Vol.2020-CSEC-91 No.32
Vol.2020-SPT-40 No.32
Vol.2020-EIP-90 No.32
2020/11/26

トレース写像を用いたDecision Ring-LWE問題への攻撃について

奥村 泰久[1,a)]　奥村 伸也[1,b)]　宮地 充子[1,c)]

概要：Lerning With Errors (LWE) 問題は，耐量子性をもつ高機能暗号の構成に用いられており，Ring-LWE 問題は代数体の整数環上で考える LWE 問題の一種である．Ring-LWE 問題は LWE 問題と比較して効率的な暗号の構成を可能としており，活発に研究されている．Chen, Lauter, Stange らは modulus となる素数の代数体における相対次数が 2 の場合において Search Ring-LWE 問題への攻撃の計算量を削減する方法を提案した．本稿ではこの攻撃を相対次数が合成数である場合に拡張し，さらにトレース写像を用いることで攻撃に必要な計算量とサンプル数を削減した Decision Ring-LWE 問題への攻撃手法を提案する．

An Attack on Decision Ring-LWE Problem by Trace Map

1. はじめに

Lerarning-with-Errors (LWE) 問題 [8] は誤差付きの連立方程式から解を求める問題であり，耐量子暗号の一種である格子暗号の構成に用いられる [1], [6]．特に格子暗号は準同型性などを持つ高機能暗号を構成することも可能であることから注目されており，活発に研究されている分野である．Ring-Learning-with-Errors (Ring-LWE) 問題 [5] は代数体の整数環上で考える LWE 問題の一種である．Ring-LWE 問題を用いることで LWE 問題を用いる場合よりも効率的な暗号が構成できることが知られている．一般的に Ring-LWE 問題は円分体上で考えられることが多いが，円分体以外の代数体を用いて構成する暗号も提案されている [2]．このことから，より一般の代数体について Ring-LWE 問題を考えることが必要である．

Chen らは，Ring-LWE 問題を小さな有限体上の問題に変換し，その中で秘密情報を総当りする攻撃を提案している [3], [4]．しかし，この攻撃には変換先の有限体のサイズに応じた数のサンプルが必要となっており，計算量もサンプル数に依存することから有限体がある程度大きなものになると攻撃することが困難となる．

[1] 大阪大学
Osaka University
[a)] yas.okumura@cy2sec.comm.eng.osaka-u.ac.jp
[b)] okumura@comm.eng.osaka-u.ac.jp
[c)] miyaji@comm.eng.osaka-u.ac.jp

そこで，我々は有限体のトレース写像を用いることで必要なサンプル数を有限体の素体のサイズのオーダーに削減した Ring-LWE 問題への攻撃手法を提案する．さらに，この攻撃はサンプルのランダム性により攻撃が困難になっているため，使用するサンプルを制限することで攻撃可能な条件を緩和した攻撃手法を提案する．また，[4] で提案された脆弱な代数体を拡大した体において攻撃可能な条件について考察する．

2. 準備

2.1 格子上の離散ガウス分布

$r > 0$ に対して $\rho_r(x) = e^{-||x||^2/r^2}$ とする．

定義 1. 格子 $\Lambda \subset \mathbb{R}^n$，$r > 0$ について幅 r の離散ガウス分布を以下のように定義する．

$$D_{\Lambda,r}(x) = \frac{\rho_r(x)}{\sum_{y\in\Lambda}\rho_r(y)}, \forall x \in \Lambda.$$

2.2 代数体の正規埋め込み

K を次数 n の代数体とし，その整数環を R とする．$\iota : K \to \mathbb{R}^n$ を以下で定義される調整された正規埋め込みとする．$\sigma_1, \sigma_2, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \ldots, \sigma_n$ を K の $\mathbb{C}$ への埋め込み写像とし，$\sigma_1, \ldots, \sigma_{r_1}$ を実埋め込みとし，$1 \le j \le r_2$ について $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ とする．$\iota : K \to \mathbb{R}^n$ を以下で定義する．

Vol.2020-CSEC-91 No.32
Vol.2020-SPT-40 No.32
Vol.2020-EIP-90 No.32
2020/11/26

$$x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sqrt{2}\Re(\sigma_{r_1+1}(x))), \sqrt{2}\Im(\sigma_{r_1+1}(x)), \ldots, \sqrt{2}\Re(\sigma_{r_1+r_2}(x))), \sqrt{2}\Im(\sigma_{r_1+r_2}(x)).$$

