NTRU公钥密码体制的等价密钥

熊志坚[1] 王衍波[2] 张 涛[1] 王金双[1]
(解放军理工大学指挥自动化学院 南京 210007)[1] (解放军理工大学通信工程学院 南京 210007)[2]

摘 要 NTRU公钥密码体制存在多个私钥对应同一个公钥的问题。首先分析了NTRU成功解密的条件,提出NTRU等价密钥的概念。然后给出了NTRU截尾多项式环上多项式可逆的充分必要条件和NTRU|.|$_\infty$半范数的相关性质,提出4种等价密钥的构造方法。最后分析了NTRU等价密钥对NTRU安全性的影响。分析表明,NTRU参数选择不当会导致一些特殊形式的等价密钥存在,严重威胁安全性。

关键词 NTRU公钥密码体制,截尾多项式环,可逆多项式,半范数,等价密钥
中图法分类号 TP309.7 **文献标识码** A

Equivalent Keys in NTRU Public Key Cryptosystem

XIONG Zhi-jian[1] WANG Yan-bo[2] ZHANG Tao[1] WANG Jin-shuang[1]
(Institute of Command Automation, PLA University of Science and Technology, Nanjing 210007, China)[1]
(Institute of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China)[2]

Abstract NTRU public Key cryptosystem has the problem that multiple private keys correspond to a common pubic key. Firstly the condition of decryption was discussed, and the conception of equivalent keys in NTRU was proposed. Secondly the invertibility of polynomials in truncated polynomial ring and the |.|$_\infty$ semi-norm were discussed, and four schemes to construct equivalent keys were presented. Finally the security effect of equivalent keys was analyzed, which indicates that if NTRU parameters are not chosen properly, some special equivalent keys will pose a serious security threat to NTRU.

Keywords NTRU public key cryptosystem, Truncated polynomial ring, Invertible polynomial, Semi-norm, Equivalent keys

1 引言

NTRU在Crypto 96被首次提出[1],其后经过两年时间的讨论,于1998年正式发表[2]。包括NTRU提出者在内的很多密码学家,分析了NTRU的安全性,提出了很多攻击方法,但攻击效果都不理想。于此同时,NTRU不断地改进,并于2009年被接受为IEEE P1363.1标准。

密码学界普遍认为,NTRU的安全性是基于格上的一类困难问题,是最可能抵抗量子攻击的公钥密码体制之一[3]。至今,还没有发现它存在什么重大的安全问题。

NTRU等价密钥的研究最早见于Coppersmith[4]等人的工作。Coppersmith提出了一种NTRU格攻击算法,该算法返回最初的私钥或者私钥的一个等价密钥。但实验表明,这些等价密钥的存在并不足以对NTRU的安全性构成威胁[2]。文献[5]提出,私钥的循环移位变形依然可以用于成功解密。此外,负密钥也可以用于解密。

本文对NTRU等价密钥进行研究,一方面是寻找密钥的规律,以缩小攻击算法中密钥搜索空间;另一方面,分析NTRU等价密码对NTRU安全性的影响,为NTRU的安全使用提供一些实际的建议。

2 NTRU公钥密码体制

NTRU公钥密码体制是基于截尾多项式环的,依赖于参数N、p、q,其中$N>1$,p、q互素,且q远大于p。

定义1(截尾多项式环) $\boldsymbol{R}=\boldsymbol{Z}[x]/(x^N-1)$表示$N-1$次整数多项式的集合。用$N$维向量$[f_0,f_1,\cdots,f_{N-1}]$表示$N-1$次整数多项式$f=f_0+f_1x+\cdots+f_{N-1}x^{N-1}$,$\boldsymbol{R}$上的加法和乘法如下

(1)$[f_0,f_1,\cdots,f_{N-1}]+[g_0,g_1,\cdots,g_{N-1}]=[f_0+g_0,f_1+g_1,\cdots,f_{N-1}+g_{N-1}]$;

(2)$[f_0,f_1,\cdots,f_{N-1}]*[g_0,g_1,\cdots,g_{N-1}]=h$,其中$h_k=\sum_{i+j=k \bmod N} f_i*g_j$。

