SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

NTRU 格子の拡張と格子攻撃
An extension of NTRU lattices and its lattice attack

中邑　聡史 *　　安田 雅哉 †
Satoshi Nakamura　　Masaya Yasuda

キーワード NTRU 格子，ベクトル回転操作，格子基底簡約，BKZ 簡約アルゴリズム

あらまし

米国標準技術研究所 NIST による耐量子計算機暗号の標準化プロジェクトにおいて，Module-LWE や NTRU の代数構造を持つ格子暗号方式が注目されている．Ring-LWE や Module-LWE などの環構造を持つ（探索）LWE 問題に対する有力な攻撃法は，環構造を持たない LWE 問題と同じで，Kannan や Bai-Galbraith の埋め込み法によりある格子上の最短ベクトル問題に帰着し，LLL や BKZ などの格子基底簡約アルゴリズムで埋め込まれた秘密情報を復元することである．近年，環構造を持つ LWE 格子上の回転操作を利用した埋め込み法の拡張が提案され，その拡張により環構造を持つ LWE 問題に対する攻撃成功確率が上がることが実験的に示された [1].

本稿では NTRU 問題に対する格子攻撃の拡張を提案する．具体的には，環 $R = \mathbb{Z}[x]/(x^N - 1)$ と奇素数 q に関する NTRU 問題の公開多項式 $h(x) \in R_q$ の係数ベクトル $\mathbf{h} = (h_0, h_1, \ldots, h_{N-1})$ の回転ベクトルを $\mathrm{rot}(\mathbf{h}) = (h_{N-1}, h_0, h_1, \ldots, h_{N-2})$ とする．通常の NTRU 格子で用いる $N \times N$ 行列 $\mathbf{H} = (\mathrm{rot}^{i-1}(\mathbf{h}))_{i=1}^{N}$ に加え，拡張パラメータ k に対し $2N+i$ 行目 $(i = 1, 2, \ldots, k)$ に $\mathrm{rot}^{i-1}(\mathbf{h})$ に関するベクトルを追加した $(2N + k) \times (2N + k)$ 行列

$$\mathbf{B}_k = \left(\begin{array}{c:c:ccccc} q\mathbf{I}_N & \mathbf{0}_{N\times N} & \multicolumn{5}{c}{\mathbf{0}_{N\times k}} \\ \hdashline \mathbf{H} & \mathbf{I}_N & \multicolumn{5}{c}{\mathbf{0}_{N\times k}} \\ \hdashline \mathbf{h} & \mathbf{0}_{1\times N} & 1 & 0 & 0 & \cdots & 0 \\ \mathrm{rot}(\mathbf{h}) & \mathbf{0}_{1\times N} & 0 & 1 & 0 & \cdots & 0 \\ \mathrm{rot}^2(\mathbf{h}) & \mathbf{0}_{1\times N} & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{rot}^{k-1}(\mathbf{h}) & \mathbf{0}_{1\times N} & 0 & 0 & 0 & \cdots & 1 \end{array}\right)$$

を考え，この $2N+k$ 個の一次独立な行ベクトルで生成される格子を $L_k = \mathcal{L}(\mathbf{B}_k)$ とする．このとき，拡張 NTRU 格子 L_k は NTRU 問題における秘密多項式の係数に関する格子ベクトルを $(k+1)N$ 個含む．復元すべき格子ベクトルの個数が増えることにより，表 1 のように拡張 NTRU 格子に対する BKZ 簡約アルゴリズムを用いた格子攻撃の攻撃成功確率が通常の NTRU 格子（$k = 0$ の場合）より上昇する原理とその実験結果を報告する．

表 1: 拡張 NTRU 格子 $L_k = \mathcal{L}(\mathbf{B}_k)$ に対する格子攻撃の平均成功確率（$k = 0$ は通常の NTRU 格子で，d は NTRU 問題の秘密多項式の Hamming 重みに関する値）

NTRU パラメータ	拡張パラメータ			
(N, q, d)	$k = 0$	$k = 1$	$k = 2$	$k = 3$
$(64, 31, 18)$	31%	**36%**	32%	31%
$(64, 41, 23)$	46%	**52%**	38%	42%
$(64, 53, 28)$	65%	71%	**78%**	67%
$(72, 31, 14)$	71%	**78%**	68%	74%
$(72, 41, 19)$	52%	**58%**	48%	51%
$(72, 53, 27)$	18%	15%	13%	**21%**
$(80, 67, 25)$	41%	**48%**	42%	45%
$(80, 89, 31)$	69%	**80%**	75%	70%
$(80, 101, 36)$	66%	**74%**	62%	69%

参考文献

[1] Satoshi Nakamura and Masaya Yasuda. An extension of Kannan's embedding for solving ring-based LWE problems. In *IMA International Conference on Cryptography and Coding (IMACC 2021)*, volume 13129 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2021.

* NTT 社会情報研究所,
NTT Social Informatics Laboratories
† 立教大学理学部数学科,
Department of Mathematics, Rikkyo University