Vol.2021-DPS-186 No.37
Vol.2021-CSEC-92 No.37
2021/3/15

Decision Ring-LWE問題に対する部分格子攻撃の改良について

室井　謙典[1,a)]　奥村　伸也[1,b)]　宮地　充子[1,2,c)]

概要：2005 年に Regev により提案された LWE 問題の計算困難性は，耐量子暗号と期待されている多くの格子暗号の安全性の根拠となっており，代数体の整数環上での LWE 問題である Ring-LWE 問題を利用することで，より効率的な暗号方式を構成できることが知られている．我々は，Decision Ring-LWE 問題に対して，代数体上の部分格子を用いた攻撃を提案したが，サンプルの条件が厳しく攻撃対象のサンプルを集めることが困難であった．本稿では，部分格子攻撃を改良し，サンプルの条件が緩和する手法を提案する．

キーワード：Ring-LWE 問題，部分格子

On Improving Sublattice Attack for the Decision Ring-LWE Problem

Abstract: The computational hardness of the LWE problem proposed by Regev in 2005 is the basis for the security of many lattice cryptosystems, which are expected to be quantum resistant. We proposed an attack on the Decision Ring-LWE problem by using a sublattice on the ring of integers, but it was difficult to collect samples for the attack due to the strict sample requirements. In this paper, we propose a method to improve the sublattice attack and loosen the sample condition.

Keywords: Ring-LWE problem, Sublattice attack

1. はじめに

様々な情報が通信によって交換される現代では，それらの情報を暗号化し，データを安全に取り扱うことは重要である．データの暗号化にはこれまで，RSA 暗号や楕円曲線暗号などの暗号方式が利用されてきた．しかし，量子コンピュータの実現時には，それらの安全性の根拠である，素因数分解問題や離散対数問題といった数学的な問題が解読されてしまうことが示されている．そのため，量子コンピュータに対しても安全な，耐量子暗号の研究が活発に行われている．2005 年に Regev によって提案された Learnig With Errors(LWE) 問題を用いる格子ベース暗号は耐量子暗号として期待されている．格子ベース暗号は主に，AD 方式 [1]，GGH 方式 [2]，NTRU 方式 [3]，LWE 方式 [4], [5] の 4 種類が存在しているが，本研究では代数体の整数環上での LWE 問題である Ring-LWE 問題 [5] に注目する．LWE 問題は，公開鍵を作成する際に，エラーと呼ばれる小さな値を誤差として付け加えることで，秘密鍵が復元されることを困難にしている．また，Ring-LWE 問題を利用することによって，より効率的な暗号方式を構成する方法 [6] も提案されている．これまでに，Ring-LWE 問題の安全性解析として, 様々な攻撃が提案されている．

室井らは，整数環上の部分格子を用いることで Hao Chen が [7] で攻撃対象とした代数体上の Ring-LWE 問題を実験的に解析した [8]．しかし，攻撃対象の代数体が限定的である．よって，既存の部分格子攻撃の攻撃対象を拡張し，アイゼンシュタインの既約判定法を用いて生成した既約多項式によって構成される代数体に対して攻撃を行った．また，この攻撃には Ring-LWE サンプル a と攻撃に用いる格子 $\mathscr{L}$ が $a\mathscr{L} \subset \mathscr{L}$ という条件を満たす必要がある．攻撃には χ^2 検定を使用しており，検定には一定のサンプル数が必要であるが，そのような条件を満たすサンプルを取得することは困難であると考えられる．よって本研究では，部分格子の基底を変更することによって，サンプル a の条件が緩和できることを提案した．また，その格子を用いて攻

[1] 大阪大学
Osaka University
[2] 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology
[a)] muroi@cy2sec.comm.eng.osaka-u.ac.jp
[b)] okumura@cy2sec.comm.eng.osaka-u.ac.jp
[c)] miyaji@cy2sec.comm.eng.osaka-u.ac.jp

