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

トレース写像を用いたRing-LWE問題に対する格子攻撃の再考
Revisiting lattice-based attacks using trace map for Ring-LWE

奥村 伸也 * 上村 周作 † 工藤 桃成 †
Shinya Okumura Shusaku Uemura Momonari Kudo

キーワード 格子暗号，Ring-LWE，中間体，トレース写像，ノルム写像

あらまし

Ring-LWE 問題 [1] は格子暗号の安全性を支える数学問題の一つで，NIST が現在進めている耐量子計算機暗号の標準化において，いくつかの候補方式の安全性を支えている．Ring-LWE 問題は代数体の整数環上で定義されるが，効率性の観点から円分体が用いられることが多く，この場合次のように定義される：L を n 次の円分体，R を L の整数環とし，q を n を割り切らない素数とする．また，$R_q := R/qR$ とし，R_q 上の誤差に関する確率分布を χ とする．秘密情報 $s \in R_q$ を固定し，一様ランダムに選ばれた $a \in R_q$ と確率分布 χ からサンプルされた e に対して，$(a, b := as + e)$ の組を任意個サンプルする．このとき，公開情報であるサンプル (a, b) たちから秘密情報 s を求める問題を，(円分体の整数環上の) n 次元 Ring-LWE 問題という．Ring-LWE 問題の求解困難性の解析は重要な課題であるが，通常の LWE 問題を通して行われることが多く，円分体の整数環の代数的構造を利用した解法についても検討する必要がある．

2021 年に池松ら [2] は，Ring-LWE 問題に現れる円分体の整数環がもつ**トレース写像**に着目し，特殊な Ring-LWE サンプルを用いたトレース写像攻撃を提案した．具体的には，2 冪の n 次円分体上の Ring-LWE 問題を $(n/2)$ 次の部分体（L の最大総実部分体 K_0）上の問題に帰着可能となる特殊な LWE サンプル (a, s) の存在を明らかにした．また，池松らはそのような特殊なサンプルが存在する確率を計算し，これらのサンプルが十分多く存在する場合には，格子攻撃によって秘密情報 s を高速に求めることができることを示した．しかしながら，このような特殊なサンプルが全サンプルの 1/2 以上存在するためには，格子の次元に関して指数的な個数（$q^{m/2}$ 個）のサンプルが必要である．一方で，池松らの攻撃では $(n/2)$ 次の部分体として，L の最大総実部分体を用いているが，$(n/2)$ 次の部分体は他にも存在する．これに加え，整数環および円分体の代数的構造を記述する写像として，トレース写像の他に**ノルム写像**がある．このことから，最大総実部分体以外の部分体や，ノルム写像を用いた場合に同様の攻撃が可能かを検討する余地があるといえる．

そこで本研究では，上記のトレース写像攻撃を再考し，円分体のガロア群を調べることで，最大総実部分体以外の部分体上に問題を帰着させ，その場合の Ring-LWE 問題の求解困難性を評価する．具体的には，$\mathrm{Gal}(L/K)$ の位数 2 の元に対応する L と Q の中間体 K は K_0 の他に二つ存在するが，これら二つの中間体に対しても池松らと同様の方法でトレース写像攻撃を構成する．また、トレース写像の代わりにノルム写像を使った場合に有効となる特殊な LWE サンプルの存在を明らかにする．

参考文献

[1] Vadim Lyubashevsky, Chris Peikert and Oded Regev, “On Ideal Lattices and Learning with Errors over Rings”, In: Advances in Cryptology-EUROCRYPT 2010, Springer LNCS **6110**, pp. 1–23, 2010.

[2] Ikematsu Y., Nakamura S., Yasuda M. (2021) A Trace Map Attack Against Special Ring-LWE Samples. In: Nakanishi T., Nojima R. (eds) Advances in Information and Computer Security. IWSEC 2021. Lecture Notes in Computer Science, vol 12835. Springer, Cham.

* 大阪大学 大学院工学研究科, Graduate School of Engineering, Osaka University, okumura@comm.eng.osaka-u.ac.jp
† 東京大学 大学院情報理工学系研究科 Graduate School of Information Science and Technology, The University of Tokyo