如此定义的$(\boldsymbol{R},+,*)$构成的代数系统称为截尾多项式环。

文中将不再区分环$\boldsymbol{R}$中元素的多项式表示和向量表示。

定义2(多项式宽度) 多项式的最大系数与最小系数的

到稿日期:2011-08-11 返修日期:2011-11-23

熊志坚(1987-),男,硕士生,主要研究方向为网络信息安全,E-mail:kuperain@sina.com;王衍波(1961-),男,教授,硕士生导师,主要研究方向为网络安全、现代密码学;张 涛(1973-),男,副教授,硕士生导师,主要研究方向为网络安全、操作系统安全;王金双(1978-),男,博士,讲师,主要研究方向为形式化方法。

差，称为多项式的宽度，记为$|F|_\infty=\max(F_i)-\min(F_i)$。

定义 3(规约模) 多项式 f 是规约模 p 的，指的是 f 的系数在$(-p/2,p/2]$区间。

定义 4 多项式 f 属于集合$L(d_1,d_2)$，表示 f 中有 d_1 个系数为 1、d_2 个系数均为 -1，其余的系数为 0。记 $L_f=L(d_f,d_f-1)$，$L_g=L(d_g,d_g)$，$L_r=L(d_r,d_r)$。

2.1 密钥生成

在 L_f 和 L_g 中选择两个多项式 f 和 g，使得存在 F_p、$F_q\in \boldsymbol{R}$，满足 $F_p*f\equiv 1(\bmod p)$，$F_q*f\equiv 1(\bmod q)$；计算 $h\equiv F_q*g(\bmod q)$。

把 h 作为公钥，N、p、q 也是公开的，并把 f 作为私钥，同时需要保密的还有 F_p、F_q。

2.2 加密算法

对多项式 m(规约模 p 的)进行加密，即 m 是明文。L_r 中任选多项式 r，计算 $e\equiv pr*h+m(\bmod q)$，即为密文。

2.3 解密算法

首先计算 $a\equiv f*e(\bmod q)$，其次把 a 的系数调整到$(-q/2,q/2]$区间内，然后计算 $m'\equiv F_p*a(\bmod p)$，最后对 m' 做规约模 p 运算，得到明文 m。

3 解密条件

NTRU 并不总是可以成功解密，但通过适当选择参数，可以以非常高的概率避免解密失败的发生[2]。

3.1 解密原理

$$a\equiv f*e\equiv f*(pr*h+m)\equiv f*(pr*F_q*g+m)$$
$$\equiv pr*g+f*m(\bmod q)$$

若假定 $pr*g+f*m$ 是规约模 q 的，则对其规约模 q，多项式系数将不发生改变，即 $a=pr*g+f*m$。

$$F_p*a\equiv F_p*(pr*g+f*m)\equiv F_p*f*m\equiv m(\bmod p)$$

由于 m 是规约模 p 的，因此只需对最后结果进行一次规约模 p 运算，就可以正确地恢复出明文。

所以，如果 $pr*g+f*m$ 是规约模 p 的，那么 NTRU 解密可以准确地恢复明文。

如果 $pr*g+f*m$ 的系数不在$(-q/2,q/2]$区间内，那么解密通常会失败，并且解密者不知道发生了失败。当然，如果参数选择是合适的，那么绝大部分情况下还是可以保证 $pr*g+f*m$ 是规约模 p 的[2]。

如果 $pr*g+f*m$ 的系数不在$(-q/2,q/2]$区间内，但满足$|pr*g+f*m|_\infty\leqslant q$，即多项式的宽度小于 q，只需把这些系数调整到$(-q/2,q/2]$区间内，就可以成功解密出原始明文 m[6]。

3.2 解密条件

前面已经分析，如果满足(1) f 是 $\boldsymbol{R}$ 上模 p、模 q 可逆的多项式，且(2) $|pr*g+f*m|_\infty\leqslant q$，那么 NTRU 可以解密成功。

定义 5(等价密钥) 设(h,f)是明密文对(m,e)的公钥和私钥。如果多项式 $T(f)$ 能与私钥 f 一样，对密文 e 成功解密，得到明文 m，则称 $T(f)$ 为 f 的等价密钥。

定理 1 多项式 $T(f)$ 满足：(1) $T(f)$ 是环 $\boldsymbol{R}$ 上模 p、模 q 可逆的；(2) $|pr*g'+T(f)*m|_\infty\leqslant q$，其中 $g'\equiv T(f)*h(\bmod q)$；则 $T(f)$ 是 f 的等价密钥。

