An Improved MITM Attack Against NTRU

Zhijian Xiong[1], Jinshuang Wang[1], Yanbo Wang[2], Tao Zhang[1] and Liang Chen[2]

[1] *Institute of Command Automation, PLA University of Science and Technology, Nanjing 210007, China*
[2] *Institute of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China*
kuperain@sina.com

Abstract

Various attacks against NTRU have been proposed without ideal effects. To cut down the huge time complexity, this paper proposed a quantum mechanical meet-in-the-middle attack method against NTRU. Our method managed to combine the advantages of Meet-in-the-middle attack and the Grover quantum searching algorithm. Our evaluation reveals that the time complexity dropped dramatically comparing with classical meet-in-the-middle attacks, with the same space complexity. Our method also decreases time complexity comparing with Wang's attacking algorithm dramatically, with the cost of space complexity. Main variants of NTRU were also studied

Keywords: *NTRU, meet-in-the-middle attack, Grover search, quantum algorithm, quantum attack*

1. Introduction

Various attack schemes against NTRU [1, 2] have been proposed without ideal effects, such as meet-in-the-middle attack [3], lattice attack [1], broadcasting attack [4, 5] etc. The reason of failure lies in the huge time complexity and space complexity. For example, meet-in-the-middle attack can cut the search time by the usual square root, but still has huge space complexity.

In 1994, Shor [6] demonstrated efficient quantum algorithms for factoring and the computation of discrete logarithms. It has therefore clear that a quantum computer would render all widely used public key cryptography insecure.

Recently, quantum attacks on NTRU were also well studied. In 2003, Ludwig [7] applied Grover [8] quantum search algorithm on lattice based algorithms. It has been revealed by paper [7] that the running time of Quantum Search Reduction Algorithm (QRS) dropped dramatically compared with classical methods, but still had exponential time complexity. In 2005, Graham [9] pointed out that the computing complexity of QSR is larger than meet-in-the-middle attack. In 2009, NTRU was believed to be secure against quantum attacks [10]. In 2010, Wang [11] proposed a quantum algorithm for searching a target solution of fixed weight, and applied it to search for the NTRU private key. Wang's method needs small storage, but the computation complexity is still larger than the meet-in-the-middle attack.

We studied the advantages of meet-in-the-middle attacks and Wang's method, and proposed a quantum mechanical meet-in-the-middle attack against NTRU.

The rest of this paper is organized as follows: section 2 gives necessary background knowledge. Section 3 presents our quantum mechanical meet-in-the-middle attack against NTRU, and the computing complexity of this method was evaluated. Section 4 discusses our attack against main NTRU parameter schemes. Section 5 concludes.

2. Preliminaries

2.1. Meet-In-The-Middle Attack on NTRU Private Key

B is the set of Boolean polynomials of degree N. $B(d)$ is a subset of B, polynomial of which has d coefficients of 1, N-d coefficients of 0. $T(d_+, d_-)$ is the set of polynomials where the number of coefficient 1 is d_+, the number of coefficient -1 is d_-, and others are 0.The space of f, g, r, m is L_f, L_g, L_r, L_m respectively. (For further details, see [8])

To keep consistent with [9], we supposed that: (1) private key $f \in B(d)$; (2) N and d are even. The concrete procedures of meet-in-the-middle attack in [9] are:

(1) Empty the set of bins, and label the bins with 0, 1…, 2^k-1.

(2) Enumerate f_1: put each f_1 into a bin based on the most significant bit of the first k coefficients of $f_1*h(\text{mod } q)$, we label this bin with label_ f_1. Each bin is then referenced by $\{0,1\}^k$. The length of f_1 is $N/2$, but we identify it with the N-tuple vectors by appending $N/2$ zeros.

(3) Enumerate f_2: put f_2 to the proper bin as f_1, and label it as label_ f_2. The check for occupation not merely the bin given by the most significant bits of the first k coefficients of $-f_2*h(\text{mod } q)$, but also the bins given by the flips of all those most significant bits that would be changed by adding 1 to the corresponding coefficient of $-f_2*h(\text{mod } q)$.

(4) Search for matches: when f_2 hits an occupied bin, take f_1 from the bin. If $(f_1+f_2)*h(\text{mod } q) \in \{0,1\}^N$, return $f=f_1+f_2$, else check next bin or next f_2. The algorithm will halt when a result is returned.

