关于D-NTRU公钥加密算法的安全性

王林
保密通信重点实验室

摘要

在现有参数选取下，D-NTRU算法存在成功概率大于99%的选择明文攻击，不具备语义安全性。建议考察应用NTRU Prime变体的可行性。

1 算法描述

以下使用的符号与算法描述 [1]原文一致。

1.1 算法简要描述

1.1.1 算法主要数据

算法涉及的主要数据包括系统参数、公钥、私钥、明文、密文。
系统参数：N，$p=3$，q_1，$q_2=q_1+2$。 其中N决定了截断多项式环$\mathbb{R}=\mathbb{Z}[x]/(x^N-1)$。
算法的公钥：$h_1\in\mathbb{R}_{q_1}$和$h_2\in\mathbb{R}_{q_2}$。
算法的私钥：$f\in\mathfrak{L}(d_f,d_f-1)$，$f_p^{-1}$和$G\in\mathbb{R}_{q_1}$。
明文编码：$M\in\mathbb{R}_{q_2}$。
密文：$c_1\in\mathbb{R}_{q_1}$和$c_2\in\mathbb{R}_{q_2}$。
算法的具体描述参见 [1]。

1.1.2 算法加密操作

加密过程：随机选取$r_1\in\mathfrak{L}(d_p,d_{r_1}^n)$和$r_2\in\mathbb{R}_p$. 计算

$$c_1=\langle r_1\otimes h_1+r_2\rangle_{q_1}; \tag{1}$$
$$c_2=\langle r_1\otimes h_2+r_2+M\rangle_{q_2}. \tag{2}$$

1.1.3 算法参数规格实例

根据算法描述文档 [1]及其实现C代码 [2]，将代码中的三组实例参数列表如下。

表格 1: D-NTRU算法中使用的实例参数

k	N	p	q_1	q_2	d	d_f^n	d_g^n	$d_{r_1}^n$
120	157	3	269	271	53	52	52	53
172	223	3	269	271	75	74	74	75
270	349	3	521	523	117	106	106	107

表格1中，列k为安全参数，N、p、q_1 和q_2如小节1.1.1中所述。多项式f、g 和r_1中的系数只属于集合$\{-1,0,1\}$。参数d表示多项式f、g 和r_1三者中任意一个多项式的系数中1的个数，参数d_f^n、d_g^n 和$d_{r_1}^n$则分别表示多项式f、g 和r_1的系数中-1的个数。

2 算法安全性评述

记一个多项式$h(x)$在$x=1$的取值为$h(1)$。

定理 1. 已知参数N、$p=3$、q_1、q_2、d、$d_{r_1}^n$、公钥h_1、h_2 和 密文c_1、c_2，存在复杂度为$O(N)$的多项式时间算法 以不低于$1-\dfrac{8N}{3q_1^2}$的概率计算获取明文的部分信息$M(1) \bmod q_2$.

证明： 根据关系式(1)先计算出

$$r_2(1) \equiv c(1) - h_1(1) \cdot r_1(1) \equiv c(1) - h_1(1) \cdot (d - d_{r_1}^n) \bmod q_1.$$

集合$\{-1,0,1\}$上的均匀分布，其期望值为0，方差为$2/3$。考察r_2的产生过程，其系数是由N个独立同分布的$\{-1,0,1\}$上的均匀分布的随机变量决定。因此，根据切比雪夫不等式，有

$$\Pr\left[|r_2(1)| < q_1/2\right] \geq 1 - \frac{N(2/3)}{(q_1/2)^2} = 1 - \frac{8N}{3q_1^2}.$$

即，以不低于$1-(8N)/(3q_1^2)$的概率，$r_2(1) = \langle r_2(1) \rangle_{q_1} = (r_2(1) \bmod q_1)$。

根据关系式(2)和上述获取的$r_2(1)$计算得到

$$M(1) \equiv c(2) - h_2(1) \cdot r_1(1) - r_2(1) \equiv c(1) - h_2(1) \cdot (d - d_{r_1}^n) - r_2(1) \bmod q_2.$$

容易看到，上述计算的复杂度为$O(N)$。 □

推论 1. 在现有参数下，D-NTRU算法不具备IND-CPA安全性。

证明： 根据表格1，现有参数下可计算定理1中的概率下界值

表格 2: D-NTRU算法中计算$\langle M(1) \rangle_{q_2}$ 的成功概率

N	q_1	$1-(8N)/(3q_1^2)$
157	269	0.994214
223	269	0.991782
349	521	0.996571

根据定理1，攻击者故意选择两个明文M_1和M_2使得$M_1(1) \not\equiv M_2(1) \pmod{q_2}$。经过加密Oracle随机挑选两者中的一个加密回答之后，攻击者就能以不低于99% 的概率回答出到底是哪一个明文被加密Oracle挑选加密的。 □

2.1 实验验证

根据 [2]提供的实例参数及代码，在此基础上增加函数INDCPAgame并跟踪数据r_1和r_2进行实验验证，可以看出上述推论1的攻击是可行和高效的。

3 建议

建议考察应用NTRU Prime及其变体的可行性。

参考文献

[1] 王保仓、雷浩、胡予濮、徐温菊、宋威、周立国：《D-NTRU 算法：IND-CPA 安全的高效公钥密码方案》。https://sfjs.cacrnet.org.cn/site/content/362.html, accessed on 12/9/2019

[2] D-NTRU 算法实现代码， https://sfjs.cacrnet.org.cn/site/content/362.html, accessed on 12/9/2019

附件

小节2.1的实验C++代码以电子文档形式随附。