3.3 多项式可逆

在密钥生成算法中，需要计算私钥 f 在环 $\boldsymbol{R}$ 上 f 模 p、模 q 的逆多项式，即寻找多项式 F_p、$F_q\in\boldsymbol{R}$，满足 $f*F_p\equiv 1(\bmod p)$、$f*F_q\equiv 1(\bmod q)$。

文献[7]指出，环 $\boldsymbol{R}$ 上的多项式几乎都是环 $\boldsymbol{R}$ 上模 p、模 q 可逆的，并给出了类似于欧几里得算法的多项式求逆算法，但没有严格地给出多项式环 $\boldsymbol{R}$ 上可逆的条件。文献[8]指出，在环 $\boldsymbol{R}$ 上求多项式的模逆多项式，即等价于求由多项式生成的循环矩阵的逆。事实上，循环矩阵是可逆矩阵，并不是环 $\boldsymbol{R}$ 上逆多项式存在的充分必要条件。

定理 2[9] 设 n 是素数，V 是一个 $n*n$ 的有理数循环矩阵，

$$V=\text{cirMatrix}(v_1,v_2,\cdots,v_{N-1}),v_i\in\boldsymbol{Q}$$

矩阵 V 的行列式 $\det(V)=0$，当且仅当 $\sum v_i=0$，或 $v_1=v_2=\cdots=v_{N-1}$。

在 NTRU 中，N 取为素数[10]，且 $\sum f_i=1$，$f_i\in L_f$，所以 $\det(C_f)\neq 0$，即 f 生成的循环矩阵 C_f 都是可逆的。但并不是 L_f 中所有多项式都是模 p、q 可逆的[2]。也就是说，循环矩阵是可逆矩阵，但并不能保证环 $\boldsymbol{R}$ 上多项式模可逆。

定义 6(矩阵模 q 可逆) 方阵 C 是模 q 可逆的，如果存在矩阵 $C-1$，满足 $C*C^{-1}\equiv I(\bmod q)$，其中 I 表示单位矩阵。

引理 1 环 $\boldsymbol{R}$ 中两个多项式的乘积等于其中一个多项式与另一个多项式生成的循环矩阵的乘积，即 f、$g\in\boldsymbol{R}$，$f*g=f*\text{cirMatrix}(g)$，其中

$$\text{cirMatrix}(g)=\begin{bmatrix} g_0 & g_1 & \cdots & g_{N-2} & g_{N-1} \\ g_{N-1} & g_0 & \cdots & g_{N-3} & g_{N-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_1 & g_2 & \cdots & g_{N-1} & g_0 \end{bmatrix}$$

证明：设 $f*g=[f_0,f_1,\cdots,f_{N-1}]*[g_0,g_1,\cdots,g_{N-1}]=h$，则

$$h_k=\sum_{i+j=k \bmod N} f_i*g_j$$

把$[h_1,h_2,\cdots,h_{N-1}]$写成矩阵形式，即为

$$[h_0\quad h_1\quad\cdots\quad h_{N-1}]=[f_0\quad f_1\quad\cdots\quad f_{N-1}]*\begin{bmatrix} g_0 & g_1 & \cdots & g_{N-2} & g_{N-1} \\ g_{N-1} & g_0 & \cdots & g_{N-3} & g_{N-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_1 & g_2 & \cdots & g_{N-1} & g_0 \end{bmatrix}$$

故 $f*g=f*\text{cirMatrix}(g)$。

定理 3 环 $\boldsymbol{R}$ 上多项式 f 模 q 可逆的充要条件是多项式 f 的循环矩阵是模 q 可逆的。

证明：把多项式写成矩阵的形式，所以 $F_q*C_f\equiv[1,0,\cdots,0](\bmod q)$。

(1)充分性。若 C_f 是模 q 可逆的，那么

$$F_q*C_f*C_f^{-1}\equiv[1,0,\cdots,0]*C_f^{-1}(\bmod q)$$
$$F_q\equiv[1,0,\cdots,0]*C_f^{-1}(\bmod q)$$

