SCIENCE CHINA
Information Sciences

• **Supplementary File** •

A Lower Dimension Lattice Attack on NTRU

Zhichao YANG[1], Shaojing FU[1,2*], Longjiang QU[2,3] & Chao LI[1,3]

[1]*College of Computer, National University of Defense Technology, Changsha* 410073*, China;*
[2]*State Key Laboratory of Cryptology, Beijing* 100878*, China;*
[3]*College of Science, National University of Defense Technology, Changsha* 410073*, China*

Appendix A Determinant Analysis

In order to estimate the length of the shortest vector in $\mathcal{L}_I$, the determinant of $\mathcal{L}_I$ has to be calculated in advance. This subsection will analyse the determinant of the *IN-Lattice* in different cases and give a general lattice determinant formula.

Definition 1. Let $\mathcal{L}$ be a lattice in $\mathbb{Z}^N$. The dual lattice of $\mathcal{L}$ is

$$\mathcal{L}^* = \{x \in \mathbb{R}^N : \forall y \in \mathcal{L}, x \cdot y \in \mathbb{Z}\}.$$

Lemma 1. [20, p10]Let $\mathcal{L}$ be a lattice, and $\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots, \boldsymbol{f}_r$ be a finite set of vectors in $\mathcal{L}$. Let m_i be integers, and let $\mathcal{M} \subset \mathcal{L}$ be the intersection of the kernels of the homomorphisms $\boldsymbol{x} \to \boldsymbol{f}_i \cdot \boldsymbol{x} \mod m_i$(thus $\mathcal{M}$ is a sublattice of $\mathcal{L}$). Then $\mathcal{M}^*$ is the lattice generated in $\mathbb{R}^N$ by $\mathcal{L}^*$ and the vectors $\frac{1}{m_i}\boldsymbol{f}_i$.

In fact, the determinant of a lattice $\mathcal{L}$ and its dual lattice $\mathcal{L}^*$ are mutually inverse. Lemma 1 suggests that the determinant of a lattice can be calculated through its dual lattice, especially when the structure of the original lattice is complex. With those notion, we can decide the determinant of $\mathcal{L}_I$ by the following proposition.

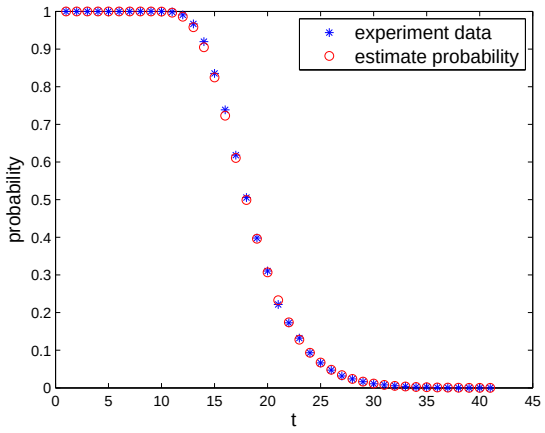

Figure A1 Probability with Different t ($N = 107$)

Proposition 1. [21]Let I be a subset of $[N]$, and $\mathcal{L}_I$ be the *IN-Lattice* obtained from Definition 4. Then, its dual lattice $\mathcal{L}_I^*$ is generated by vectors $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_N$ and vectors $\frac{1}{q}\boldsymbol{h}_i\,(i \in I)$, where $\{\boldsymbol{e}_i\}_{i=1}^N$ is a basis of $\mathbb{Z}^N$ and $\boldsymbol{h}_i$ is given in Eq. (2).

Let M be the matrix whose row vectors are $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_N$ and $\frac{1}{q}\boldsymbol{h}_i\,(i \in I)$. Thus, $\mathcal{L}_I^*$ is the lattice of degree N generated by row vectors of M. Through the definition of determinant, we have $\det\left(\mathcal{L}_I^*\right) = \sqrt{\det\left(\mathrm{Gram}(M)\right)}$ where $\mathrm{Gram}\,(M)$ is the Gram matrix of M. Since the determinant of $\mathcal{L}_I$ and its dual lattice $\mathcal{L}_I^*$ are mutually inverse, $\det\left(\mathcal{L}_I\right)$ can be calculated by

$$\det\left(\mathcal{L}_I\right) = \frac{1}{\det\left(\mathcal{L}_I^*\right)} = \frac{1}{\sqrt{\det\left(\mathrm{Gram}(M)\right)}}.$$

* Corresponding author (email: shaojing1984@163.com)

Appendix B Experiments

In this section we first figured out the relation between t and Prob $\left(\boldsymbol{f}^{ls(k)} \in \mathcal{L}_I\right)$, where $t = \#I$, and then the new attack was fully implemented on different scale to confirm its feasibility. Since the parament t is a key point in *IN-Lattice* attack, a principle was given to determine it in advance. Finally, target root Hermite factor and runtime in different attack are presented which verify the efficiency of our new attack.