2.3 χ^2 検定

χ^2 検定は，仮説検定の一つである．仮説検定とは，ある仮説を与えられた標本から検証する統計学的方法の一つである．χ^2 検定では，ある分布を仮定し，サンプルが仮定した分布に適合するかどうかを検定することができる．S を有限集合とすると，$S_1, S_2, \ldots, S_r$ の部分集合に分割することができる．仮定した分布でサンプリングされた確率変数が S_i に含まれる確率が p_i であるとすると，n 個のサンプルについて各 S_i に含まれるサンプル数の期待値は，$c_i := np_i$ である．実際の部分集合 S_i に含まれるサンプル数を f_i とした時，

$$\chi^2 = \sum_i \frac{(f_i - c_i)^2}{c_i}$$

を計算する．実際のサンプルの分布が仮定した分布と一致する場合，この χ^2 値は自由度 $r-1$ の χ^2 分布に従う．次に，レベルパラメータ α を設定し，自由度 $r-1$ の χ^2 分布の累積分布関数 $F_{r-1}(x)$ から $\delta = F_{r-1}^{-1}(\alpha)$ を計算し，以下の判別を行う．

- $\chi^2 < \delta$
  サンプルの分布は仮定した分布と一致する．
- $\chi^2 \geq \delta$
  サンプルの分布は仮定した分布と一致するとは言えない．

検定には少なくとも $5r$ 以上のサンプル数が必要であるとされている．

2.4 Ring-LWE 問題

$K/\mathbb{Q}$ を次数 n の代数体とする．K の整数環を R とし，$R_q = R/qR$ とする．

定義 2 (Ring-LWE サンプル)**.**

$s \in R_q$，$r > 0$ とする．a を R_q 上の一様分布に従って選択し，e を離散ガウス分布 $D_{\iota(R),r}$ に従って選択したとき，$(a, b = as + e) \in R_q \times R_q$ を Ring-LWE サンプルと呼ぶ．このとき，s を secret，q を modulus，e をエラー，$D_{\iota(R),r}$ を離散エラー分布と呼ぶ．

定義 3 (Decision Ring-LWE 問題)**.**

任意個の独立なサンプル (a, b) が与えられたときに，そのサンプルが Ring-LWE サンプルであるか $R_q \times R_q$ 上の一様分布に従って選択されたサンプルであるかを識別する問題を Dicision Ring-LWE 問題と呼ぶ．

定義 4 (Search Ring-LWE 問題)**.**

任意個の独立な Ring-LWE サンプル (a, b) が与えられたときに，そのサンプルから secret s を求める問題を Search Ring-LWE 問題と呼ぶ．

2.5 素イデアル分解

$K/\mathbb{Q}$ を n 次の代数体とし，その整数環を R とする．K 上の素数 q に対して R 上の異なる r 個の素イデアル $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ が存在し，R 上のイデアル qR は以下のように素イデアル分解できる．

$$qR = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}.$$

このときの e_i を分岐指数と呼ぶ．また，各 $\mathfrak{q}_i$ について

$$R/\mathfrak{q}_i \cong \mathbb{F}_{q^{f_i}}$$

が成立し，この f_i を q の $\mathfrak{q}$ 上の相対次数と呼ぶ．全ての i $(1 \leq i \leq r)$ に対して $e_i = 1$ であるとき q は K 上不分岐であるといい，そうでないときは分岐するという．また，全ての i $(1 \leq i \leq r)$ に対して $f_i = 1$ であるとき q は K 上完全分解するという．また，$\sum_{i=1}^{r} e_i f_i = n$ が成り立つ．中国式剰余定理より，R/qR は

$$R/qR \cong R/\mathfrak{q}_1^{e_1} \times \cdots \times R/\mathfrak{q}_r^{e_r}$$

のように分解できる．特に q が K 上不分岐であるならば，

$$R/qR \cong \mathbb{F}_{q^{f_1}} \times \cdots \times \mathbb{F}_{q^{f_r}}$$

が成り立つ．

3. 既存研究

Chen ら [3] は，R_q から小さな体 F への環準同型写像を用いて Ring-LWE 問題を F 上の問題に変換し，F 上で secret を総当りした際に対応するエラーの分布が一様分布であるかを判別することでサンプルが Ring-LWE サンプルであるか識別する攻撃を提案した．さらに，この Decision 攻撃では F 上での secret の値が得られることから，q が K 上で不分岐である場合について q 上の各素イデアル $\mathfrak{q}$ について $R/\mathfrak{q}$ で Decision 攻撃を行い中国式剰余定理を用いることで R_q での secret の値を計算する Search 攻撃を提案した．この攻撃に必要なサンプル数は $O(q^f)$ であり，計算量は $O(nq^{2f})$ である．