用 $C_f^{-1}[1,:]$表示$[1,0,\cdots,0]*C_f^{-1}$，即 C_f^{-1} 的第一行元素构成的向量，所以

$$F_q\equiv C_f^{-1}[1,:](\bmod q)$$

(2)必要性。由于循环矩阵的逆矩阵也是循环矩阵[8]，因此 F_q 存在，表明多项式 f 的循环矩阵是模 q 可逆的。

引理 2[11] 方阵 C 模 q 可逆的充分必要条件是矩阵 C 的行列式与 q 互素，即 $GCD(\det(C),q)=1$。

定理 4 NTRU 公钥密码体制中，多项式 f 模 p、模 q 可

逆的充分必要条件是 $\det(C_f)\equiv\pm1 \pmod 6$。

证明：NTRU 的参数方案中，$p=3$，q 为 2 的指数。由定理 3 和引理 2，得 $GCD(\det(C_f),2)=1$，$GCD(\det(C_f),3)=1$。所以，$\det(C_f)\equiv\pm1 \pmod 6$。

3.4 $|.|_\infty$ 半范数

前面已经给出了多项式宽度的定义。由于其满足绝对齐次性和三角不等式，但不满足正定性，因此 $|.|_\infty$ 是多项式的一个半范数。

定理 5 $\forall s,t\in R,\lambda\in Z,I=1+x+\cdots+x^{N-1}$，$|.|_\infty$ 有如下性质：

(1)非负性：$|s|_\infty\geqslant0$，$|s|_\infty=0$ 当且仅当 $s=\lambda I$；

(2)绝对齐次性：$|\lambda s|_\infty=|\lambda|*|s|_\infty$；

(3)三角不等式：$|s+t|_\infty\leqslant|s|_\infty+|t|_\infty$，当且仅当 s、t 的最大、最小系数的位置相同时，等号成立。

此外，可以证明如下结论。

定理 6 $\forall s,t\in R$，$|s*t|_\infty\leqslant(\sum|t_i|)|s|_\infty$。

证明：$s*t=\sum s*(t_ix^i)=\sum(t_is)*x^i$，其中 $(t_is)*x^i$ 表示把多项式 s 的系数都乘以 t_i，然后循环右移 i 位，$i=1,2,\cdots,N-1$。所以

$$|(t_is)*x^i|_\infty=|t_is|_\infty=|t_i|*|s|_\infty$$

$$|s*t|_\infty=|\sum(t_is)*x^i|_\infty\leqslant\sum|(t_is)*x^i|_\infty=\sum(|t_i|*|s|_\infty)=(\sum|t_i|)|s|_\infty$$

其中，$|\sum(t_is)*x^i|_\infty\leqslant\sum|(t_is)*x^i|_\infty$ 等号成立，当且仅当所有多项式 $(t_is)*x^i$ 的最大、最小系数的位置相同。

我们可以对 $|pr*g+f*m|_\infty$ 进行估计：

$$|pr*g+f*m|_\infty\leqslant|pr*g|_\infty+|f*m|_\infty=p|r*g|_\infty+|f*m|_\infty$$

由于 f、g、r 是系数为 -1、0、1 的多项式，因此 $|f|_\infty=|g|_\infty=|r|_\infty=2$，

$$|r*g|_\infty\leqslant4d_r$$

$$|f*m|_\infty\leqslant2(2d_f+1)$$

这里不把不等式右边写成 $4d_g$ 的原因是，实际参数中，$d_r<d_g$。所以，$|pr*g+f*m|_\infty\leqslant4d_f+12d_r+2$。

如果 $4d_f+12d_r+2\leqslant q$ 成立，则不会出现解密失败的情况(文献[12]中有类似的结论)。由定理 1 知，L_f 中任意满足 $d_f\leqslant(q-12d_r-2)/4$ 的可逆多项式，都可以对密文 e 成功解密。显然，这样的 NTRU 毫无安全性可言。

因此，在选择 NTRU 参数的时候，我们至少需要使得 $(q-12d_r-2)/4<1$。NTRU 标准参数[2]即是如此，见表 1。

表 1 NTRU 标准参数

N	P	q	d_r	$d_f\leqslant(q-12d_r-2)/4$	$\lvert h\rvert_\infty\leqslant(q-p+1)/(2pd_r)$
107	3	64	5	$\leqslant0.5$	$\leqslant2$
167	3	128	18	<0	$\leqslant1$
503	3	256	55	<0	$=0$

4 等价密钥

环 $\boldsymbol{R}$ 上，任选一个多项式，只要能恢复出原始明文，就称为相应明、密文对的解密密钥的等价密钥。定理 1 给出了构造等价密钥的方法，即满足定理 1 中(1)、(2)这两个条件的多项式，都可以用于加密。设 (h,f) 是明、密文对 (m,e) 的公钥和私钥，$T(f)$ 是 f 的等价密钥。若无特别说明，下文中的 f、$T(f)$ 都不仅限于 L_f。

