 年 Gentry 分析了文献[20]中改进后 NTRU 密码算法,在参数 $N=pq$ 的情况下给出了更有效的格攻击方法[21].Gentry 首先定义了从 $\mathbf{Z}[X]/(X^N-1)$ 到 $\mathbf{Z}[X]/(x^p-1)$ 的环同态 φ,然后构造关于多项式 $\varphi(h)$ 的 CML 格:$L_{\varphi(h)}$,此时 $(\varphi(f),\varphi(g))$ 一定属于格 $L_{\varphi(h)}$.相对于原始的 NTRU 格,$L_{\varphi(h)}$ 的维数从 $2N$ 降为 $2p$,因而攻击者对 $L_{\varphi(h)}$ 进行格基约化能更容易求得向量 $(\varphi(f),\varphi(g))$,进而恢复 (f,g).2005 年 Han[31] 提出了另一种恢复 NTRU 明文的全新格攻击,在攻击者事先知道明文部分比特信息的情况下,Han 利用这些比特信息构造了具有特殊结构的 $N+2$ 维格,然后通过这些低维格的不断求交获得目标格,最后通过对目标格求解最短向量恢复剩下的明文信息.由于求交不会增加格的维数,目标格的维数始终为 $N+2$,从而降低了攻击时间复杂度,提高了运行效率.与 Zero-Force 格相似,Yang 等人[32] 利用多项式 g 中大部分系数等于 0 这一特点,提出了在一般情况下恢复 NTRU 私钥的 IN-格攻击.与 Zero-Force 攻击相比,IN-格攻击以相同的概率猜测多项式 g 系数为 0 的位置,但待约化格的维数从 Zero-Force 格的 $2N-r$ 维降为 N 维,进而提高了攻击效率.

3.3　子域攻击

子域攻击是另一种通过降低格的维数来恢复密钥的攻击,也是目前关于 NTRU 密码算法的最新攻击方

式.在子域攻击中攻击者考虑特殊的数域 K,使得其代数整数环恰好同构于多项式环 $R=\mathbf{Z}[X]/(X^N-1)$,因此对于 K 的子域 L,L 的代数整数环也同构于 R 的某一子环.Albrecht,Bai 和 Ducas[33] 在 CRYPTO2016 上推广了 Gentry 的工作[21],用 K 到 L 的绝对模函数 $\mathrm{N}_{K/L}$ 代替了文献[21]中的环同态 φ,进而构造关于 $\mathrm{N}_{K/L}(h)$ 的 CML 格以求解向量 $(\mathrm{N}_{K/L}(g),\mathrm{N}_{K/L}(f))$. 同年 Cheon、Jeong 和 Lee[34] 独立地提出了另一种关于 NTRU 密码算法的子域攻击,在该攻击中 Cheon 等人将 φ 替换为域 K 到 L 的绝对迹函数 $\mathrm{Tr}_{K/L}$,然后在关于 $\mathrm{Tr}_{K/L}(h)$ 的 CML 格中求解目标向量 $(\mathrm{Tr}_{K/L}(f),\mathrm{Tr}_{K/L}(g))$.随后 Kirchner 和 Fouque 在 EUROCRYPT2017 上[35]对上述两种子域攻击进行总结归纳,分析当多项式 g 的模长远远大于 f 时,利用迹函数进行子域攻击的效率更高,当两者模长相近时,环同构应选择模函数,进而构造了更简单高效的新子域攻击.为提高子域攻击效率,Duong 等人[36]对子域攻击中的参数进行了分析,并提出了相应的参数选取方案.

虽然子域攻击成功地将求解 NTRU 密钥问题转化为子域上求解特定向量问题,大大降低了待约化格维数,提高了攻击效率.但攻击过程中需要参数 q 尽可能大,如 $N=512$ 时,$\log_2(q)$ 需大于等于 40,因此子域攻击只适用于 NTRU 算法的变体.并且即使求得子域中的目标向量,如何高效恢复原始的密钥仍然是需要考虑的问题.

4 非格攻击

这里的非格攻击是指不利用格这一数学工具直接对 NTRU 密码进行安全分析的方法,主要包括:选择密文攻击、多重加密传输攻击以及中间相遇攻击等.这些攻击方法利用了 NTRU 在加解密过程中存在的漏洞,直接恢复原始明文或算法私钥.为避免这类攻击,只能改变算法相应的参数或优化加解密流程.

