SCIENCE CHINA
Information Sciences

• LETTER •

May 2018, Vol. 61 059101:1–059101:3
doi: 10.1007/s11432-017-9175-y

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*

Received 12 January 2017/Revised 11 April 2017/Accepted 21 June 2017/Published online October 30, 2017

Citation Yang Z C, Fu S J, Qu L J, et al. A lower dimension lattice attack on NTRU. Sci China Inf Sci, 2018, 61(5): 059101, doi: 10.1007/s11432-017-9175-y

Dear editor,

Because of reasonably short length, easily created keys, high speed, low memory requirements and potential resistance to quantum attack, NTRU becomes one of the most popular public-key encryption systems and has drawn considerable attention. Motivated by [1–9], we devote to constructing a class of lower dimension lattices, called the *IN-Lattice*, and proposing a new lattice attack on NTRU cryptosystem.

Notions and NTRU problem. Let $\mathbb{Z}$ be the integer ring and $\mathbb{Z}_q$ be the residue class ring $\mathbb{Z}/q\mathbb{Z}$. We use bold letters to denote vectors in row notation. If $\boldsymbol{v}$ is a vector, then the i-th entry of $\boldsymbol{v}$ is denoted by v_i and the length of $\boldsymbol{v}$ is the standard Euclidean norm.

Definition 1 (Lattice)**.** Given n linearly independent vectors $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n \in \boldsymbol{R}^m$, the lattice $\mathcal{L}$ generated by them is defined as

$$\mathcal{L}(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) = \left\{ \sum_{i=1}^{n} x_i \boldsymbol{b}_i | x_i \in \mathbb{Z} \right\}.$$

The rank of the lattice is n and its dimension is m. $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ is a basis of the lattice.

For natural numbers i and j with $i < j$, $[i : j]$ is the set of integers $\{i, i+1, \ldots, j\}$. Particularly, $[1 : j]$ is denoted by $[j]$. $\lceil r \rceil$ represents the ceil of a ration number r. The NTRU problem can be described as follows.

Definition 2 (NTRU problem [6])**.** The NTRU problem is defined by four parameters: a ring $\mathbb{R}$ (of rank N and endowed with an inner product), a modulus q, a distribution D, and a target norm τ. Precisely, NTRU$(\mathbb{R}, q, D, \tau)$ is the problem of, given $h = [gf^{-1}]_q$ (conditioned on f being invertible mod q) for $f, g \leftarrow D$, finding a vector $(x, y) \in \mathbb{R}^2$ such that $(x, y) \neq (0, 0) \bmod q$ and of Euclidean norm less than $\tau\sqrt{2N}$ in the lattice

$$\mathcal{L}^{\text{ntru}} = \{(x, y) \text{ s.t. } hx - y = 0 \mod q\}. \quad (1)$$

In this letter, the distribution D is uniform distribution in set $\mathscr{L}(d_1, d_2)$ which contains all polynomials with d_1 coefficients equal to 1, d_2 coefficients equal to -1, and the rest 0. Our target is to find valid private keys in certain lattices.

Definition 3 (RHF)**.** The root Hermite factor of a basis $\boldsymbol{B}$ is defined as

$$\delta(\boldsymbol{B}) = \left(||\boldsymbol{b}_1|| / \det(\mathcal{L}(\boldsymbol{B}))^{1/\dim(\mathcal{L})} \right)^{1/\dim(\mathcal{L})},$$

where $\boldsymbol{b}_1$ is the shortest vector in $\boldsymbol{B}$.

It is well-known that BKZ reduction with bigger blocksize outputs more reduced basis with smaller RHF. $\times$ denotes the multiplication in $\mathbb{R}$, then $f \times g$ can be represented by

$$\left(f_0, f_1, \ldots, f_{N-1}\right) \begin{pmatrix} h_0 & h_1 & \cdots & h_{N-1} \\ h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 \end{pmatrix} = \boldsymbol{f}\boldsymbol{H}.$$

* Corresponding author (email: shaojing1984@163.com)
The authors declare that they have no conflict of interest.

We rewrite the circular matrix of h as follows:

$$\boldsymbol{H} = \left(\boldsymbol{h}_0^{\mathrm{T}}, \boldsymbol{h}_1^{\mathrm{T}}, \ldots, \boldsymbol{h}_{N-1}^{\mathrm{T}}\right), \tag{2}$$

where $\boldsymbol{h}_i^{\mathrm{T}}$ $(0 \leqslant i \leqslant N-1)$ is the i-th column vector in $\boldsymbol{H}$.