4.1 方法一

命题 1 k 是环上任意多项式，$f+qk$、$f+pk$、$f+Nk$ 都是 f 的等价密钥。

证明：对 $f+qk$ 进行规约模 q 运算，即可得到原始密钥 f，所以 $f+qk$ 是 f 的等价密钥；同理，$f+pk$、$f+Nk$ 也是 f 的等价密钥。

值得说明的是，这些等价密钥用于解密，并不遵循 NTRU 解密算法。在解密过程中，如果采用 NTRU 解密算法，则无法保证解密得到的消息就是原始明文。

4.2 方法二

命题 2 如果公钥 h 满足 $|r*h|_\infty\leqslant(q-p+1)/p$，则 $T(f)=1$ 是 f 的等价密钥，且对任意的明密文对都成立。

证明：首先 $T(f)=1$ 是可逆的。令 $g'=h$，其满足 $h\equiv T(f)^{-1}*g' \pmod q$。由于 $|pr*g'+T(f)*m|_\infty=|pr*h+m|_\infty$，且

$$|pr*h+m|_\infty\leqslant|pr*h|_\infty+|m|_\infty=p|r*h|_\infty+p-1$$

又 $|r*h|_\infty\leqslant(q-p+1)/p$，因此 $|pr*g'+T(f)*m|_\infty\leqslant q$。

推论 如果公钥 h 满足 $|h|_\infty\leqslant(q-p+1)/(2pd_r)$，则 $T(f)=1$ 是 f 的等价密钥，且对任意的明密文对都成立。

证明：由于 $|r*h|_\infty\leqslant(\sum|r_i|)|h|_\infty=2d_r*|h|_\infty$，且 $|h|_\infty\leqslant(q-p+1)/(2pd_r)$，因此 $|r*h|_\infty\leqslant(q-p+1)/p$。

NTRU 标准参数中，$T(f)=1$ 这种等价密钥是可能存在的，见表 1。虽然发生的概率很低，但它却是致命的安全隐患。

不难看出，如果 $|pr*h+m|_\infty\leqslant q$，则对明文 m 的加密过程中模 q 运算不发挥实质的作用。通过对密文 e 进行一定的移位，然后进行模 p 运算，就可以完成解密。为了避免这种情况的发生，最直接的方法就是使用系数尽可能“随机的”公钥；且在加密过程中，计算 $r*h$，如果其宽度与 $q/3$ 很接近，则重新选择多项式 r，直到 $r*h$ 的范数远大于 $q/3$。

4.3 方法三

引理 3 s、t 是 $\boldsymbol{R}$ 上可逆多项式，则 $s*t$ 也是可逆的，且 $(s*t)^{-1}\equiv s^{-1}*t^{-1} \pmod q$。

证明：$t^{-1}*s^{-1}*s*t\equiv1 \pmod q$，故 $(s*t)^{-1}\equiv s^{-1}*t^{-1} \pmod q$。

命题 3 设 c 是一个 $\boldsymbol{R}$ 上的可逆多项式，且满足以下条件之一：(1) $\sum|c_i|\leqslant\dfrac{q}{|pr*g+f*m|_\infty}$；(2) $|c|_\infty\leqslant\dfrac{q}{\sum|(pr*g+f*m)_i|}$；则 $T(f)=f*c$ 是 f 的等价密钥。

证明：由于 f、c 都是可逆多项式，因此 $f*c$ 也是可逆多项式。令 $g'=g*c$，则 $h\equiv T(f)^{-1}*g' \pmod q$。

$$pr*g'+T(f)*m=(pr*g+f*m)*c$$

由定理 6，得

$$|(pr*g+f*m)*c|_\infty\leqslant(\sum|c_i|)|pr*g+f*m|_\infty$$

$$|(pr*g+f*m)*c|_\infty\leqslant(\sum|(pr*g+f*m)_i|)|c|_\infty$$

由(1)或(2)都可以得到，$|(pr*g+f*m)*c|_\infty\leqslant q$。

综上，$T(f)=f*c$ 是 f 的等价密钥。

特别地，由于 $\dfrac{q}{|pr*g+f*m|_\infty}\geqslant1$，且 $\pm x^i$ 可逆($i=0,1,\cdots,N-1$)，因此 $f*(\pm x^i)$ 是 f 的等价密钥，可以对任意密文解密。文献[5]中的结论是方法三的一种特殊情况。