撃を行い，実験的な解析も行った．

2. 準備

2.1 代数体と整数環

有理数体 $\mathbb{Q}$ の有限次拡大を代数体という．また代数体 K に対して，K に含まれている代数的整数全体の集合を K の整数環といい R と表す．

2.2 χ^2 検定

χ^2 検定には，独立検定と適合度検定の二種類が存在するが，ここでは本稿で用いる適合度検定のみを記載する．適合度検定では，検定するサンプルがある分布に従ってサンプルされていると仮定し，その仮定した分布が実際にサンプルが従う分布と適合しているかを検定する．起こりえる試行の結果が k 通りあるとき，試行回数を n, それぞれの結果が起こりうる確率を p_i と表す．それぞれの結果の観測度数を O_i，$E_i = np_i$ を期待度数とする．ここで，帰無仮説と対立仮説を以下のように定義する．

- H_0 : 観測度数は仮定した分布に従って得られたものである
- H_1 : 観測度数は仮定した分布に従って得られたものではない

また，χ^2 検定統計量 χ_0^2 を

$$\chi_0^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}$$

と定義する．帰無仮説 H_0 が真であるとき，χ_0^2 は自由度が $k-1$ の χ^2 分布に従う優位水準が α であるとき，自由度 $k-1$ の χ^2 分布の累積密度関数より $\chi_\alpha^2(k-1)$ を計算する．このとき，以下のように仮説を採択するか棄却するかを決定する

- $\chi_0^2 > \chi_\alpha^2$ のとき
  帰無仮説 H_0 を採択し，得られた分布が優位水準 α において仮定した分布と一致しないと結論づける．
- $\chi_0^2 \leq \chi_\alpha^2$ のとき対立仮説 H_1 を採択し，得られた分布が優位水準 α において仮定した分布と一致すると結論づける．

2.3 Ring-LWE 問題

ここでは，本研究で攻撃対象となっている Ring-LWE 問題について述べる．

定義 2.1 (Ring-LWE 問題)**.** Ring-LWE 問題は整数環上での LWE 問題である．q を素数とし，K を代数体，R を K の整数環，$R_q = R/qR$ とする．$a \in R_q$ を一様ランダムにサンプリングし，シークレットとエラーの係数をそれぞれ R_q 上の確率分布 $D_{\sigma_s}, D_{\sigma_e}$ からサンプリングする．このとき $(a, b = a \cdot s + e \in R_q)$ を Ring-LWE サンプルという．

Ring-LWE 識別問題

サンプル $(a,b) \in R_q \times R_q$ が与えられたとき，サンプルが一様分布からサンプリングされたものか，Ring-LWE サンプルかどうか識別する問題.

Ring-LWE 探索問題

Ring-LWE サンプルが与えられたとき，そのサンプルからシークレット s を求める問題.

2.4 アイゼンシュタインの既約判定法

定義 2.2 (アイゼンシュタインの既約判定法)**.** ある素数 p が存在して係数が整数である次のような多項式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

に対して，以下の三つの条件

- $p \mid a_0$ かつ $p^2 \nmid a_0$,
- $p \mid \{a_1, \cdots, a_{k-1}\}$,
- $p \nmid a_k$.

を満たすとき，多項式 $f(x)$ は既約である.

2.5 素イデアル分解

K を n 次の代数体とし, K の整数環を R とする．K 上の素数 q に対して，R の異なるイデアル $\mathfrak{P}_1^{e_1}\mathfrak{P}_1^{e_2}\cdots\mathfrak{P}_1^{e_k}$ が存在し，イデアル qR は次のように

$$qR = \mathfrak{P}_1^{e_1}\mathfrak{P}_1^{e_2}\cdots\mathfrak{P}_1^{e_k}$$

と分解される．また，

$$R/\mathfrak{P}^{e_i} \simeq \mathbb{F}_{q^{f_i}}$$

が成り立ち，e_i を分岐指数，f_i を相対次数という．また，中国式剰余定理より，R/qR は次のように

$$R/qR \simeq R/\mathfrak{P}_1^{e_1} \times \ldots \times R/\mathfrak{P}_k^{e_k}$$

と分解され，q が K 上不分岐であるとき

$$R/qR \simeq \mathbb{F}_{q^{f_1}} \times \ldots \times \mathbb{F}_{q^{f_k}}$$

が成り立つ.