It was revealed that this algorithm can always return a result, which is very likely to be the private key f, or a cyclic shift of f. The time complexity of meet-in-the-middle attack is $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$, and the space complexity is $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$.

2.3. Wang's Attack for NTRU

Many NTRU schemes have the property of $f=1+pF$ for the private key f, where $F \in B(d_F)$. WANG took the NTRU private key problem as a fixed weight target searching problem. Based on the Grover quantum search algorithm, WANG gave a quantum search algorithm for fixed weight target.

Definition 1 Assume v is an n-tuple vector of weight d. The positions of 1 in v are i_1, i_2…, i_d for $i_1 \le i_2 \le ... \le i_d \le n$. The label of v is defined as:

$$I_v = 1 + C_{i_1}^1 + C_{i_2}^2 + ... + C_{i_d}^d, \quad (1)$$

The label of target vector which needs to be searched was named as "target label".

The maximum value of I_v is C_{N+1}^d, which has 1-1 correspondence with Boolean vector. Wang's attack procedures are as follows:

(1) Compute the maximum value of labels $C_{N+1}^{d_F}$, let $t = \left\lceil \log_2^{C_{N+1}^{d_F}} \right\rceil$;

(2) Search the *t*-tuple vector using Grover quantum searching algorithm, derive the target label b_0;

(3)Derive target vector v_0 from target label b_0, return v_0 as F.

Since $C_{N+1}^{dF} \le C_{N+1}^{\lceil (N+1)/2 \rceil} < 2^N$, and $d_F << N$, the searching space of Wang's attack is smaller than 2^N.

3. A Quantum MITM Attack Against NTRU

Meet-in-the-middle attack is the most effective method against NTRU at present, though the time complexity is still very large. Wang's method can be seen as a quantum brute-force search, which reduced the time complexity from $O(C_N^{d_F})$ to $O(\sqrt{C_{N+1}^{d_F}})$ .It is attractive to combine the quantum computation with meet-in-the-middle attack. We managed to provide such a method.

3.1. Algorithm Describe

Without loss of generality, we assumed: (1) private key $f \in B(d)$; (2)N and d are even; (3)The bin which contains polynomial f_1 will be labeled as $lable\_f_1$, and $bin(f_1)=\{label\_f_1\}$; (4) $bin(f_2)=\{label\_f_2\}$;

The basic ideal of quantum meet-in-the-middle attack against NTRU is:

(1) Compute all $\{label\_ f_1, f_1\}$ and arranged as a table L indexed by $label\_ f_1$;

(2) Search f_2 with the Grover search algorithm, with $label\_f_1 \in bin(f_2)$, and $(f_1+f_2)*h(\mathrm{mod}\ q) \in \{0,1\}^N$;

(3) Search f_1 correspond to $label\_ f_1$ in L;

(4) Verifies f_1+f_2 with other conditions.

The detail of searching f_2 based on Grover algorithm is:

(1) Compute the maximum label value $C_{N/2+1}^{d_f/2}$, let $n = \left| \log_2^{C_{N+1}^{d_F}} \right|$.

(2) Initialize the quantum system with $|0\rangle^{\otimes n} \otimes |0\rangle$. Apply Hadamard transform $H^{\otimes n}$ to the first register to produce the equally-weighted superposition state $|s\rangle$.

$$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x=0}^{2^{n/2}-1} |x\rangle \tag{2}$$

(3)Oracle details: $F_{f_2} : B(d_f/2) \to \{0,1\}$, where:

$$F_{f_2} = \begin{cases} 1, \exists label\_ f_1 \in bin(f_2), (f_1 + f_2) * h(\mathrm{mod}\, q) \in \{0,1\}^N \\ 0, others \end{cases} . \tag{3}$$

(4) Apply Grover algorithm $\frac{\pi}{4} 2^{n/2}$ times. There are two operations performed in Grover iteration:

①Apply the Oracle;

② Apply the unitary operator $I_\phi = 2|\phi\rangle\langle\phi| - I$ on the superposition state $|s\rangle$, note $\phi = \frac{1}{2^{n/2}} \sum_{x=0}^{2^{n/2}-1} |x\rangle$.

(5) Measure the first register, and return f_2.