4.1 选择密文攻击

在早期的 NTRU 版本中,不合理的参数往往会导致解密算法输出错误的结果,这不仅影响了算法的可靠性,更是为攻击者提供了许多可乘之机.Jaulmes 和 Joux 在 CRYPTO 2000[37] 上首次提出了针对 NTRU-1998 的选择密文攻击.在该攻击中他们首先构造了少量具有特殊结构的非法密文,由于这些密文结构的特殊性,当作为解密算法的输入时,解密算法以很高的概率发生错误并给出特定的输出,对这些输出进行分析能快速的恢复解密密钥.

为应对选择密文攻击,Hoffstein 和 Silverman 提出了 3 种[16,38] 填充方案,希望新方案能抵抗选择密文攻击.然而 Nguyen 和 Pointcheval 在 CRYPTO 2002[39] 上指出,其中的一种填充方案甚至都不是 IND-CPA 安全的,另外两种方案虽然可以在随机谕言机下被证明是 IND-CCA2 安全,但其证明过程基于一个很强的安全假设.因此,Nguyen 和 Pointcheval 在随机谕言机模型下提出了新的填充方案,改进后方案的 IND-CCA2 安全性只需基于一般的安全性假设.随后,Howgrave-Graham 等人在 CRYPTO 2003[40] 上给出了关于 NTRU 密码算法的一般选择密文攻击,该攻击适用于当时所有的填充方案,在该攻击模型下攻击者需对大量随机选取的明文进行加解密,从而获得足够多的解密错误,进而恢复算法密钥.为减少完成一次攻击所需的明密文对数目,Gama 和 Nguyen 在 PKC2007[41] 上对一般选择密文攻击进行了改进,通过进一步分析解密结果,减少了攻击所需的解密错误数目.

对 NTRU 解密错误的分析推动了 NTRU 密码的可证明安全研究,Stehlé 和 Steinfeld 在 EUROCRYPT 2011[42] 上首次将 NTRU 密码问题的困难性归约到理想格上的 worst-case 问题.随后 Yu 等人在 PKC2017[43] 上将 NTRU 算法的可证明安全方案推广到了分圆环上,并在文献[44]中给出了更一般的结果.

4.2 中间相遇攻击与混合攻击

中间相遇攻击是密码分析的重要手段,在针对 NTRU 密码算法的中间相遇攻击提出之前,遍历求解 NTRU 密钥的时间复杂度是 $\dfrac{\binom{N}{d_f}\binom{N-d_f}{d_f-1}}{\sqrt{N}}$,由于该方法的时间复杂度是关于 N 的指数函数,当 N 取值较大时求解私钥的计算量远远超过了实际的计算能力.为降低直接求解密钥的时间复杂度,2003 年 Nick,Silverman 以及 Whyte 首次将中间相遇攻击的思想应用到恢复 NTRU 密钥中[45],他们将私钥 f 拆分成 f_1,$f_2\in R$ 重量相等的两部分,分别遍历 f_1 与 f_2 的取值空间并计算 $h*(f_1+f_2)$,若 $h*(f_1+f_2)$ 属于集合

$\mathcal{L}_g$,则称 f_1 与 f_2 发生了碰撞,此时容易证明 f_1+f_2 会以很高的概率等于 x^i*f,其中 i 为一正整数.此时中间相遇攻击恢复 NTRU 密钥的时间复杂度是 $\frac{\binom{N/2}{d_f/2}}{\sqrt{N}}$,空间复杂度是 $\frac{\binom{N/2}{d_f/2}}{\sqrt{N}}$.例如:对于 $N=251$ 规模的 NTRU 密码算法,当 $d_f=72$ 时,中间相遇攻击的时间复杂度、空间复杂度均为 2^{100}.

虽然中间相遇攻击大大降低了直接求解密钥的时间复杂度,但消耗了大量的存储空间,并且当参数 N 选取足够大时,该方法依然不能有效恢复密钥.2007 年,Nick 在 CRYPTO2007[47] 上提出了一种结合中间相遇攻击和格攻击的新算法:混合攻击.在混合攻击中,Nick 首先定义了格同构 ϕ,将经典的 NTRU-格同构到另一具有良好结构的格,再对多项式 $\phi(f)$ 的部分系数进行中间相遇攻击,然后用格基约化算法得到完整的 $\phi(f)$,最后对 $\phi(f)$ 进行求逆操作 ϕ^{-1} 恢复原始私钥.这被认为是目前恢复 NTRU 私钥效率最高的算法,在相应实验中当 NTRU 规模 $N=251$ 时,利用混合攻击可使恢复私钥的时间复杂度从 $2^{84.2}$ 降为 $2^{60.3}$,空间复杂度约为 $2^{69.4}$.

