NTRU Cryptosystems Technical Report

Report # 011, Version 2
Title: Wraps, Gaps, and Lattice Constants
Author: Joseph H. Silverman
Release Date: March 15, 2001

Abstract. This note describes how the choice of a parameter set $(N, p, q, d_f, d_g, d_\phi)$ for an NTRU Public Key Cryptosystem determine various operating characteristics of the cryptosystem, such as the security level and the probabilities of wrapping failure and of gap failure.

Contents

§1. Wrapping Failure and Gap Failure.

For any polynomial

$$a = a_0 + a_1X + a_2X^2 + \cdots + a_{N-1}X^{N-1},$$

write

$$\operatorname{Max} a = \max a_i, \qquad \operatorname{Min} a = \min a_i, \qquad \operatorname{Spread} a = \operatorname{Max} a - \operatorname{Min} a.$$

Consider an NTRU Public Key Cryptosystem using the parameters

$$(N, p, q, d_f, d_g, d_\phi),$$

and let

$$b = p\phi g + mf$$

be a typical polynomial that occurs during the decryption process. We say that *wrapping failure* occurs if either $\operatorname{Max} b \ge q/2$ or $\operatorname{Min} b \le q/2$. We say that *gap failure* occurs if $\operatorname{Spread} b \ge q$.

During the NTRU decryption process, Bob recovers the value of $b \bmod q$, but he needs to have its exact value to complete the decryption. If wrapping failure, but not gap failure, occurs, Bob can determine the correct value of b by computing successively

$$\big(b \bmod q + (k, k, \ldots, k)\big) \bmod q - (k, k, \ldots, k) \qquad \text{for } k = \pm 1, \pm 2, \ldots.$$

(Note that reduction modulo q always means to reduce into the interval between $-q/2$ and $q/2$.)

It is also possible to fix gap failure by moving individual coefficients of b mod q that are near to the edges of the interval $[-q/2, q/2]$, but this is a more time-consuming process, so it is worthwhile to make the probability of gap failure very small.

It is possible to estimate the probability of wrapping and gap failure experimentally by computing a large number of b polynomials. For wrapping failure, it is quite reasonable to perform such experiments; but gap failure occurs rarely enough that it is helpful to combine theory and experiment. The first step is to experimentally compute a sufficent number of b's to obtain estimates for the quantities

$$\text{Prob}(\text{Max}\, b = k) \qquad \text{and} \qquad \text{Prob}(\text{Min}\, b = k).$$

In order to estimate the probability of gap failure, there should be at least a few b's which have $\text{Max}\, b \geq q/2$ and at least a few b's which have $\text{Min}\, b \leq -q/2$. In other words, the data must be sufficient to give a reasonable estimate for the probability of various amounts of wrapping failure. Having accumulated this data, it is easy to estimate the probability of gap failure using the following formula:

$$\text{Prob}(\text{Spread}\, b \geq q) = \sum_j \text{Prob}(\text{Max}\, b \geq j)\, \text{Prob}(\text{Min}\, b = j - q). \tag{1}$$

Remark. If one performs T trials and finds no instances of wrapping failure, then one can estimate that

$$\text{Prob}(\text{wrapping failure}) \leq \frac{1}{T} \qquad \text{and} \qquad \text{Prob}(\text{gap failure}) \leq \frac{1}{T^2}.$$

The justification for the second estimate is that the most likely cause of gap failure will be when $\text{Max}\, b = q/2$ and $\text{Min}\, b = -q/2$, so one needs to have wrapping failure at both the top and the bottom. Since the values of the coefficients of b are essentially independent events, we obtain

$$\begin{aligned} \text{Prob}(\text{gap failure}) &\approx \text{Prob}(\text{Max}\, b = q/2) \cdot \text{Prob}(\text{Min}\, b = -q/2) \\ &\leq \text{Prob}(\text{wrapping failure})^2. \end{aligned}$$

Remark. In order to decrease the likelihood of wrapping failure and gap failure, one naturally wants to make the value of $\text{Spread}\, b$ as small as possible. However, it is important to note that one should not make $\text{Spread}\, b$ too small, or else there is a small possibility that an attacker could use a spurious decryption key (found, e.g., by lattice reduction) whose length is considerably longer than the true private decryption key. Experimentally, it appears to be difficult to find a spurious key which is less than 10 times as long as the true key, so one should be safe with parameters for which the vast majority of b's have Spreads which are greater than (say) $q/3$ or $q/4$.

§2. Lattice Constants.