2.6 格子

m 次元ユークリッド空間を $\mathbb{R}^m$ と表す．$\mathbb{R}^m$ における n 個 $(m \geq n)$ の線形独立なベクトル $b_1, \ldots, b_n$ のすべての整数係数の線形結合の集合

$$\mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z} \right\}$$

のことを $\mathbb{R}^m$ における格子という．m を次元，n を階数といい，$B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ を格子基底, または単に基底と呼ぶ.

3. 既存研究

本章では，室井らによって提案された整数環上の部分格子を用いた，Ring-LWE 識別問題に対する攻撃を説明する．

Vol.2021-DPS-186 No.37
Vol.2021-CSEC-92 No.37
2021/3/15

3.1 部分格子

整数環 $R_q = R/qR$ は素イデアル分解を用いて，

$$R/qR = \mathbb{F}_q^{f_1} \times \ldots \times \mathbb{F}_{q^{f_k}} \ (f_1 \leq f_2 \leq \ldots \leq f_k)$$

と分解される．このとき，

$$\mathbb{F}_{q^{f_1}} \times \mathbb{F}_{q^{f_2}} \times \ldots \times \mathbb{F}_{q^{f_k}} = \langle 1, x, \ldots, x^{f_1-1} \rangle_{\mathbb{F}_q} \times \langle 1, x, \ldots, x^{f_2-1} \rangle_{\mathbb{F}_q} \times \ldots \times \langle 1, x, \ldots, x^{f_k-1} \rangle_{\mathbb{F}_q}$$

と表すことができ，それぞれの係数を格子の基底とみなすことができる．本節以降，基底の添え字 $\mathbb{F}_q$ は省略する．整数環上の部分格子を

$$\mathscr{L}_{i,j}^{(f_k)}/qR := \langle 1, x, \ldots, x^{f_1} \rangle \times \langle 1, x, \ldots, x^{f_2} \rangle \times \ldots \times \langle 1, x, \ldots, 0 \times x^i, \ldots, 0 \times x^j, \ldots, x^{f_k} \rangle$$

と定義する．$\mathscr{L}_{i,j}^{(f_k)}$ は f_k 番目のイデアルの i 番目と j 番目の基底がない格子を表している．最も大きな相対次数を $f_k = d$ とする．本章以降では，部分格子の区別が必要でない場合，簡単に $\mathscr{L}$ と記載する．部分格子 $\mathscr{L}$ を用いて写像 ϕ を

$$\phi : R \to R/\mathscr{L} : a \mapsto a \bmod \mathscr{L}$$

と定義する．

3.2 部分格子攻撃

Ring-LWE サンプルに対して写像 ϕ を施すと，

$$\begin{aligned} \phi(b) &= \phi(as+e) \\ &= \phi(as) + \phi(e) \\ &= (a+\mathscr{L})(s+\mathscr{L}) + (e+\mathscr{L}) \end{aligned}$$

となる．このとき $(a+\mathscr{L})(s+\mathscr{L}) = as + a\mathscr{L} + s\mathscr{L} + \mathscr{L}^2$ であり，$a\mathscr{L} \subset \mathscr{L}$ かつ $s\mathscr{L} \subset \mathscr{L}$ であるとき，

$$\phi(as) + \phi(e) = \phi(a)\phi(s) + \phi(e)$$

と変形でき，格子 $\mathscr{L}$ 上の Ring-LWE サンプルとみなすことができる．ここで $a\mathscr{L} \subset \mathscr{L}$ をみたす a がサンプリングできたと仮定すると，$s' = \phi(s)$ を予想し，

$$b - as' = a(s - s') + e \equiv e \bmod \mathscr{L}$$

を計算することができる．m 個のサンプル $(a_i, b_i = a_i s + e_i)\ (1 \leq i \leq m)$ に対し，$\{e_i \bmod \mathscr{L}\}_{1 \leq i \leq m}$ が $R/\mathscr{L}$ で一様か χ^2 検定を用いて調べることで，与えられたサンプルが Ring-LWE サンプルか識別する．部分格子攻撃のアルゴリズムを Algorithm1 に示す．