Appendix B.1 Experiments on Different Scale

To test Eq. (3), we conducted one million experiments to simulate the probability Prob $\left(\boldsymbol{f}^{ls(k)} \in \mathcal{L}_I\right)$ with different t when $N = 107$. Those results are illustrated in Figure B1 together with the data calculated from Eq. (3).

Figure B1 shows that Eq. (3) predicts the probability very well. The vector $\boldsymbol{f}^{ls(k)}$ will belong to $\mathcal{L}_I$ with very high probability when t is small, and as t increases, the probability drops dramatically.

To determine the practicality of our new lattice attack, we implied Algorithm 1 into NTRU cryptosystem with different security levels. The parameters sets in different scales are listed in Table B1.

Table B1 The Parameters Used in Our Experiments.

N	d_f	d_g	d_r	q
19	3	2	1	16
37	6	4	2	16
57	8	6	2	32
73	8	6	2	32
83	10	8	3	32
97	11	9	3	64
107	15	14	5	64

In our experiments, the value of t was recorded when **a valid private key $\boldsymbol{f}'$ was found**, and the probability Prob $\left(\boldsymbol{f}^{ls(k)} \in \mathcal{L}_I\right)$ were calculated through Eq. (3). Those results are listed in Table B2.

Table B2 The Results of New Attack in Different NTRU Security Levels.

N	19	37	57	73	83	97	107
t	3	7	11	12	14	13	16
Prob	1	0.999	0.975	0.999	0.967	0.998	0.723

In fact, Algorithm 1 outputted a short vector which can be used to decrypt if and only if it is a shift of the private key. In Table B1, the parameter t is small enough when the new attack succeed, it means that a target vector $\boldsymbol{f}^{ls(k)}$ will belong to $\mathcal{L}_I$ with high probability. Thus our new attack is feasible.

Appendix B.2 Experiments Analysis

An implementation of a lattice reduction algorithm will have the best chance of locating $\boldsymbol{f}^{ls(k)}$, or another vector whose length is closed to $\boldsymbol{f}^{ls(k)}$, when the ratio γ is sufficiently small [3].

$$\gamma = ||\boldsymbol{f}^{ls(k)}||/\sigma\left(\mathcal{L}_I\right),$$

where $\sigma\left(\mathcal{L}_I\right)$ is the expected smallest length in $\mathcal{L}_I$ given by Gaussian heuristic. In fact, the value of γ only relies on t, since $||\boldsymbol{f}^{ls(k)}||$ is fixed. Figure B2 presents the ratio in different cases when t takes the value in Table B2.

It seems that a target vector can most likely be found by the *IN-Lattice* attack when $\gamma \approx 1.1$. So t can be determined in advance such that γ approximates to 1.1.

On the other hand, the runtime of the lattice reduction algorithm is also exponential with blocksize β. In order to obtain a more reduced basis, one needs more powerful reduction algorithm. Hence, we considered the target root Hermite factor δ_{tar} that one has to reach to find a target vector $\boldsymbol{v}_{tar}$ in different attacks. Here

$$\delta_{tar} = \left(||\boldsymbol{v}_{tar}||/\det\left(\mathcal{L}\right)^{1/\dim(\mathcal{L})}\right)^{1/\dim(\mathcal{L})}.$$

With the value of t given in Table B1, we calculated the target root Hermite factor in *CS* attack, *Zero-Force* attack and the *IN-Lattice* attack. Specifically, in *Zero-Force* attack, we let the number of columns that multiply a large constant equal to t. Thus in both the *Zero-Force* and the *IN-Lattice* attacks the target vectors will belong to lattice with the same probability. As for *CS* attack the target vectors are always belonging to *NTRU* lattice.