また，Chen ら [4] は modulus q の K における相対次数が 2 である場合において $R/\mathfrak{q} \cong \mathbb{F}_{q^2}$ 上の secret を $\mathbb{F}_q$ の部分と $\mathbb{F}_{q^2}/\mathbb{F}_q$ の部分に分割し，$\mathbb{F}_{q^2}/\mathbb{F}_q$ の部分のみを推測することで Search 攻撃に必要なサンプル数と計算量を削減する方式を提案した．この攻撃に必要なサンプル数は $O(q)$ であり，計算量は $O(nq^2)$ である．

4. 攻撃手法

この章では提案する攻撃手法について説明する．まず，[4] の Search 攻撃を 2 以上の偶数の相対次数 f を持つ代数体に適用可能な形に拡張する．次に，拡張した攻撃を基にトレース写像を用いることで必要なサンプル数を削減した攻撃手法について説明する．さらに，トレース写像を用い

Vol.2020-CSEC-91 No.32
Vol.2020-SPT-40 No.32
Vol.2020-EIP-90 No.32
2020/11/26

た攻撃に用いるサンプルを制限することで攻撃可能な代数体の条件を緩和した攻撃手法について説明する．

4.1 既存手法の拡張攻撃

以下の条件を仮定する．

- modulus q は q 上の素イデアル $\mathfrak{q}$ 上で偶数の相対次数 f を持ち，$f' = f/2$ を満たす整数 f' が存在する．
- 環準同型写像 $\rho : R_q \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}$ が以下の条件を満たすような q 上の素イデアル $\mathfrak{q}$ が存在する：$e \in R_q$ を離散エラー分布から取られたサンプルとする．$\rho(e)$ が $\mathbb{F}_{q^f}$ の部分体 $\mathbb{F}_{q^{f'}}$ に含まれている確率が $1/q^{f'}$ と識別可能である．

環準同型写像 ρ を用いてサンプル $(a, b) \in R_q \times R_q$ を $\mathbb{F}_{q^f} \times \mathbb{F}_{q^f}$ に写像する．

$t_1, \cdots, t_{q^{f'}}$ を $\mathbb{F}_{q^f}/\mathbb{F}_{q^{f'}}$ の完全代表系とする．このとき，$\rho(s) = s_0 + t_i$ となる添字 i と $s_0 \in \mathbb{F}_{q^{f'}}$ が一意に存在する．

Frobenius 写像を以下のように定義する．

$$\overline{a} := a^{q^{f'}}, \forall a \in \mathbb{F}_{q^f}.$$

Frobenius 写像は $\mathbb{F}_{q^f}$ 上の自己準同型写像となる．

簡単のため，$b = \rho(b), a = \rho(a), s = \rho(s), e = \rho(e)$ と表す．このとき，$s = s_0 + t_i$ より，$\overline{b} - b - \overline{at_i} + at_i = s_0(\overline{a} - a) + \overline{e} - e$ が得られる．$\overline{a} \neq a$ のとき，両辺を $\overline{a} - a$ で割ることで以下の式が得られる．

$$\frac{\overline{b} - b - \overline{at_i} + at_i}{\overline{a} - a} = s_0 + \frac{\overline{e} - e}{\overline{a} - a}. \tag{1}$$

ここで，各 j $(1 \leq j \leq q^{f'})$ について以下を計算することができる．

$$m_j(a, b) := \frac{\overline{b} - b - \overline{at_j} + at_j}{\overline{a} - a}.$$

命題 5. 各 j $(1 \leq j \leq q^{f'})$ について，

- $i \neq j$ のとき，$m_j(a, b)$ は $\mathbb{F}_q$ 上で一様に分布する．
- $i = j$ のとき，$m_j(a, b) := s_0 + \frac{\overline{e} - e}{\overline{a} - a}$ となる．

証明. $i = j$ のときは (1) より明らかである．

$i \neq j$ のときを示すために以下の補題を示す．

補題 6. $A_q = \mathbb{F}_{q^f} \backslash \mathbb{F}_{q^{f'}}$ とする．a を A_q 上の一様分布からサンプリングされた乱数とする．e を a と独立な $\mathbb{F}_{q^f}$ 上の乱数とする．このとき，$\delta \in A_q, s_0 \in \mathbb{F}_{q^{f'}}$ について

$$m_\delta = g_\delta + s_0 + \frac{\overline{e} - e}{\overline{a} - a}$$

は $\mathbb{F}_{q^{f'}}$ 上で一様に分布する．ここで，g_δ は以下である．

$$g_\delta = \frac{\overline{a\delta} - a\delta}{\overline{a} - a}.$$

証明. 集合 V を $V = \left\{x \in \mathbb{F}_{q^f} : \overline{x} = -x\right\}$ とする．任意の $c, d \in V; c \neq 0$ について，以下が成り立つことを示す．

$$P\left(\overline{a} - a = c, \overline{a\delta} - a\delta = d\right) = \frac{1}{q^{f'}(q^{f'} - 1)}. \tag{2}$$