3.2. Algorithm Evaluation

Our attack can return the solution with high probability, and the probability can be increased with a big k value. Oracle is a simple judging function, therefore the time complexity of Grover quantum searching algorithm only depends on the iterative times. The time complexity of NTRU quantum meet-in-the-middle attack is $O(\sqrt{C_{N/2+1}^{d_f/2}})$.The table L needs to be saved, which is similar to meet-in-the-middle attack, so the space complexity is $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$. A detailed comparison was given in Table 1.

Table 1. Time and Space Complexity Comparison for Different NTRU Attacks

	Brute-force	MITM Attack	Wang's attack	Quantum MITM attack
Time complexity	$O(C_N^d)$	$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$	$O(\sqrt{C_{N+1}^{d_F}})$	$O(\sqrt{C_{N/2+1}^{d/2}})$
Space complexity	$O(1)$	$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$	$O(1)$	$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$

4. Attack Against Main NTRU Variants

In section 3, private key f was taken as Boolean vectors, N and d are even. In this section, we will discuss the quantum MITM attack under three main NTRU parameter schemes, as was shown in Table 2.

Table 2. Main NTRU Parameter Schemes

Variants	q	p	L_f	L_g	L_m	L_r	F	*Dec.Fail*	*Ref.*
NTRU-1998	$2^k \in [N/2,N]$	3	$T(d_f,d_f\text{-}1)$	$T(d_g,d_g)$	T	$T(d_r,d_r)$	-	*Yes*	[1]
NTRU-2001	$2^k \in [N/2,N]$	x+2	1+pF	$B(d_g)$	B	$B(d_r)$	$B(d_F)$	*Yes*	[12]
NTRU-2005	prime	2	1+pF	$B(d_g)$	B	$B(d_r)$	$B(d_F)$	*No*	[13]

4.1. NTRU-1998

In NTRU-1998, p=3, and the coefficients of private key is -1, 0 or 1. Under this scheme, the attack procedures are：(1)Splitting f as f_1 and f_2, where f_1 was derived by replacing all occurrences of -1 in f with 0, and f_2 by replacing all occurrences of 1 with 0, obviously $f=f_1+f_2$; (2)Apply the quantum MITM attack same as section 3. Under this scheme, the time complexity is $O(\sqrt{C_{N+1}^{d_f-1}})$, and space complexity is $O(\frac{C_N^{d_f}}{\sqrt{N}})$.

Wang's method only search target solutions in *B*, therefore it cannot be applied to NTRU-1998 directly. To tackle this problem, we extend Definition 1 as below:

Definition 2 Suppose the number of 1 and -1 in a *n*-tuple vector is fixed, represented as $d_{(+)}$ and $d_{(-)}$ respectively, and other coefficients are 0. The positions for coefficients 1 are i_1^+, $i_2^+,\ldots,i_{d(+)}^+$, and positions for coefficients -1 are i_1^-, $i_2^-,\ldots,i_{d(-)}^-$, where $1\le i_1^+\le i_2^+\le\ldots\le i_{d(+)}^+\le n$, $1\le i_1^-\le i_2^-\le\ldots\le i_{d(-)}^-\le n$. The label for vector *v* is defined as

$$I_v = (I_{v-} - 1)\cdot Max(I_{v+}) + I_{v+}\ , \tag{4}$$

where $I_{v+} = 1 + C_{i_1^+}^1 + C_{i_2^+}^2 + \ldots + C_{i_{d(+)}^+}^{d(+)}$, $I_{v-} = 1 + C_{i_1^-}^1 + C_{i_2^-}^2 + \ldots + C_{i_{d(-)}^-}^{d(-)}$.

Obviously, $Max(I_{v+}) = C_{N+1}^{d(+)}$, $Max(I_{v-}) = C_{N+1}^{d(-)}$, therefore $Max(I_v) = C_{N+1}^{d(+)}\cdot C_{N+1}^{d(-)}$, and $Max(f) = C_{N+1}^{d_f}\cdot C_{N+1}^{d_f-1}$ for NTRU-1998. Under this scheme, Wang's method has time complexity of $O(C_{N+1}^{d_f})$, and the space complexity is $O(1)$.