Let $\boldsymbol{v} = (v_0, v_1, \ldots, v_{N-1}) \in \mathbb{Z}^N$. Then we define $\boldsymbol{v}^{ls(l)} = (v_l, v_{l+1}, \ldots, v_{l-1})$ as cycle leftshift of $\boldsymbol{v}$ by l positions.

New lattice attack. With those notions above, we can define a new class of lattice.

Definition 4 (The *IN-Lattice*)**.** Guessing a subset I of $[N]$ such that g_{i+k} is 0 for all $i \in I$, where k is a constant integer belonging to $[N]$. Let $t = \#I$. An *IN-Lattice* $\mathcal{L}_I$ with size t is defined by

$$\mathcal{L}_I = \{\boldsymbol{x} \in \mathbb{Z}^N : \forall i \in I,\ \boldsymbol{x} \cdot \boldsymbol{h_i} \equiv 0 \mod q\}.$$

Remark 1. The definition of the *IN-Lattice* does not depend on the assumption that $\boldsymbol{H}$ is a circular matrix. Thus, our attack can still work when $\boldsymbol{H}$ is not a circular matrix. Moreover, it should be noted that the *IN-Lattice* cannot be obtained by simply deleting some columns in *NTRU-Lattice*.

Since the runtime of the lattice reduction algorithm is exponential with the lattice dimension, as for *IN-Lattice*, $\dim(\mathcal{L}_I) = N$ is relative small, $\mathcal{L}_I$ can be reduced more efficiently. One new lattice attack against NTRU is introduced in Algorithm 1.

Algorithm 1 *IN-Lattice* attack

Require: Fixed N, q, d_g, h and the probability $\mathrm{Prob}(\boldsymbol{f}^{ls(k)} \in \mathcal{L}_I)$;
Ensure: A valid private key $\boldsymbol{f}'$;
$t \leftarrow 2$;
while $t < N$ **do**
  count $\leftarrow 1$;
  while count $<= \lceil 1/\mathrm{Prob}(\boldsymbol{f}^{ls(k)} \in \mathcal{L}_I) \rceil$ **do**
    Randomly choose a subset I of $[N]$ such that $\#I = t$;
    Construct an *IN-Lattice* $\mathcal{L}_I$ with size t;
    Reduce $\mathcal{L}_I$;
    if the reduced basis contains a vector $\boldsymbol{v}$ which can be used to decrypt **then**
      $\boldsymbol{f}' = \boldsymbol{v}$;
      Output $\boldsymbol{f}'$, t and break;
    end if
    count = count + 1;
  end while
  $t \leftarrow t + 1$;
end while

Heuristic claim. There exists an integer $k \in [N]$ such that the vector $\boldsymbol{f}^{ls(k)}$ belongs to $\mathcal{L}_I$ if and only if $\bigcap_{i \in I} K_i \neq \emptyset$ and $k \in \bigcap_{i \in I} K_i$, where $K_i = \{l \in [N] : g_{i+l} = 0\}$. The probability $\mathrm{Prob}(\boldsymbol{f}^{ls(k)} \in \mathcal{L}_I)$ can be estimated by the following formula:

$$1 - \left(1 - \prod_{i=0}^{2d_g - 1} \left(1 - \frac{t}{N-i}\right)\right)^N, \tag{3}$$

where $2d_g$ is the Hamming wight of g and $t = \#I$.

The Gaussian heuristic predicts that the shortest vectors of $\mathcal{L}_I$ have norm $\sigma(\mathcal{L}_I)$ which is

$$\frac{(\Gamma(1 + \dim(\mathcal{L}_I)/2) \det(\mathcal{L}_I))^{1/\dim(\mathcal{L}_I)}}{\sqrt{\pi}}. \tag{4}$$

Since the dimension of $\mathcal{L}_I$ is fixed, the value of $\sigma(\mathcal{L}_I)$ only relies on $\det(\mathcal{L}_I)$.

In fact, $\det(\mathcal{L}_I)$ will equal to q^t with overwhelming probability when $\mathcal{L}_I$ is an *IN-Lattice* with size t. Eq. (4) can be rewritten as

$$\sigma(\mathcal{L}_I) \approx \frac{(\Gamma(1 + N/2)\, q^t)^{1/N}}{\sqrt{\pi}}, \tag{5}$$

for $\dim(\mathcal{L}_I)$ is always N. More details about calculating $\det(\mathcal{L}_I)$ are given in Appendix A.