集合 V は 1 次元 $\mathbb{F}_{q^{f'}}$-ベクトル空間であり，以下のような $\mathbb{F}_{q^{f'}}$-線形写像 $f_\delta : \mathbb{F}_{q^{f'}} \to V^2$ が定義できる．

$$f_\delta : a \mapsto (\overline{a} - a, \overline{a\delta} - a\delta).$$

$\mathrm{Ker}(f_\delta) = \{0\}$ より，f_δ は単射である．また，$\mathbb{F}_{q^{f'}}$ と V^2 の位数が一致することから，f_δ は同型写像となる．ここで f_δ の定義域を A_q に制限することで，A_q と $(V \backslash \{0\}) \times V$ の間の全単射が得られる．これより，(2) が成り立つ．

$e' = \frac{\overline{e} - e}{\overline{a} - a}$ とする．任意の $z \in \mathbb{F}_{q^{f'}}$ について以下が成り立つ．

$$\begin{aligned}
&P(g_\delta + e' = z) \\
&= \sum_{x+y=z} P(g_\delta = x, e' = y) \\
&= \sum_{x+y=z} \sum_{c \in V \backslash \{0\}} P(\overline{a\delta} - a\delta = xc, \overline{e} - e = yc, \overline{a} - a = c) \\
&= \sum_{x+y=z, c \in V \backslash \{0\}} P(\overline{a\delta} - a\delta = xc, \overline{a} - a = c) P(\overline{e} - e = yc) \\
&= \frac{1}{q^{f'}(q^{f'} - 1)} \sum_{y \in \mathbb{F}_{q^{f'}}, c \in V \backslash \{0\}} P(\overline{e} - e = yc) \\
&= \frac{1}{q^{f'}(q^{f'} - 1)} (q^{f'} - 1) \sum_{c' \in V} P(\overline{e} - e = c') \\
&= \frac{1}{q^{f'}}.
\end{aligned}$$

□

$\delta = t_i - t_j$ として補題 6 を適用すると，$m_j(a, b) = g_\delta + s_0 + \frac{\overline{e} - e}{\overline{a} - a}$ であるから $m_j(a, b)$ は $\mathbb{F}_{q^{f'}}$ 上で一様に分布する． □

各 j $(1 \leq j \leq q^{f'})$ についてサンプルから $m_j(a, b)$ を計算する．ただし，$a \in \mathbb{F}_{q^{f'}}$ の場合はそのサンプルを無視する．$m_j(a, b)$ に対して χ^2 検定をする．$i \neq j$ のときこの分布は一様分布となる．$i = j$ のとき $P(m_i(a, b) = s_0) = P(e \in \mathbb{F}_{q^{f'}})$ であり，仮定よりこの確率は $1/q^{f'}$ より大きい．これより，$m_i(a, b)$ の中で最も出現する頻度が高い値を調べることで s_0 の値がわかる．$s = s_0 + t_i$ とすることで s の値が得られる．

この攻撃に必要なサンプル数は $O(q^{f'})$ である．計算量については，各 j $(1 \leq j \leq q^{f'})$ について写像 ρ の計算が必要である．ρ は $O(n)$ で計算が可能である．この計算を $O(q^{f'})$ 個のサンプルに対して行うため，攻撃に必要な計算量は $O(nq^f)$ となる．

4.2 トレース写像を用いた Decision 攻撃

以下の条件を仮定する．

- modulus q は q 上の素イデアル $\mathfrak{q}$ 上で偶数の相対次数

Vol.2020-CSEC-91 No.32
Vol.2020-SPT-40 No.32
Vol.2020-EIP-90 No.32
2020/11/26

f を持ち，$f' = f/2$ を満たす整数 f' が存在する．

- 環準同型写像 $\rho : R_q \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}$ が以下の条件を満たすような q 上の素イデアル $\mathfrak{q}$ が存在する：$e \in R_q$ を離散エラー分布から取られたサンプルとする．$\rho(e)$ が $\mathbb{F}_{q^f}$ の部分体 $\mathbb{F}_{q^{f'}}$ に含まれている確率が $1/q^{f'}$ より十分に大きい．