Algorithm 1 一つのイデアルを用いた簡略化部分格子攻撃

Require: $10 \times q^2$ 個の Ring-LWE サンプル $(a, b = as + e)$，代数体を生成する既約多項式 f
Ensure: Ring-LWE サンプルと識別 or 識別不能

```
f_1,...,f_d ← f mod q で因数分解されたそれぞれの多項式で f_d が最も次数が高いもの
(b_1, b_2) ← f_d の任意の項の次数
for i ← 1 to q do
    for j ← 1 to q do
        f_d で生成されるイデアルの次数が b_1, b_2 の係数 ← (i, j), その他の係数 ← 0
        中国式剰余定理を用いて f_1,...,f_d より s' を生成 {s' ← s mod L を予想する }
        χ2 ← 0
        for kk ← 1 to サンプル数 do
            e' ← b − a·s' mod f_d
            観測度数のリスト n に e' mod f_d の係数を一組として追加
        end for
        χ^2 ← Σ_{i=1}^{SampleNum} (n_i − E_i)^2 / E_i
        if χ^2 > χ^2_theory then
            攻撃成功
        else
            ランダムなサンプル or 識別不能
        end if
    end for
end for
```

4. 提案手法

本章では，3 章で説明した既存攻撃では用いられていない部分格子を用いて，$a\mathscr{L} \subset \mathscr{L}$ という条件を緩和する手法を説明する．$a\mathscr{L}_{2i}^{(d)} \subset \mathscr{L}_{2i}^{(d)}$ を満たすように，以下のように条件を仮定する．

- R/qR を素イデアル分解時に，最も次数が高いイデアル $\mathfrak{P}_k$ の次数が偶数のみである
- Ring-LWE サンプル a に対して，$a \bmod \mathfrak{P}_k$ の次数が偶数のみである．

4.1 部分格子生成

3 章の部分格子と同様に以下のように部分格子 $\mathscr{L}_{2i}^{(f_k)}$ を

$$\mathscr{L}_{2i}^{(f_k)}/qR := \langle 1, x, \ldots, x^{f_1-1} \rangle \times \langle 1, x, \ldots, x^{f_2-1} \rangle \times \ldots \times \langle 1, 0 \times x, x^2, \ldots, x^{2i}, 0 \times x^{2i+1}, \ldots \rangle$$

と定義する．格子 $\mathscr{L}_{2i}^{(f_k)}$ は f_k 番目のイデアルの偶数番目の基底を持つ格子を表している．

4.2 攻撃手順

既存研究と同様に $s - s' \in \mathscr{L}$ であるような s' を探索し，$b - as'$ を計算することで $e \bmod \mathscr{L}$ を得る．このとき，エラーの部分情報である $e \bmod \mathscr{L}$ は次のように表される．

$$e \bmod \mathscr{L}_{2i} = \langle 0, 0 \times x, \ldots, 0 \times x^{f_1-1} \rangle \times \langle 0, 0 \times x, \ldots, 0 \times x^{f_2-1} \rangle \times \ldots \times \langle 0, f_1 \times x, 0 \times x^2, \ldots, 0 \times x^{2i}, e_{2i+1} \times x^{2i+1}, \ldots, \rangle$$

つまり，e の次数が奇数である項の係数を取得することができる．既存研究では二つの係数をペアとして検定を行っているため，本攻撃でも，添え字の小さなものから二つを一組としてペアを生成し χ^2 検定を行った．