4.4 方法四

引理 4 NTRU 算法中，对于私钥 f(包括等价密钥)，$\sum f_i \equiv \pm 1 \pmod 6$。

证明：私钥 f 必须可逆，即存在多项式 F_p、$F_q \in \boldsymbol{R}$，满足 $f * F_p \equiv 1 \pmod p$、$f * F_q \equiv 1 \pmod q$。所以，$f(1) * F_p(1) \equiv 1 \pmod p$、$f(1) * F_q(1) \equiv 1 \pmod q$，即 $f(1) = \sum f_i$ 存在模 p、q 的乘法逆元。

NTRU 算法中，取 $p=3$，q 为 2 的指数，所以 $\sum f_i$ 与 2、3 互素，即 $\sum f_i \equiv \pm 1 \pmod 6$。

引理 5 环 $\boldsymbol{R}$ 上，$s * I = (\sum s_i) I$。

证明：$s * I = s * \begin{bmatrix} 1 & \cdots & 1 \\ \cdots & \cdots & \cdots \\ 1 & & 1 \end{bmatrix} = (\sum s_i) I$。

命题 4 当 $\sum f_i \equiv 1 \pmod 6$，$f+\lambda I$ 是 f 的等价密钥的充要条件是 $\lambda \equiv 0、2 \pmod 6$；当 $\sum f_i \equiv -1 \pmod 6$，$f+\lambda I$ 是 f 的等价密钥的充要条件是 $\lambda \equiv 0、-2 \pmod 6$。$T(f)$ 模 q 的逆元为 $F \equiv F_q - \lambda (\sum f_i)^{-1} (\sum f_i + N\lambda)^{-1} I \pmod q$，模 p 的逆元有类似的形式。

证明：$g' \equiv T(f) * h \equiv (f+\lambda I) * h \equiv g + (\lambda \sum h_i) I \pmod q$。

令 $g' = g + (\lambda \sum h_i) I$，则 $pr * g' + T(f) * m = pr * g + p\lambda (\sum h_i) r * I + f * m + \lambda I * m = pr * g + f * m + p\lambda (\sum h_i) * (\sum r_i) I + \lambda (\sum m_i) I$。显然，$|pr * g' + T(f) * m|_\infty = |pr * g + f * m|_\infty \leqslant q$。

下面考虑 $T(f) = f + \lambda I$ 在环 $\boldsymbol{R}$ 上的可逆问题。

假设 $T(f)$ 是环 $\boldsymbol{R}$ 上模 q 可逆的，且 $T(f) * F \equiv 1 \pmod q$，则

$(f+\lambda I) * F \equiv 1 \pmod q$

$F \equiv F_q * [1 - (\lambda \sum F_i) I] \equiv F_q - \lambda (\sum F_i)(\sum F_{qi}) I \pmod q$

由于 $\sum F_{qi} \equiv (\sum f_i)^{-1} \pmod q$，$\sum F_i \equiv (\sum f_i + N\lambda)^{-1} \pmod q$，因此 $T(f)$ 模 q 的逆元为 $F \equiv F_q - \lambda (\sum f_i)^{-1} (\sum f_i + N\lambda)^{-1} I \pmod q$。

显然，$T(f)$ 存在模 q 的逆元，当且仅当 $\sum f_i + N\lambda$ 存在模 q 的逆元。

NTRU 算法中，取 $p=3$，q 为 2 的指数，故 $T(f)$ 是模 p、q 可逆的充要条件是 $\sum f_i + N\lambda$ 与 2、3 互素，即 $\sum f_i + N\lambda \equiv \pm 1 \pmod 6$。一般地，$N = 107、167、503$ 均为奇素数，且 $N \equiv -1 \pmod 6$，故 $\sum f_i - \lambda \equiv \pm 1 \pmod 6$。

由引理得：

(1)当 $\sum f_i \equiv 1 \pmod 6$，$\sum f_i - \lambda \equiv 1 \pmod 6$ 时，$\lambda \equiv 0 \pmod 6$；

(2)当 $\sum f_i \equiv 1 \pmod 6$，$\sum f_i - \lambda \equiv -1 \pmod 6$ 时，$\lambda \equiv 2 \pmod 6$；

(3)当 $\sum f_i \equiv -1 \pmod 6$，$\sum f_i - \lambda \equiv 1 \pmod 6$ 时，$\lambda \equiv -2 \pmod 6$；