各 j $(1 \leq j \leq q^{f'})$ について，4.1 節の攻撃と同様に $m_j(a,b)$ を計算する．

トレース写像 $\mathrm{Tr} : \mathbb{F}_{q^f} \to \mathbb{F}_q$ を以下のように定義された写像とする．

$$\mathrm{Tr}(a) := \sum_{i=0}^{f-1} a^{q^i}, \forall a \in \mathbb{F}_{q^f}.$$

Tr は加法準同型を満たすことから，Ring-LWE サンプル (a,b) に対し以下を得る．

$$\mathrm{Tr}(m_i(a,b)) := \mathrm{Tr}(s_0) + \mathrm{Tr}\left(\frac{\overline{e}-e}{\overline{a}-a}\right). \tag{3}$$

各 j $(1 \leq j \leq q^{f'})$ についてサンプルから $\mathrm{Tr}(m_j(a,b))$ を計算する．ただし，$a \in \mathbb{F}_{q^{f'}}$ の場合はそのサンプルを無視する．$m_j(a,b)$ に対して χ^2 検定をする．サンプルが Ring-LWE サンプルでない場合，全ての j について $m_j(a,b)$ は一様に分布する．サンプルが Ring-LWE サンプルである場合，命題 5 より $i \neq j$ の場合 $m_j(a,b)$ は一様に分布するため，$\mathrm{Tr}(m_j(a,b))$ も $\mathbb{F}_q$ 上で一様に分布する．$i = j$ の場合，$P(\mathrm{Tr}(m_j(a,b)) = \mathrm{Tr}(s_0)) = P(\frac{\overline{e}-e}{\overline{a}-a} \in \mathrm{Ker}(\mathrm{Tr}))$ となる．$0 \in \mathrm{Ker}(\mathrm{Tr})$ より，$e \in \mathbb{F}_{q^{f'}}$ のとき $\frac{\overline{e}-e}{\overline{a}-a} \in \mathrm{Ker}(\mathrm{Tr})$ である．$e \notin \mathbb{F}_{q^{f'}}$ のとき $\mathrm{Tr}(\frac{\overline{e}-e}{\overline{a}-a})$ が $\mathbb{F}_q$ 上の一様分布になると仮定すると，e が $\mathbb{F}_{q^{f'}}$ の元である確率が $1/q^{f'}$ と十分に離れている場合 $\mathrm{Tr}(m_j(a,b)) = \mathrm{Tr}(s_0)$ となる確率は $1/q$ と識別可能となる．

これより，すべての j について $\mathrm{Tr}(m_j(a,b))$ が一様分布であるならサンプルは Ring-LWE サンプルではない，ある j についてのみ $\mathrm{Tr}(m_j(a,b))$ が一様分布でないならサンプルは Ring-LWE サンプルであるとして識別ができる．この攻撃のアルゴリズムを Algorithm 1 に示す．

この攻撃に必要なサンプル数は $O(q)$ である．計算量については，各 j $(1 \leq j \leq q^{f'})$ について写像 ρ と Tr の計算が必要である．ρ は $O(n)$ で計算が可能であり，Tr は $\mathbb{F}_{q^{f'}}$ の $\mathbb{F}_q$ 上の基底について事前に計算しておくことで $O(f')$ で計算が可能である．これを $O(q)$ 個のサンプルに対して行うため，攻撃に必要な計算量は $O(nf'q^{f'+1})$ となる．

この攻撃は 4.1 節の攻撃と比べて必要となるサンプル数が減少している．また，計算量もサンプル数の減少に伴い小さくなっている．しかし，トレース写像を使用したため攻撃成功時に得られる情報が t_i と $\mathrm{Tr}(s_0)$ となっており s の復元ができなくなっている．そのため，この攻撃は Decision 攻撃となる．

Algorithm 1 トレース写像を用いた Decision 攻撃

Input: K-代数体; R-K の整数環; $\mathfrak{q}$-素数 q 上で偶数の相対次数 f をもつ R の素イデアル; $\mathcal{S}$-M 個のサンプルの集合; δ-χ^2 検定に用いる閾値パラメータ;
Output: 推測値 t_i と $\mathrm{Tr}(s \pmod{\mathfrak{q}})$，もしくは **NOT-RLWE**，もしくは **INSUFFICIENT-SAMPLES**

```
G ← ∅
for j in 1, ..., q^{f'} do
    E_j ← ∅
    for a, b in S do
        ā, b̄ ← a (mod q), b (mod q)
        m_j ← (b̄ − b − ā t_j + a t_j) / (ā − a)
        E_j に m_j を追加
    end for
    一様分布についての χ^2 検定を E_j に行う
    if χ^2(E_j) > δ then
        ts_0 := E_j で最も出現頻度が高い要素
        g ← (t_j, ts_0), G に g を追加
    end if
end for
if G = ∅ then
    return NOT-RLWE
else if G = {g} then
    return g
else
    return INSUFFICIENT-SAMPLES
end if
```