4.3　多重传输加密攻击

多重加密传输攻击是一种在未知密钥任何信息的情况下,直接恢复明文的攻击方式.攻击者假设通信中存在的不稳定信道,会导致同一明文在传送过程中被同一公钥多次加密、重复发送.此时攻击者可以利用这些信息获得噪声多项式部分系数,然后遍历搜索恢复噪声多项式剩下的系数,进而得到原始明文.早在文献[15]中,Silverman 就对这种攻击方式进行了描述,并指出单纯的多重传输加密攻击不会对 NTRU 密码算法的安全产生实质性威胁,但这仍是 NTRU 密码算法的一个安全缺陷.为此 Hoffstein 和 Silverman 等人在文献[47]中提供了两种填充方案来抵抗多次加密传输攻击,新的加密方案将噪声多项式隐藏起来,从而免疫了传统的多重加密传输攻击.

虽然文献[47]中提出的填充方案在一定程度上能抵抗简单的多重传输加密攻击,但 Xu 等人在文献[48]中证明,通过简单的变换第一种填充后的加密方案会退化为原始加密方案,因而利用多次加密传输攻击仍能获得噪声多项式部分信息.同时 Xu 发现在第二种填充加密方案中,噪声多项式只有部分信息被隐藏,因此 Xu 提出了基于格的多重传输加密攻击,在多重传输加密模型下成功将恢复噪声多项式的问题转化为格中求最短向量问题,并以 $N=107$ 规模的 NTRU 算法为例成功破解了第二种填充方案.多重加密传输攻击对 NTRU 密码算法安全性的威胁,直到 NTRU-2005 的提出才得到彻底解决.

4.4　广播攻击

在广播环境下假设有一个发送者和 n 个接收者,且所有的接收者都使用相同参数 N,p,q 的 NTRU 密码算法保证通信安全,但有各自的公、私钥对.当发送者将消息广播出去时,他首先独立选取噪声多项式,再利用各自公钥对消息进行加密并将得到的密文发送给 n 个接收者.与多次加密传输攻击相似,广播攻击是另一种直接恢复明文的攻击方法.

Ding 等人在文献[49]中提出了针对 NTRU 密码算法的代数广播攻击,利用 $m\in\{0,1\}$ 这一特点建立了足够多关于明文 m 的非线性方程组,然后通过线性化方法对其进行求解,实验表明,利用该方法能够在多项式时间复杂度和空间复杂度的条件下恢复原始明文.另外,Li 等人[50] 注意到噪声多项式模长固定,提出了更加高效的新型广播攻击.与 pan 等人提出的代数广播攻击相比,新攻击所需的信道数目和建立方程所引入的变量数目更少,因而攻击条件更弱、效率更高.以 NTRU-1998 为例,文献[49]中攻击方法的时间复杂度是 $O(N^9)$,而利用文献[50]中的新型广播攻击,攻击者能在 $O(N^3)$ 的时间复杂度内恢复明文.

5　结　论

本文首先介绍了 NTRU 密码算法的加解密流程及其改进方案,然后从格攻击和非格攻击两种思路分析了 NTRU 算法的安全性.自 1998 年 NTRU 密码算法正式提出,针对 NTRU 算法的分析就层出不穷,为提高算法运算效率,尽可能抵抗已有的攻击,设计者对算法的参数选取方案、加解密流程进行了多次优化和改进,进而缩小了 NTRU 算法与实际应用的差距.

在分析方法中,基于格的经典攻击在待约化格维数较小时能直接恢复私钥,其攻击效率很大程度上取决

于格基约化算法的运行效率.在经典的格攻击中待约化格维数往往很大,使得利用已有格基约化算法很难高效恢复解密密钥.虽然子域攻击较之经典的格攻击极大地降低了待约化格的维数,进而降低了算法的时间复杂度和空间复杂度,但子域攻击只适用于 NTRU 算法的变体,需要相关参数满足特殊的条件,因而子域攻击对原始 NTRU 密码算法安全性没有产生实际的威胁.相对而言,非格攻击是利用 NTRU 算法在参数选取和特定使用情况下存在的漏洞进行的安全分析,因此当设计者对 NTRU 进行相应调整后,这些攻击的时间、空间复杂度远远超过实际接受范围或直接被免疫.