(4)当 $\sum f_i \equiv -1 \pmod 6$，$\sum f_i - \lambda \equiv -1 \pmod 6$ 时，$\lambda \equiv 0 \pmod 6$。

所以，当 $\sum f_i \equiv 1 \pmod 6$，$f+\lambda I$ 在环 $\boldsymbol{R}$ 上的可逆的充要条件是 $\lambda \equiv 0、2 \pmod 6$；当 $\sum f_i \equiv -1 \pmod 6$，$f+\lambda I$ 在环 $\boldsymbol{R}$ 上的可逆的充要条件是 $\lambda \equiv 0、-2 \pmod 6$。

特别地，如果 $f \in L_f$，则 $\sum f_i = 1$，$f+\lambda I$ 是 f 的等价密钥，其中 $\lambda \equiv 0、2 \pmod 6$。

4.5 等价密钥对 NTRU 安全性的影响

方法一构造得到的等价密钥，其解密方法与 NTRU 解密算法不一样，所以不能直接作为 NTRU 解密算法的输入；方法二表明，NTRU 使用过程中，应尽可能地使用系数“随机”化的多项式作为公钥，且多项式 r 的选择不能是随机的，必须保证 $|r * h|_\infty$ 远大于 $q/3$，否则加密算法存在一个“万能的”解密密钥；方法三表明，对密钥取负，或循环移位，依然可用于解密，甚至密钥乘上一个小系数多项式，也可以解密；L_f 中循环密钥的个数为 $N-1$；方法四表明，如果 $f \in L_f$，则在 $L_f + \lambda I$ 空间中，存在等价密钥 $f+\lambda I$，其中 $\lambda \equiv 0、2 \pmod 6$。显然，如果把“$-1$”、“0”、“1”和“$-1+\lambda$”、“$0+\lambda$”、“$1+\lambda$”看作是相同符号的两种不同表示方式，则方法四中“平移”得到的密钥，与原始密钥等价，即没有新的形式的密钥出现。

结束语 NTRU 公钥密码体制存在多个私钥对应同一个公钥的问题。通过研究 NTRU 解密条件，提出了 4 种构造等价密钥的方法，并分析了它们对 NTRU 安全性的影响。研究表明，NTRU 的等价密钥非常多，如在 L_f 中就至少有 $O(N)$ 个；此外，多项式 g、r 不能随机选择，除了必须满足解密成功的条件外，还需要保证它们的计算结果足够地随机，否则就可能出现一些特殊形式的等价密钥，这将严重威胁 NTRU 的安全性。关于等价密钥的更多构造方法，如系数之间的置换以及如何使得两个多项式的卷积结果尽可能随机化，是本文的后续工作。

参 考 文 献

[1] Hoffstein J, Pipher J, Silverman J H. NTRU: A new high speed public key cryptosystem [J]. Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, 1423

[2] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem [J]. Algorithmic Number Theory, 1998, 1423: 267-288

[3] Perlner R A, Cooper D A. Quantum Resistant Public Key Cryptography: A Survey[C]// Proc. of IDtrust. 2009: 85-93

[4] Coppersmith D, Shamir A. Lattice attacks on NTRU [C] // Proceedings of the 16th Annual International Conference on Theory and Application of Cryptographic Techniques. Konstanz, Germany: Springer-Verlag, 1997: 52-61

[5] Jarvis K. NTRU over the Eisenstein Integers [D]. Carleton University, 2011

[6] Hoffstein J, Silverman J H. Optimizations for NTRU [J]. Public-key Cryptography and Computational Number Theory, De-Gruyter, 2000

[7] Silverman J H. NTRU Report 014. Almost Inverses and Fast NTRU Key Creation[EB/OL]. http://www.ntru.com, 1999

[8] Bini D, Corso G M D, Manzini G, et al. Inversion of circulant matrices over Z_m[J]. Mathematics of Computation, 2001, 70(235): 1169-1182

[9] Geller D, Kra I, Popescu S, et al. On circulant matrices [M]. Preprint, Stony Brook University

[10] Gentry C. Key recovery and message attacks on NTRU-composite[C]// Advances in Cryptology—Eurocrypt 2001. 2001: 182-194

[11] Stinson D R. Cryptography: theory and practice [M]. CRC Press, 2006

[12] Hoffstein J, Pipher J, Silverman J H. An introduction to mathematical cryptography [M]. Springer Verlag, 2008