As we can see in Table B3, among three attacks, the root Hermite factor in our new attack is the largest, which means that the *IN-Lattice* attack is the most efficient and requires less on the strength of lattice reduction algorithm. Moreover, the dimension of the lattice in *Zero-Force* attack is $2N - t$, and t is roughly $[N/5]$ according to Table 2 in [6]. Since the dimension of the *IN-Lattice* is always N, our method has much low time complexity comparing with other two attack.

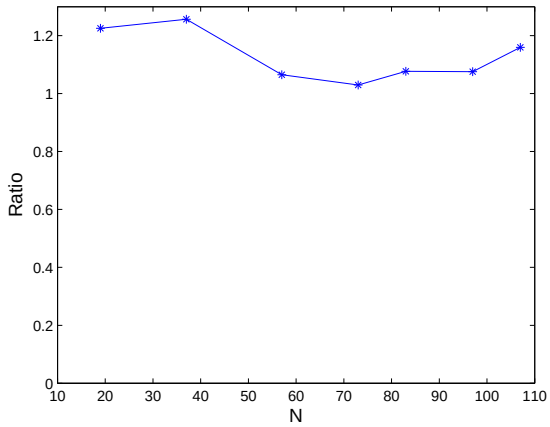

Figure B1 Ratio in *IN-Lattice* Attack

Table B3 Target Root Hermite Factor in Different Attacks

N	19	37	57	73	83	97	107
Prob $\left(\boldsymbol{f}^{ls(k)} \in \mathcal{L}\right)$	1	0.999	0.975	0.999	0.967	0.998	0.723
IN-Lattice Attack	1.0436	1.0227	1.0148	1.0116	1.0102	1.0087	1.0079
Zero-Force Attack	1.0258	1.0134	1.0087	1.0067	1.0059	1.0049	1.0045
CS Attack	1.0215	1.0110	1.0071	1.0055	1.0049	1.0042	1.0038

Appendix B.3 Runtime of the *IN-Lattice* Attack

As described in Algorithm 1, we can recovered the private key f as long as the lattice reduction algorithm outputted a target vector $\boldsymbol{f}^{ls(k)}$. Then we made experiments to estimate the breaking time in larger scale.

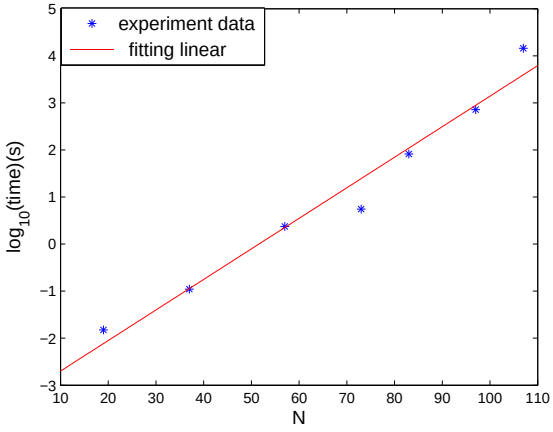

Figure B2 Runtime of *IN-Lattice* Attack

Extensive experimental evidence [3] suggests that the logarithm of the time needed to find a target vector grows (at least) linearly in the dimension. In other words, for families of NTRU-type lattice we have

$$\log_{10}(T) \geqslant A \cdot N + B,$$

for certain constants A and B. Specific example is given in [5], that is, $\log_{10}(T) \geqslant 0.1339N - 2.9983$ for lattice of type NTRU-107(Time in that formula is MIPS-years).

To determine the practicality of our new attack, we used the BKZ-NTL algorithm [22] of NTL package [18] to reduce those lattices and recorded the runtime only when we found a target vector $\boldsymbol{f}^{ls(k)}$ successfully. Figure B3 gives the results of the experiments. Times in this figure are given in seconds. Since those experiments were run on 3.2 GHz Core machines, the time in seconds is converted to the time in MIPS-years by first multipying by $3.2 \cdot 1024$(to account for the 3.2GHz

machines) and then dividing by 31557600 which is the number of seconds in a year. In this case, the extrapolation line for *IN-Lattice* attack is

$$\log_{10}(T) \approx 0.065N - 7.3.$$

It is obvious that the coefficient A in *IN-Lattice* attack is much smaller than that in [5]. Moreover, we broken the NTRU cryptosystem when $N = 107$ within two hours. Though it is similar to the results presented in [19], the lattice reduction algorithm used in [19] is BKZ2.0 which is much more powerful than BKZ-NTL. In Table B4, we gave the expected time(MIPS-years) to break NTRU cryptosystem in different attacks. Those data verified the efficiency of our new attack.