4.3 サンプルを制限した Decision 攻撃

4.2 節の攻撃では a がランダムであることから $e \notin \mathbb{F}_{q^{f'}}$ のときのトレースについて考えることが難しかった．そこで $\overline{a} - a$ がある値を取るときについてのみ考えることで攻撃可能な条件をより厳密にできると考えた．以下，攻撃について説明する．

以下の条件を仮定する．

- modulus q は，ある q 上の素イデアル $\mathfrak{q}$ が存在し，$\mathfrak{q}$ における分岐指数が 1 であり，相対次数 f が $f' = f/2$ を満たす整数 f' を持つ．
- 環準同型写像 $\rho : R_q \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}$ が以下の条件を満たす：$e \in R_q$ を離散エラー分布から取られたサンプルとする．4.2 節と同様の Frobenius 写像とトレース写像を考える．$U := \{\overline{x} - x : x \in \mathbb{F}_{q^f}\}$ とする．ある $\theta \in V, \theta \neq 0$ が存在し，$(\overline{\rho(e)} - \rho(e))/\theta$ が $\mathrm{Ker}(\mathrm{Tr})$ に含まれている確率が $1/q$ と識別可能である．

環準同型写像 ρ を用いてサンプル $(a,b) \in R_q \times R_q$ を $\mathbb{F}_{q^f} \times \mathbb{F}_{q^f}$ に写像する．簡単のため，サンプルを $(a,b) = (\rho(a), \rho(b)) \in \mathbb{F}_{q^f} \times \mathbb{F}_{q^f}$ と表す．サンプル (a,b) のうち a が

$$\overline{a} - a = m\theta, (m \in \mathbb{F}_q)$$

を満たすもののみを用いる．

このサンプルに対して 4.2 節の攻撃と同様に j $(1 \leq j \leq q^{f'})$ に対して $\mathrm{Tr}(m_j(a,b))$ を計算する．

命題 7. 各 j $(1 \leq j \leq q^{f'})$ について，

Vol.2020-CSEC-91 No.32
Vol.2020-SPT-40 No.32
Vol.2020-EIP-90 No.32
2020/11/26

- $i \neq j$ のとき，$\mathrm{Tr}(m_j(a,b))$ は $\mathbb{F}_q$ 上で一様に分布する．
- $i = j$ のとき，$\mathrm{Tr}(m_j(a,b)) := \mathrm{Tr}(s_0) + \mathrm{Tr}\left(\frac{\overline{e}-e}{\overline{a}-a}\right)$ となる．

証明. $i = j$ のときについては明らかである．$i \neq j$ のときについては補題 6 を修正した以下の補題を示せば良い．

補題 8. $A_q = \mathbb{F}_{q^f} \backslash \mathbb{F}_{q^{f'}}$ とする．$A'_q = \{x \in \mathbb{F}_{q^f} \backslash \mathbb{F}_{q^{f'}} : \exists m \in \mathbb{F}_q, \overline{x} - x = m\theta\}$ とする．a を A'_q 上の一様分布からサンプリングされた乱数とする．e を a と独立な $\mathbb{F}_{q^f}$ 上の乱数とする．このとき，$\delta \in A_q, s_0 \in \mathbb{F}_{q^{f'}}$ について

$$m_\delta = g_\delta + s_0 + \frac{\overline{e} - e}{\overline{a} - a}$$

は $\mathbb{F}_{q^{f'}}$ 上で一様に分布する．ここで，g_δ は以下である．

$$g_\delta = \frac{\overline{a\delta} - a\delta}{\overline{a} - a}.$$

証明. 集合 V を $V = \left\{x \in \mathbb{F}_{q^f} : \overline{x} = -x\right\}$ とする．V' を $V' = \{m\theta : \forall m \in \mathbb{F}_q\}$ とする．任意の $c \in V' \backslash \{0\}, d \in V$ について，以下が成り立つことを示す．

$$P\left(\overline{a} - a = c, \overline{a\delta} - a\delta = d\right) = \frac{1}{q^{f'}(q-1)}. \qquad (4)$$

補題 6 の証明で用いた同型写像 f_δ の定義域を A'_q に制限することで，A'_q と $V' \backslash \{0\} \times V$ の間の全単射が得られる．これより，(4) が成り立つ．