4.3 計算機実験

本節では，室井らが [8] において Hao Chen[7] が攻撃対象とした代数体への攻撃と，アイゼンシュタインの既約判定法を用いてランダムに生成した既約多項式による代数体への攻撃，さらには前節で述べた部分格子 $\mathscr{L}_{2i}^{(d)}$ を用いた攻撃の計算機実験について示す．表 1 と表 2 に Hao Chen が攻撃対象とした代数体に対しての攻撃結果を，表 3 と表 4 にアイゼンシュタインの既約判定法を用いて生成した代数体に対しての攻撃結果を示す．また，表 5 と表 6 に部分格子 $\mathscr{L}_{2i}^{(d)}$ を用いた攻撃結果を示す．

既存研究，本研究共に，$e \bmod \mathscr{L}$ が一様分布と識別可能であることが重要であると考え，本来必要なシークレット s の探索を省略し，エラー e に直接攻撃を行っている．また，検定に用いるサンプルは $10q^2$ 個としているが，$\mathscr{L}_{2i}^{(d)}$ を用いた攻撃においては，一つの Ring-LWE サンプルから複数のエラーの観測度数が得られるため，観測度数が $10q^2$ に近くなるように Ring-LWE サンプルを使用している．また，χ^2 検定の優位水準 α は 0.005 としている．本研究においてはモジュラス q を固定しているが，既存研究においては代数体を生成する既約多項式が固定されているため，相対次数が大きいイデアルが存在するようにモジュラス q を変化させている．実験環境は以下の通りである．

- CPU
  Intel(R) Xeon(R) CPU E7-4830 v4 @ 2.00GHz
- MEMORY
  3.0T
- OS
  Ubuntu 16.04.7 LTS
- プログラミング言語
  SageMath version 7.5.1

表 1 エラーに対する攻撃

q	d	攻撃数	非一様分布	成功確率 (%)
233	69	2346	2346	100
229	68	2278	2278	100
181	67	2211	2211	100
271	64	2016	224	11.0
149	61	1953	2	0.3
383	58	1830	0	0
367	54	1431	0	0

表 2 一様分布に対する攻撃

q	d	攻撃数	非一様分布	成功確率 (%)
233	69	2346	0	100
229	68	2278	0	100
181	67	2211	1	99.9
271	64	2016	0	100
149	61	1953	2	99.9
383	58	1830	1	99.9
367	54	1431	1	99.9

表 3 エラーに対する攻撃

q	d	攻撃数	非一様分布	成功確率 (%)
149	69	2346	2346	100
149	68	2278	2278	100
149	67	2211	2211	100
149	66	2145	1337	62.3
149	65	2080	265	12.7
149	64	2016	60	3.0
149	63	1963	11	0.6
149	61	1830	2	0.1
149	59	1711	0	0
149	54	1431	2	0.1

表 4 一様分布に対する攻撃

q	d	攻撃数	非一様分布	成功確率 (%)
149	69	2346	0	100
149	68	2278	0	100
149	67	2211	1	99.9
149	66	2145	1	99.9
149	65	2080	1	99.9
149	64	2016	1	99.9
149	63	1963	2	99.9
149	61	1830	1	99.9
149	59	1711	1	99.9
149	54	1431	0	100

表 5 エラーに対する攻撃

q	d	攻撃数	非一様分布	成功確率 (%)
149	70	10	10	100
149	68	10	10	100
149	66	10	10	100
149	64	10	10	100
149	62	10	10	100
149	60	10	10	100
149	58	10	10	100
149	56	10	10	100

表 6　一様分布に対する攻撃

q	d	攻撃数	非一様分布	成功確率 (%)
149	70	10	0	100
149	68	10	0	100
149	66	10	0	100
149	64	10	0	100
149	62	10	10	0
149	60	10	10	0
149	58	10	10	0
149	56	10	10	0

以上の実験結果から，アイゼンシュタインの既約判定法を用いて生成された既約多項式によって構成される代数体上の Ring-LWE 問題に対して，既存攻撃が有効であることがわかる．また，一部の基底の次数が偶数である場合も，攻撃が成功していることがわかる．しかし，最大の相対次数が減少するにつれて攻撃の成功率が低下しており，今後の課題として，より小さな相対次数に対しても攻撃が成功するような格子基底の発見があげられる．