Table B4 Breaking Time in Different Attacks.

	New Attack	Zero-Force Attack [5]	CS Attack [5]
NTRU-167	$10^{3.55}$	$9.63 \cdot 10^4$	$10^{19.4}$
NTRU-263	$10^{9.80}$	$3.3 \cdot 10^{12}$	$10^{32.2}$
NTRU-503	$10^{25.4}$	$1.43 \cdot 10^{34}$	$10^{64.4}$

References

1 Hoffstein J, Pipher J, and Silverman J H. NTRU: A ring-based public key cryptosystem. In International Algorithmic Number Theory Symposium, pages 267-288. Springer, 1998.
2 Hoffstein J, Pipher J, Silverman J. NTRU: A ring-based public key cryptosystem. Algorithmic number theory. 1998, 1423: 267-288
3 Silverman J H and Whyte W. Estimating decryption failure probabilities for NTRUEncrypt. https://assets.onboardsecurity.com/static/downloads/NTRU/resources/NTRUTech018.pdf. 2003.
4 May A. Cryptanalysis of NTRU. preprint, February, 1999. https://pdfs.semanticscholar.org/d9af/ae316fc92954f2c23bf85bc15b3c328ed2c8.pdf.
5 Silverman J H. Dimension-reduced lattices, zero-forced lattices, and the NTRU public key cryptosystem. https://assets.securityinnovation.com/static/downloads/NTRU/resources/NTRUTech013.pdf. 1999.
6 May A and Silverman J H. Dimension reduction methods for convolution modular lattices. In Cryptography and Lattices. 2001, 2146: 110-125
7 Howgrave-Graham N, Silverman J H, and Whyte W. A Meet-in-the-Middle Attack on an NTRU Private key. https://assets.onboardsecurity.com/static/downloads/NTRU/resources/NTRUTech004v2.pdf. 2003.
8 Howgrave-Graham N. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. CRYPTO. 2007, 4622: 150-169
9 Albrecht M, Bai S, and Ducas L. A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes. CRYPTO. 2016, 9814: 153-178
10 Cheon J H, Jeong J, and Lee C. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero. Lms Journal of Computation & Mathematics, 2016, 19(A): 255-266
11 Kirchner P, Fouque P A. Revisiting lattice attacks on overstretched ntru parameters. EUROCRYPT. 2017, 10210: 3-26
12 Bi J and Cheng Q. Lower bounds of shortest vector lengths in random NTRU lattices. TAMC. 2012, 7287: 143-155
13 Rosenberg D. NTRUEncrypt and Lattice Attacks. PhD thesis, Royal Institute of Technology, 2010.
14 Hoffstein J and Silverman J. Optimizations for NTRU. In Proceedings of Public-Key Cryptography and Computational Number Theory. de Gruyter, Warsaw, September 2000.
15 Howgrave-Graham N, Silverman J H, and Whyte W. Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3. In: Menezes A. (eds) Topics in Cryptology C CT-RSA 2005. 2005, 3376: 118-135
16 Han D. A new lattice attack on NTRU cryptosystem. Trends Math. 2005, 8(1): 197-205
17 Gama N, Howgrave-Graham N, and Nguyen P Q. Symplectic lattice reduction and NTRU. EUROCRYPT. 2006, 4004: 233-253
18 Shoup V et al. NTL: A library for doing number theory, 2001.
19 Chen Y and Nguyen P Q. BKZ 2.0: Better lattice security estimates. ASIACRYPT. 2011, 7073: 1-20
20 Martinet J. Perfect Lattices in Euclidean Spaces. Springer Berlin Heidelberg, 2003
21 Gentry C, Peikert C, Vaikuntanathan V. How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions. https://eprint.iacr.org/2007/432.pdf. 2008
22 Schnorr C-P. A hierarchy of polynomial time lattice basis reduction algorithms. Theoretical computer science. 1987, 53(2): 201C224
23 Chen Y M. Réduction de réseau et sécurité concrete du chiffrement completement homomorphe. PhD thesis, ENSLyon, France, 2013