$e' = \frac{\overline{e}-e}{\overline{a}-a}$ とする．任意の $z \in \mathbb{F}_{q^{f'}}$ についていかが成り立つ．

$$\begin{aligned}
&P(g_\delta + e' = z) \\
&= \sum_{x+y=z} P(g_\delta = x, e' = y) \\
&= \sum_{x+y=z} \sum_{c \in V' \backslash \{0\}} P(\overline{a\delta} - a\delta = xc, \overline{e} - e = yc, \overline{a} - a = c) \\
&= \sum_{x+y=z, c \in V' \backslash \{0\}} P(\overline{a\delta} - a\delta = xc, \overline{a} - a = c) P(\overline{e} - e = yc) \\
&= \frac{1}{q^{f'}(q-1)} \sum_{y \in \mathbb{F}_{q^{f'}}, c \in V' \backslash \{0\}} P(\overline{e} - e = yc) \\
&= \frac{1}{q^{f'}(q-1)} (q-1) \sum_{c' \in V} P(\overline{e} - e = c') \\
&= \frac{1}{q^{f'}}.
\end{aligned}$$

□

補題 8 を $\delta = t_i - t_j$ として適用することで $i \neq j$ のときについて成り立つことがわかる． □

a の条件より，$\overline{a} - a = m\theta, (m \in \mathbb{F}_q)$ と表せる．これより，$i = j$ のとき $\mathrm{Tr}(m_j(a,b)) = \mathrm{Tr}(s_0) + \mathrm{Tr}(\frac{\overline{e}-e}{m\theta})$ と表せる．仮定より $\mathrm{Tr}(\frac{\overline{e}-e}{m\theta}) = 0$ である確率が $1/q$ と識別可能であるから，サンプルが Ring-LWE サンプルで $i = j$ のとき，$\mathrm{Tr}(m_j(a,b))$ は一様分布にはならない．また，すべての j について $\mathrm{Tr}(m_j(a,b))$ が一様分布であるならサンプルは Ring-LWE サンプルではない．これを χ^2 検定を用いて検定することで Decision 攻撃が可能である．

この攻撃に必要な計算量は $O(nf'q^{f'+1})$ である．また，攻撃に必要なサンプル数は $O(q)$ であるが，これは使用するサンプルを a の値に基づいて制限した後のサンプル数である．a が条件を満たす確率は $1/q^{f'-1}$ であるから，全体として必要なサンプル数は $O(q^{f'})$ となる．

5. 攻撃が適用可能である条件の考察

この章では，[4] で提案された脆弱な代数体を拡大した体について，4.3 節の攻撃が適用可能な条件について考察する．

p を奇素数とし，f を 2 以上の偶数で，$f' = f/2$ とする．$d > 1$ を整数に f 乗根を持たないような p と互いに素な整数とする．奇素数 q を $q \equiv 1 \pmod{p}, q^{f'} \equiv 1 \pmod{f}$ を満たし，$\mathbb{F}_q$ 上に d の f 乗根が存在しないように選択する．

$M = \mathbb{Q}(\zeta_p)$ を p 次円分体とし，$L = \mathbb{Q}(\sqrt[f]{d})$ とする．$K = M \cdot L$ を合成体とし，その整数環を $\mathcal{O}_K$ とする．このとき，$K/\mathbb{Q}$ は拡大次数 $f(p-1)$ の分離拡大となる．素数 q は M 上で完全分解し，L 上で惰性 ($q\mathcal{O}_L$ 自体が素イデアルとなる) であるため，K 上で相対次数 f を持つ．

K の q 上の素イデアル $\mathfrak{q}$ について $\mathcal{O}_K/\mathfrak{q} \cong \mathbb{F}_{q^f}$ は $\mathbb{F}_{q^f} \cong \mathbb{F}_q[x]/(x^f - d)$ となる．このとき，仮定より $\overline{x} = -x$ となる．$a = \sum_{i=0}^{f-1} a_i x^i \in \mathbb{F}_{q^f}, a_i \in \mathbb{F}_q$ とすると，$\overline{a} = \sum_{i=0}^{f-1} (-1)^i a_i x^i$ となる．これより，$\mathbb{F}_{q^{f'}}$ の元は $\sum_{i=0}^{f/2-1} a_i x^{2i}$，$U$ の元は $\sum_{i=0}^{f/2-1} a_i x^{2i+1}$ と表せる．また，

$$\mathrm{Tr}(x) = \sum_{i=0}^{f-1} x^{q^i} = \sum_{i=0}^{f'-1} x^{q^i} - \sum_{i=0}^{f'-1} x^{q^i} = 0$$