4.2. NTRU-2001

In NTRU-2001, $f=1+pF$, $p=x+2$, $F\in B(d_F)$. F can be split into F_1 and F_2 as section 3, and $F*x^i=F_1+F_2$.

$$(1+pF)*h \equiv g \pmod q \Leftrightarrow (1+pF)*x^i*h \equiv g*x^i \pmod q$$
$$\Leftrightarrow pF_1*h \equiv g*x^i - (x^i+pF_2)*h \pmod q \Rightarrow pF_1*h \equiv \{0,1\}^N - (x^i+pF_2)*h \pmod q$$

We compute the bin label for F_1 from left, and the bin labels for F_2 from right. Note a little difference from section 3 is that F_2 should be put into *N* bins at least, with no effect on the definition of Oracle. The time complexity for the quantum MITM attack against NTRU-2001 is $O(\sqrt{C_{N/2+1}^{d_F/2}})$, and the space complexity is $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$.

4.3. NTRU-2005

In NTRU-2005, $f=1+pF$, $p=2$, and $F\in B(d_F)$.We can apply the MITM attack on F same as NTRU-2001. Besides, private key f can be also attacked directly. In this scheme, private key f has two possible formats: 1) the constant is 1, the number of coefficients 2 is d_F, and others are 0. Polynomial f_1 and f_2 can be derived by cyclic shifting on f, each has half non-zero coefficients of f. Without loss of generality, we can put coefficient 1 or 3 into f_1. Then the MITM attack can be applied on f_1 and f_2, with time complexity $O(\sqrt{C_{N/2+1}^{d_F/2}})$, and space complexity $O(C_{N/2}^{d_F/2})$.

5. Conclusions

Quantum computation strongly influenced cryptography. Combining meet-in-the-middle attack and the Grover quantum searching algorithm, this paper proposed a quantum meet-in-the-middle attack method against NTRU. Our evaluation reveals that

our time complexity $O(\sqrt{C_{N/2+1}^{d/2}})$ dropped dramatically comparing with classical meet-in-the-middle attacks' $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$, with the same space complexity. Our method also improves time complexity comparing with Wang's attacking algorithm dramatically, with the cost of space complexity.

Acknowledgements

This paper is supported by the National Natural Science foundation of China (Grant No.61072042/F010102) and PLAUST research foundation (20110509).

References

[1] J. Hoffstein, J. Pipher and J. Silverman, "NTRU: A ring-based public key cryptosysytem", ANTS III, 1423: 267-288, **(1998)**.

[2] IEEE Computer Society, IEEE Standard Specification for Public Key Cryptographic Tehniques Based on Hard Problems over Lattice, **(2009)**.

[3] J. Silverman and A. Odlyzko, NTRU Report 004, Version 2, A Meet-The Middle Attack on an NTRU Private Key, Technical Report, NTRU Cryptosysytems, **(2003)**.

[4] Y. Pan and Y. Deng, "A Broadcast Attack against NTRU Using Ding's Algorithm", eprint.iacr.org, **(2011)**.

[5] J. Li, M. Liu and G. Zhu, "An Efficient Broadcast Attack against NTRU", eprint.iacr.org, **(2011)**.

[6] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM review, 41(2): 303-332, **(1999)**.

[7] C. Ludwig, "A faster lattice reduction method using quantum search", Algor Comput, 2906: 199-208, **(2003)**.

[8] L. K. Grover, "A fast quantum mechanics algorithm for database search", Proceeding of the 28th ACM Symposium on Theory of Computation, New York: ACM Press, 212-219, **(1996)**.

[9] H. G. Nick, "A hybrid lattice-reduction and meet-in-the-middle attack against NTRU", Proceeding of CRYPTO'07, Springer-Verlag, **(2007)**.

[10] R. A. Perlner and D. A. Cooper, "Quantum Resistant Public Key Cryptography: A Survey", ACM Press, **(2009)**.

[11] X. Wang, W. S. Bao and X. Q. Fu, "A quantum algorithm for searching a target solution of fixed weight", Chinese Sci Bull, 55(29) , **(2010)**.

[12] Consortium for Efficient Embedded Security, Efficient embedded security standards#1: Implementation aspects of NTRUEncrypt and NTRUSign, **(2002)**.

[13] H. G. Nick, H. S. Joseph and W. William, "Choosing Patameter Sets for NTRUEncrypt with NAEP and SEVS-3", Technical Report, NTRU Cryptosysytems, **(2005)**.