Aside from various sorts of exhaustive searches whose time can be estimated, the principal attack on an NTRU cryptosystem is via lattice reduction. In this attack one sets up a lattice $L_{\rm key}$ (respectively $L_{\rm m}$) which contains a moderately small vector whose value will break the private key (respectively break the message). The security of the NTRU cryptosystem relies on the fact that it is very difficult to find moderately small vectors in lattices of high dimension. These lattice attacks are described in great detail in [1], so we will not repeat the description here.

The time needed for an exhaustive search for a private key (using a meet-in-the-middle approach [2]) is approximately the square root of the number of possible keys, and similarly for message searches. This gives the following formulas for the key security $S_{\rm key}$ and the message security $S_{\rm m}$ under meet-in-the-middle searches:

$$S_{\rm key} = \sqrt{\frac{N!}{(N-2d_g)!\cdot d_g!\cdot d_g!}} \qquad S_{\rm m} = \sqrt{\frac{N!}{(N-2d_\phi)!\cdot d_\phi!\cdot d_\phi!}}.$$

(It is assumed that $d_g \le d_f$, as will be the case in any reasonable set of NTRU parameters.)

The time to find the target vector in a lattice L using lattice reduction is determined experimentally, but there are several constants associated with the NTRU lattices whose value will help predict the lattice security level of a particular set of NTRU parameters. For an NTRU lattice L we let

$$\begin{aligned}\sigma(L) &= \text{Expected length of shortest non-zero vector in } L.\\ \tau(L) &= \text{Length of the target vector in } L.\end{aligned}$$

The important NTRU lattice constants are

$$\begin{aligned} c_{\rm key} &= \frac{\tau(L_{\rm key})}{\sigma(L_{\rm key})} = \sqrt{\frac{\pi e\sqrt{2d_g(2d_f-1)}}{Nq}}\\ c_{\rm m} &= \frac{\tau(L_{\rm m})}{\sigma(L_{\rm m})} = \sqrt{\frac{2\pi e\sqrt{2(1-1/p)Nd_\phi}}{Nq}}\\ c_q &= \frac{\sigma(L_{\rm key})}{q} = \sqrt{\frac{N}{\pi eq}\sqrt{\frac{2d_g}{2d_f-1}}} \end{aligned}$$

(We have assumed that $p = 2$ or 3. If $p > 3$, the formula for $c_{\rm m}$ must be modified.) It is clear why the first two NTRU lattice constants are important, since they measure the extent to which the target vector is small. The third NTRU lattice constant c_q is useful because the NTRU lattices have a large number of vectors of length q. In

practice, if c_q is not too small, then efficient lattice reduction algorithms such as LLL tend to have a difficult time finding vectors which have length smaller than q. Indeed, what generally happens is that the algorithm returns vectors of length q until, after a great deal of computation, the algorithm finally finds the target vector. More precisely, if c_q is not too small, then the amount of time to find any vector of length strictly smaller than q is approximately equal to the time it takes to find the actual target vector.

Remark. We will not give the complete derivation of the above formulas, but we note that if L is a lattice of dimension n and discriminant D, then the Gaussian heuristic predicts that the expected length of the shortest non-zero vector in L satisfies

$$D^{1/n}\sqrt{\frac{n}{2\pi e}} \le \sigma(L) \le D^{1/n}\sqrt{\frac{n}{\pi e}}.$$

The NTRU lattice L_{key} has dimension $n = 2N$ and discriminant $D = q^N\alpha^N$ for a certain lattice balancing constant $\alpha = \sqrt{2d_g/(2d_f - 1)}$, and similarly for L_{m}. For further details, see [1, §3.4].

§3. Parameter Choices.

Table 1 gives a selection of parameter choices for the NTRU Public Key Cryptosystem which provide a balance of security and decryption levels. This list is by no means exhaustive, and it would be easy to create many additional acceptable parameter sets. For ease of reference, we have labeled each set with the parameters N and p. In the case that $p = 2$, the values of $q = 127$ and $q = 253$ have been chosen so that numbers modulo q fit easily into 7 bits and 8 bits respectively.

	N	p	q	d_f	d_g	d_ϕ
NTRU107.3	107	3	64	15	12	5
NTRU167.3	167	3	128	61	20	18
NTRU263.3	263	3	128	50	24	16
NTRU503.3	503	3	256	216	72	55
NTRU167.2	167	2	127	45	35	18
NTRU263.2	263	2	127	35	35	22
NTRU503.2	503	2	253	155	100	65

Table 1. NTRU Parameter Sets

Table 2 gives security values and lattice constants for the parameter sets in Table 1. It also gives the probability of wrapping failure and the probability of gap failure based on the experiments described in the next section.