NTRU 密码算法至今已发展近 20 年,在此期间全世界的密码学家围绕着如何提高算法运行效率、安全性,以及如何高效地分析和恢复私钥展开了大量研究,并取得了丰富结果.作为后量子密码的候选者之一,NTRU 不仅保证了数据传输的安全性,更是在签名、构造多线性映射、全同态加密等多个方面得到了广泛应用.相信在未来的 10 年里关于 NTRU 密码算法的研究仍会是密码学的一个热点.

参 考 文 献

[1] Hoffstein J,Pipher J,Silverman J H.NTRU: A high speed public key cryptosystem[C]//Rump Session of CRYPTO.[s.l.:s.n.],1996.

[2] 王小云,刘明洁.格密码学研究[J].密码学报,2014,1(1):13-27.

[3] 周福才,徐剑.格理论与密码学[M].北京:科学出版社,2013.

[4] Goldreich O,Goldwasser S,Halevi S.Public-Key Cryptosystems from Lattice Reduction Problems[M].Berlin:Springer,1997:112-131.

[5] Micciancio D.The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant[J].Foundations of Computer Science,1998,30(6):92-98.

[6] Arora S,Babai L,Stern J,et al.The hardness of approximate optima in lattices,codes,and systems of linear equations[J].Journal of Computer System Sciences,1993,54(2):724-733.

[7] Goldreich O,Micciancio D,Safra S,et al.Approximating shortest lattice vectors is not harder than approximating closest lattice vectors [J].Information Processing Letters,1999,71(2):55-61.

[8] Gama N,Nguyen P Q,Regev O.Lattice Enumeration Using Extreme Pruning[M].Berlin:Springer,2010:257-278.

[9] Chen Y.Réduction de réseau et sécurité concrete du chiffrement completement homomorphe[D].Paris:Université Paris Diderot-paris 7,2013.

[10] Aono Y,Nguyen P Q.Random Sampling Revisited: Lattice Enumeration with Discrete Pruning[M].Berlin:Springer,2017:65-102.

[11] Lenstra A K,Jr H W L,Lovász L.Factoring polynomials with rational coefficients[J].Mathematische Annalen,1982,261(4):515-534.

[12] Schnorr C P,Euchner M.Lattice basis reduction: Improved practical algorithms and solving subset sum problems[J].Mathematical Programming,1994,66(1/2/3):181-199.

[13] Chen Y,Nguyen P Q.BKZ 2.0: Better Lattice Security Estimates[M].Berlin:Springer,2011:1-20.

[14] Aono Y,Wang Y,Hayashi T,et al.Improved Progressive BKZ Algorithms and Their Precise Cost Estimation by Sharp Simulator[M].Berlin:Springer,2016:789-819.

[15] Hoffstein J,Pipher J,Silverman J H.NTRU: A ring-based public key cryptosystem[M].Berlin:Springer,1998:267-288.

[16] Hoffstein J,Silverman J.Optimizations for NTRU[R].[s.l.:s.n.],2001.

[17] Howgrave-Graham N,Silverman J,Whyte W.Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3[J].Topics in Cryptology - CT-RSA,2005(3376):118-135.

[18] Silverman J H.Invertibility in Truncated Polynomial Rings[R].[s.l.:s.n.],1998.

[19] Silverman J H.High Speed Multiplication of (Truncated) Polynomials[R].[s.l.:s.n.],1999.

[20] Silverman J H.Wraps,Gaps,and Lattice Constants[R].[s.l.:s.n.],1999.

[21] Gentry C.Key Recovery and Message Attacks on NTRU-Composite[M].Berlin:Springer,2001:182-194.

[22] Consortium for Efficient Embedded Security.Efficient embedded security standards]1: Implementation aspects of NTRU and NSS[R].[s.l.:s.n.],2001.

[23] Consortium for Efficient Embedded Security.Efficient embedded security standards]1: Implementation aspects of NTRUEncrypt and NTRUSign[R].[s.l.:s.n.],2001.

[24] Bernstein D J,Chuengsatiansup C,Lange T,et al.NTRU Prime[J].IACR Cryptology ePrint Archive,2016(2016):461.

[25] Coppersmith D,Shamir A.Lattice Attacks on NTRU[M].Berlin:Springer,1997:52-61.

[26] Silverman J H,Whyte W.Estimated Breaking Times for NTRU Lattices[R].[s.l.:s.n.],1999.

[27] Bi J,Cheng Q.Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices[J].Theoretical Computer Science,2014(560):121-130.