Obviously, $\sigma(\mathcal{L}_I)$ only relates to t, since $||\boldsymbol{f}^{ls(k)}||$ is a fixed value, $\boldsymbol{f}^{ls(k)}$ will be the shortest vector in $\mathcal{L}_I$ with high probability when t is sufficient large. However, Eq. (3) indicates that $\boldsymbol{f}^{ls(k)}$ will less probably belong to $\mathcal{L}_I$ when t is large. Thus, choosing a suitable t is the key point in finding $\boldsymbol{f}^{ls(k)}$ in $\mathcal{L}_I$.

Experiments and analysis. To determine the practicality of our new lattice attack, we implemented Algorithm 1 on 3.2 GHz core machines. Related parameters are listed in Appendix B. The probability $\mathrm{Prob}(\boldsymbol{f}^{ls(k)} \in \mathcal{L}_I)$ was calculated through (3).

Moreover, we considered target RHF δ_{tar} that one has to reach to find a target vector $\boldsymbol{v}_{\mathrm{tar}}$ in different attacks. Here

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

With the value of t, we calculated the target RHF in the *IN-Lattice* attack, *Zero-Force* attack and *CS* 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*.

In our experiments, a short vector in the reduced lattice can be used to decrypt if and only if it is a shift of the private key. But the probability of success is difficult to determine, because it depends on not only the set I and its size t but also relates

Table 1 The results of expermients and target RHF

N	19	37	57	73	83	97	107
t	3	7	11	12	14	13	16
Prob($\boldsymbol{f}^{ls(k)} \in \mathcal{L}$)	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

to the BKZ algorithm, their relationship are still confusing. All the results are listed in Table 1, which indicates that $\lceil 1/\text{Prob}(\boldsymbol{f}^{ls(k)} \in \mathcal{L}_I)\rceil = 2$ is enough in these experiments. Among three attacks, the target RHF 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.

From [3], 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.

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

Those experiments also indicated 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.

Runtime of IN-Lattice attack. Extensive experimental evidence in [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

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

for certain constants A and B. Specific example is given in [4], that is, $A = 0.1339, B = 2.9983$ for lattice of type NTRU-107 (time in that formula is MIPS-years).

Then, we used the BKZ-NTL [5] algorithm of NTL package to reduce those lattices and recorded the runtime. In this case, the extrapolation line for *IN-Lattice* attack is

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

It is obvious that the coefficient A in *IN-Lattice* attack is much smaller than that in [4]. Moreover, we broken the NTRU cryptosystem when $N = 107$ within two hours. Though it is similar to the results presented in [4], the lattice reduction algorithm used in [6] is BKZ 2.0 which is much more powerful than BKZ-NTL. Complete experiment results are presented in Appendix B.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 11531002, 61572026) and Open Foundation of State Key Laboratory of Cryptology.

Supporting information Appendixes A and B. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Hoffstein J, Pipher J, Silverman J H. NTRU: a ring-based public key cryptosystem. Algorithmic Number Theory, 1998, 1423: 267–288
2 Coppersmith D, Shamir A. Lattice attacks on NTRU. In: Proceedings of the 16th Annual International Conference on Theory and Application of Cryptographic Techniques, Konstanz, 1997. 52–61
3 Silverman J H, Whyte W. Estimating decryption failure probabilities for NTRUEncrypt. 2003. https://assets.onboardsecurity.com/static/downloads/NTRU/resources/NTRUTech018.pdf
4 Silverman J H. Dimension-reduced lattices, zero-forced lattices, and the NTRU public key cryptosystem. 1999. https://assets.securityinnovation.com/static/downloads/NTRU/resources/NTRUTech013.pdf
5 Shoup V. NTL: A Library for Doing Number Theory Version 5.5.2, 2010. http://shoup.net/ntl/
6 Chen Y M, Nguyen P Q. BKZ 2.0: better lattice security estimates. In: Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, 2011. 1–20
7 Albrecht M, Bai S, Ducas L. A subfield lattice attack on overstretched NTRU assumptions: cryptanalysis of some FHE and graded encoding schemes. In: Proceedings of the 36th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 2016. 153–178
8 Cheon J H, Jeong J, Lee C. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero. Lms J Comput Math, 2016, 19: 255–266
9 Kirchner P, Fouque P A. Revisiting lattice attacks on overstretched NTRU parameters. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2017. 3–26