	S_{key}	S_{m}	c_{key}	c_{m}	c_q	P_{wrap}	P_{gap}
NTRU107.3	$2^{50.0}$	$2^{26.5}$	0.257	0.258	0.422	$7.0 \cdot 10^{-5}$	$2.4 \cdot 10^{-9}$
NTRU167.3	$2^{82.9}$	$2^{77.5}$	0.236	0.225	0.296	$5.5 \cdot 10^{-5}$	$2.1 \cdot 10^{-9}$
NTRU263.3	$2^{110.6}$	$2^{82.10}$	0.187	0.195	0.409	$1.5 \cdot 10^{-6}$	$5.0 \cdot 10^{-13}$
NTRU503.3	$2^{284.10}$	$2^{241.4}$	0.182	0.160	0.365	$4.8 \cdot 10^{-5}$	$3.8 \cdot 10^{-9}$
NTRU167.2	$2^{113.2}$	$2^{77.5}$	0.252	0.210	0.370	$< 10^{-6}$	$< 10^{-12}$
NTRU263.2	$2^{141.1}$	$2^{104.2}$	0.189	0.197	0.494	$< 4 \cdot 10^{-6}$	$< 2 \cdot 10^{-11}$
NTRU503.2	$2^{339.4}$	$2^{268.1}$	0.183	0.156	0.433		

Table 2. Security Constants, Lattice Constants and Wrap/Gap Probabilities

Remark. There is a temptation to take N to be divisible by a large power of 2, since this might allow the use of Fast Fourier Transforms to compute the convolution product. In particular, if one were to take N to be a power of 2 and q to be a prime satisfying $q \equiv 1 \pmod{N}$ or $q^2 \equiv 1 \pmod{N}$, then one might compute FFTs directly over the field with q or q^2 elements. However, if N is highly composite, then $X^N - 1$ will have many factors, so the convolution ring $\mathbf{F}_q[X]/(X^N - 1)$ will decompose via the Chinese Remainder Theorem. This suggests that highly composite values of N might lead to better attacks, via algebraic manipulations and/or improved lattice methods.

Gentry's Folding Method [3] takes advantage of highly composite values of N to construct lower dimensional lattices, which can be used to search for the private key and for plaintext messages. In particular, Gentry's method is quite effective in the case that N is a power of 2. For this reason, it is recommended that N always be chosen to be a prime, and in any case, it should always have a large prime factor.

§4. Wrap/Gap Experiments.

Experiments were performed using messages m consisting of an approximately equal number of 1's, -1's, and 0's. For each parameter set studied, Table 3 gives the number of samples computed, the largest observed spread, the number of samples that exhibited wrapping failure, the probability of wrapping failure, and the probability of gap failure. Note that this final quantity, the probability of gap failure, was computed from the data using formula (1) in Section 1, since the number of samples was too small to expect an instance of gap failure to occur.

	Samples	Spread	Wraps	P_{wrap}	P_{gap}
NTRU107.3	10^5	57	7	$7.0 \cdot 10^{-5}$	$2.4 \cdot 10^{-9}$
NTRU167.3	$2 \cdot 10^5$	111	11	$5.5 \cdot 10^{-5}$	$2.1 \cdot 10^{-9}$
NTRU263.3	$2 \cdot 10^6$	105	3	$1.5 \cdot 10^{-6}$	$5.0 \cdot 10^{-13}$
NTRU503.3	10^6	226	48	$4.8 \cdot 10^{-5}$	$3.8 \cdot 10^{-9}$
NTRU167.2	10^6	100	0	$< 10^{-6}$	$< 10^{-12}$
NTRU263.2	$3 \cdot 10^5$	86	0	$< 4 \cdot 10^{-6}$	$< 2 \cdot 10^{-11}$

Table 3. Wrap/Gap Experiments

References

[1] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: A new high speed public key cryptosystem, Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, Lecture Notes in Computer Science 1423, J.P. Buhler (ed.), Springer-Verlag, Berlin, 1998, 267–288

[2] Joseph H. Silverman, A Meet-In-The-Middle Attack on an NTRU Private Key, NTRU Cryptosystems Technical Report 004, July 15, 1997. ⟨`www.ntru.com`⟩

[3] C. Gentry, Key Recovery and Message Attacks on NTRU-Composite, Proc. EUROCRYPT 2001, Lecture Notes in Computer Science, Springer-Verlag,, 2001, to appear.

Comments and questions concerning this technical report should be addressed to

`techsupport@ntru.com`

Additional information concerning NTRU Cryptosystems and the NTRU Public Key Cryptosystem are available at

`www.ntru.com`