[28] May A.Cryptanalysis of NTRU[R].[s.l.:s.n.],1999.

[29] Silverman J H.Dimension-reduced lattices，zero-forced lattices，and the NTRU public key cryptosystem[R].[s.l.：s.n.]，1999.
[30] May A，Silverman J H.Dimension reduction methods for convolution modular lattices[M].Berlin：Springer，2001：110-125.
[31] Han D.A new lattice attack on NTRU cryptosystem[J].Trends Math，2005，8(1)：197-205.
[32] Yang Z C，Fu S J，Qu L J，et al.A lower dimension lattice attack on NTRU[J].Science China Information Sciences，2018，61(5)：059101：1-059101：3.
[33] Albrecht M，Bai S，Ducas L.A subfield lattice attack on overstretched NTRU assumptions[M].Berlin：Springer，2016：153-178.
[34] Cheon J H，Jeong J，Lee C.An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero[J].LMS Journal of Computation and Mathematics，2016，19(A)：255-266.
[35] Kirchner P，Fouque P A.Revisiting Lattice Attacks on Overstretched NTRU Parameters[M].Berlin：Springer，2017：3-26.
[36] Duong D H，Yasuda M，Takagi T.Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU[C]//International Conference on Information Security.Berlin：Springer，2017：79-91.
[37] Jaulmes É，Joux A.A chosen-ciphertext attack against NTRU[M].Berlin：Springer，2000：20-35.
[38] Hoffstein J，Silverman J H.Protecting NTRU against chosen ciphertext and reaction attacks[R].[s.l.：s.n.]，2000.
[39] Nguyen P Q，Pointcheval D.Analysis and Improvements of NTRU Encryption Paddings[M].Berlin：Springer，2002：210-225.
[40] Howgrave-Graham N，Nguyen P Q，Pointcheval D，et al.The Impact of Decryption Failures on the Security of NTRU Encryption[M].Berlin：Springer，2003：226-246.
[41] Gama N，Nguyen P Q.New Chosen-Ciphertext Attacks on NTRU[M].Berlin：Springer，2007：89-106.
[42] Stehlé D，Steinfeld R.Making NTRU as Secure as Worst-Case Problems over Ideal Lattices[M].Berlin：Springer，2011：27-47.
[43] Yu Y，Xu G，Wang X.Provably Secure NTRU Instances over Prime Cyclotomic Rings[M].Berlin：Springer，2017：409-434.
[44] Yu Y，Xu G，Wang X.Provably Secure NTRUEncrypt over More General Cyclotomic Rings[J].IACR Cryptology ePrint Archive，2017(2017)：304.
[45] Howgrave-Graham N，Silverman J H，Whyte W.A Meet-In-The-Middle Attack on an NTRU Private Key[R].[s.l.：s.n.]，2003.
[46] Howgravegraham N.A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU[M].Berlin：Springer，2007：150-169.
[47] Hoffstein J，Silverman J H.Implementation notes for NTRU PKCS multiple transmissions[R].[s.l.：s.n.]，1998.
[48] Xu J，Hu L，Sun S，et al.Cryptanalysis of countermeasures against multiple transmission attacks on NTRU[J].IET Communications，2014，8(12)：2142-2146.
[49] Ding J，Pan Y，Deng Y.An algebraic broadcast attack against NTRU[C]//Australasian Conference on Information Security and Privacy.Berlin：Springer，2012：124-137.
[50] Li J，Pan Y，Liu M，et al.An efficient broadcast attack against NTRU[C]//Proceedings of the 7th ACM Symposium on Information，Computer and Communications Security.[s.l.]：ACM，2012：22-23.

Cryptanalysis of NTRU cryptosystem

Li Chao[a,b]，Yang Zhichao[a]

(a.College of Computer Science；b.College of Arts and Sciences，National University of Defense Technology，Changsha 410073，China)

Abstract：With the rapid development of quantum computing，most public key cryptosystem such as RSA，ECC etc. can be broken within polynomial time complexity by quantum computer algorithm.NTRU has drawn considerable attention for its potential anti-quantum ability，high speed，low memory requirements. In this paper，we first introduce the NTRU cryptosystem. Then，our attention will be focused on the security of NTRU cryptosystem under the lattice attack and non-lattice attack，especially，the latest works on the subfield lattice attack and the decryption failed attack.

Keywords：NTRU；cryptanalysis；lattice；lattice algorithm

[责任编校　陈留院]