5. 既存攻撃と本攻撃の比較

本章では，既存攻撃と本攻撃について，攻撃に必要な条件である $a\mathscr{L} \subset \mathscr{L}$ を満たす a を取得するための計算量を比較する．

5.1 既存攻撃

既存攻撃に用いられている格子 $\mathscr{L}^d_{i,j}$ は i 番目と j 番目の以外の基底をもつ．また, サンプル a が定数項が 0 でないとき，$a\mathscr{L}$ が i 番目または j 番目の項に基底を持つ．よって，サンプル a が最も大きな相対次数を持つ剰余体で定数項であること，つまり以下のように

$$a \bmod \mathscr{L}^{(d)}_{i,j} \in \mathbb{F}_{q^{f_1}} \times \mathbb{F}_{q^{f_2}} \times \ldots \times \mathbb{F}_q$$

と分解されるとき，$a\mathscr{L} \subset \mathscr{L}$ を満たす．また，このようなサンプルが存在する確率は

$$\frac{q}{q^d} = \frac{1}{q^{d-1}}$$

であるから，検定に必要なサンプルを得るためには $10q^2 \times q^{d-1} = 10q^{d+1}$ 個の Ring-LWE サンプルを取得する必要がある．

5.2 本攻撃

本攻撃で用いた格子 $\mathscr{L}^{(d)}_{2i}$ は最も相対次数の高い剰余体の偶数次数の係数を基底としている．サンプル a が素イデアル分解時に以下のように

$$a \bmod \mathscr{L}^{(d)}_{2i} \in \langle 1, x, \ldots, x^{f_1} \rangle \times \langle 1, x, \ldots, x^{f_2} \rangle \times \ldots, \times \langle 1, 0 \times x, x^2, \ldots, x^{2i}, 0 \times x^{2i+1}, \ldots, \rangle$$

と表されるとき，$a\mathscr{L} \subset \mathscr{L}$ を満たす．また，このようなサンプルが存在する確率は

$$\frac{q^{\frac{d}{2}}}{q^d} = \frac{1}{q^{\frac{d}{2}}}$$

である．また本攻撃では，一つの Ring-LWE サンプルから，検定に必要なサンプルを複数得ることができる．つまり，$\frac{10q^2}{\frac{d-1}{4}} \times q^{\frac{d}{2}} = \frac{40q^{\frac{d}{2}-1}}{d-1}$ 個のサンプルを取得する必要がある．

6. おわりに

本論文では，Ring-LWE 識別問題への整数環上の部分格子を用いた既存攻撃に対して，必要なサンプル条件の緩和のために，新たな格子基底の取り方を提案した．また，実験解析を行い，新たに用いた部分格子による攻撃が有効であることを示した．しかし，シークレット s の探索範囲が広がるという問題点が存在している．また既存攻撃と同様に，用いる素イデアルの相対次数が高い必要がある．

今後の課題として，シークレット s の探索範囲の減少や，攻撃に用いる素イデアルの相対次数の減少，円分体などのその他の代数体への攻撃の適応などがあげられる．

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] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In Frank Thomson Leighton and Peter W. Shor, editors, *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El Paso, Texas, USA, May 4-6, 1997*, pages 284–293. ACM, 1997.

[2] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 112–131. Springer, 1997.

[3] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

[4] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.

[5] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *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*, volume 6110 of *Lecture Notes*

in Computer Science, pages 1–23. Springer, 2010.

[6] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 505–524. Springer, 2011.

[7] Hao Chen. Sublattice attacks on ring-lwe with wide error distributions I. *IACR Cryptol. ePrint Arch.*, 2020:440, 2020.

[8] 室井 謙典, 奥村 信也, and 宮地 充子. 簡略化部分格子攻撃による ring-lwe 問題の実験解析. In *IEICE 2021. submitted.*