が成り立つため，$\mathrm{Tr}(a) = 0$ となるのは $a_0 = 0$ のときとなる．

4.3 節における θ を $\theta = x^{f-1}$ とすると $e \in \mathbb{F}_{q^f}$ について $(\overline{e} - e)/\theta$ が $\mathrm{Ker}(\mathrm{Tr})$ に含まれているための条件は e の x^{f-1} の係数が 0 であることとなる．

f は偶数で d は整数と $\mathbb{F}_q$ 上に平方根も持たないため，$K' = M \cdot \mathbb{Q}(\sqrt{d})$ は K の部分体となる．この K' について [4], 定理 1 より，エラーが K' の q 上の素イデアル $\mathfrak{q}$ について $\mathcal{O}_{K'}/\mathfrak{q} \cong \mathbb{F}_{q^2}$ 上で $\mathbb{F}_q$ の元になる確率がエラー分布の幅 r が十分小さい場合に $1/q$ より大きくなることが言える．

これを K で考えると，エラーが K の q 上の素イデアル $\mathfrak{q}$ について $\mathcal{O}_K/\mathfrak{q} \cong \mathbb{F}_{q^f}$ 上で $f' \leq i \leq f-1$ において x^i の係数が全て 0 となる確率が $1/q$ より大きくなると考えられる．このとき，x^{f-1} の係数も 0 となるため 4.3 節の攻撃の条件を満たす．さらに $f' \leq i \leq f-1$ において x^i の係数が全て 0 となるというのはより強い条件であるためより大きなエラー幅 r に対しても攻撃が可能であると予測できる．

6. おわりに

本論文では Ring-LWE 問題への既存攻撃に対してトレース写像を適用することで攻撃に必要なサンプル数と計算量を抑えた Decision 攻撃を提案した．また，攻撃に使用するサンプルを制限することにより攻撃が可能な代数体の条件を緩和した攻撃を提案した．さらに，既存の脆弱な代数体を拡大した体について攻撃が適用可能な条件について考察した．その結果，既存攻撃の拡張では攻撃できないサイズのエラー幅を持つ Ring-LWE サンプルに対しても攻撃可能であることが期待できるとわかった．

今後の課題として，論文内で考察した代数体について実験を行い攻撃の有効性を確認することが挙げられる．また，これ以外にも攻撃が適用可能な代数体が存在するかについても考察する．さらには，この攻撃を Search 攻撃に持ち上げることでより効率的に Search Ring-LWE 問題への攻撃ができないか検討する．

謝辞

本研究の一部は文部科学省「Society5.0 に対応した高度技術人材育成事業成長分野を支える情報技術人材の育成拠点の形成 (enPiT)」さらに文部科学省の平成 30 年度「Society 5.0 実現化研究拠点支援事業」の助成を受けています．

参考文献

[1] Alkim, E., Ducas, L., Pöppelmann, T. and Schwabe, P.: Post-quantum key exchange - a new hope, *IACR Cryptol. ePrint Arch.*, Vol. 2015, p. 1092 (online), available from ⟨http://eprint.iacr.org/2015/1092⟩ (2015).

[2] Arita, S. and Handa, S.: Subring Homomorphic Encryption, *Information Security and Cryptology - ICISC 2017 - 20th International Conference, Seoul, South Korea, November 29 - December 1, 2017, Revised Selected Papers* (Kim, H. and Kim, D., eds.), Lecture Notes in Computer Science, Vol. 10779, Springer, pp. 112–136 (online), DOI: 10.1007/978-3-319-78556-1_7 (2017).

[3] Chen, H., Lauter, K. E. and Stange, K. E.: Attacks on the Search RLWE Problem with Small Errors, *SIAM J. Appl. Algebra Geom.*, Vol. 1, No. 1, pp. 665–682 (online), DOI: 10.1137/16M1096566 (2017).

[4] Chen, H., Lauter, K. E. and Stange, K. E.: Security considerations for Galois non-dual RLWE families, *CoRR*, Vol. abs/1710.03316 (online), available from ⟨http://arxiv.org/abs/1710.03316⟩ (2017).

[5] Lyubashevsky, V., Peikert, C. and Regev, O.: On Ideal Lattices and Learning with Errors over Rings, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings* (Gilbert, H., ed.), Lecture Notes in Computer Science, Vol. 6110, Springer, pp. 1–23 (online), DOI: 10.1007/978-3-642-13190-5_1 (2010).

[6] Lyubashevsky, V., Peikert, C. and Regev, O.: A Toolkit for Ring-LWE Cryptography, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings* (Johansson, T. and Nguyen, P. Q., eds.), Lecture Notes in Computer Science, Vol. 7881, Springer, pp. 35–54 (online), DOI: 10.1007/978-3-642-38348-9_3 (2013).

[7] Neukirch, J.: *Algebraic Number Theory*, Springer (1999).

[8] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005* (Gabow, H. N. and Fagin, R., eds.), ACM, pp. 84–93 (online), DOI: 10.1145/1060590.1060603 (2005).