LWR問題解読のための サンプル増幅法を用いたBKWアルゴリズム

岡田 大樹[1]　高安 敦[2]　福島 和英[1]　清本 晋作[1]　高木 剛[2]

概要：Learning with Errors（LWE）問題，Learning with Rounding（LWR）問題の計算困難性は，次世代公開鍵暗号の構成などを目的として盛んに研究されている．LWE 問題を解く手法の一つとして，Blum-Kalai-Wasserman（BKW）アルゴリズムは広く研究されている．Duc らは，LWE 問題に対してサンプル増幅法を用いた BKW アルゴリズムが適用可能であることを示し，また，BKW アルゴリズムが LWR 問題にも適用できることを示している．本研究では，LWR 問題における丸め誤差の和の分布を解析的に求め，LWR 問題に適用可能であるサンプル増幅法を用いた BKW アルゴリズムを初めて提唱し，解読に必要となるパラメータの条件について解析を行った．

キーワード：LWE 問題，LWR 問題，BKW アルゴリズム，サンプル増幅法

BKW Algorithm for Solving LWR Problem Using Sample Amplification

Hiroki Okada[1]　Atsushi Takayasu[2]　Kazuhide Fukushima[1]　Shinsaku Kiyomoto[1]
Tsuyoshi Takagi[2]

1. はじめに

1.1 背景

2017 年 11 月には，アメリカ国立標準技術研究所（NIST）による次世代公開鍵暗号の標準アルゴリズムの選定が開始される予定であり，Learning with Errors（LWE）問題及び Learning with Rounding（LWR）問題の求解アルゴリズムとその計算量は，次世代公開鍵暗号の設計や安全性評価を目的として，広く研究されている．LWE 問題は，Regev [1] によって初めて定義され，Learning Parity with Noise (LPN) 問題の拡張とみなすことができる．LWE 問題の解読者は，LWE オラクルから $\mathbb{Z}_q$ 上で一様にランダムなベクトル $\boldsymbol{a}_j \in \mathbb{Z}_q^n$ と，それに固定の秘密ベクトル $\boldsymbol{s} \in \mathbb{Z}_q^n$ の内積にノイズ ν_j を付与されたサンプル $(\boldsymbol{a}_j, \langle \boldsymbol{a}_j, \boldsymbol{s} \rangle + \nu_j)$ から，$\boldsymbol{s}$ を解読することを目的とする．LPN 問題では，$q = 2$ となり，ノイズの種類も異なっている．

LWR 問題は，Banerjee ら [2] によって初めて提唱された．LWR 問題は LWE 問題におけるノイズ付加の部分を決定的な丸め演算に置き換えた問題と捉えられる．LWR 問題を応用した暗号アルゴリズムは，LWE 問題を応用したものと比較し，小さな法 p を用いた演算が可能であり，エラーサンプリングの処理も削減できるため，高速かつ軽量な実装を実現できる．その中には，擬似乱数関数 [2] や，lossy trapdoor functions [3]，key-homomorphic PRFs [4]，暗号アルゴリズム [5] などが挙げられ，LWR 問題を応用した暗号アルゴリズムの研究も注目を集めている．その一方，LWR 問題の困難性の評価に関する研究は，LWE 問題と比較すると十分には行われていない．

本研究においては，もともとは LPN 問題の求解を目的として考案された，Blum-Kalai-Wasserman（BKW）アルゴ

[1] 株式会社 KDDI 総合研究所
KDDI Research, Inc.
[2] 東京大学大学院情報理工学研究科数理情報学専攻
Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo

リズム [6] について着目する．Regev [1] らは，BKW アルゴリズムを用いて LWE 問題を計算量 $q^{O(n/\log n)}$ で解読できることを言及し，その後 Albrecht ら [7] が具体的な構成を示した．

多くの LPN 問題，LWE 問題，LWR 問題を応用した暗号技術においては，オラクルから得られるサンプル数に限りがあるのに対し，BKW アルゴリズムは多数のサンプルを必要とし，LPN 問題及び LWE 問題を解くためにはそれぞれ $2^{O(n/\log n)}$ 個及び $q^{O(n/\log n)}$ 個のサンプルをオラクルから取得する必要があるという欠点がある．Lyubashevsky [8] は，LPN 問題を解くために必要なサンプル数を削減し，オラクルから取得したサンプルをランダムに線型結合するサンプル増幅法を提案した．この手法では，計算時間は $2^{O(n/\log\log n)}$ と増えるものの，オラクルから取得するサンプル数は任意の定数 $\varepsilon > 0$ に対して $n^{1+\varepsilon}$ となる．その後 Duc ら [9] は，LWE 問題を解くためのサンプル増幅法を解析し，$O(nq)$ 個のサンプルのみを用いて解けることを示した．そして，上中谷らは [10]，BKW アルゴリズムとサンプル増幅法の挙動に関わる重要なパラメータであるブロック数と線形結合数の設定をより詳細に解析することで，必要なサンプル数は $O(n\log q)$ で，LWE 問題が解読可能であることを示した．また，Duc らは [9] において，LWR 問題を解くための BKW アルゴリズムを初めて提案した．

LWE 問題は，最悪時格子問題からの帰着が証明されている．そして，LWR 問題は LWE 問題からの帰着が証明されており [2], [3]，そのことを計算困難性の解析的な根拠としているといえる．しかしながら，LWE 問題から LWR 問題へと帰着する際にはオラクルから得るサンプル数に制限がある [2], [3]．よって，LWR 問題の計算困難性評価のためにその求解アルゴリズムを考える時には，サンプル数を少なくする必要がある．つまり，以上のことから，LWR 問題を解くための BKW アルゴリズムに対してのサンプル増幅法は特に必用な手法である．

1.2 研究成果

本研究で我々は，Duc ら [9] の，LWE 問題を解くためのサンプル増幅法を用いた BKW アルゴリズムと，LWR 問題を解くための BKW アルゴリズムと，上中谷らのサンプル増幅法を用いた BKW アルゴリズムの解析に基づき，LWR 問題を解くためのサンプル増幅法を用いた BKW アルゴリズムについて研究を行い，以下の結果を得た

- LWR 問題を解くための BKW アルゴリズムを解析し，計算量を最小化する入力パラメータであるブロック分割数 a の最適値を求め，オラクルから受け取るサンプル数 $m = q^{O(n/\log n)}$，計算量が $t = q^{O(n/\log n)}$ で解けることを示す．
- 導出した LWR 問題の最小計算量と LWE 問題の最小計算量を比較し，BKW アルゴリズムによる同一の解読計算量を持つ LWE 問題と LWR 問題のパラメータ間の関係式を導出する．
- サンプル増幅法が LWR 問題を解くための BKW アルゴリズムにおいても適用可能であることを，詳細な構成とともに初めて示し，計算量は少なくともサンプル増幅法を用いない場合よりも大きくなるが，オラクルから受け取るサンプル数 $m = O(n\log q)$ で解くことができることを示す．
- サンプル増幅法において，線形結合の結合数 w とサンプル数 m を決定するパラメータ β について詳細な解析を初めて行い，解読の成功率とサンプル数のトレードオフの中での最適な値を求め，オーダーは変わらないがサンプル数，計算量をより少なくできることを示す．また，この結果は LPN 問題，LWE 問題におけるサンプル増幅法にも適用可能である．

1.3 構成

本論文の構成は以下のとおりである．

- 2 章: 表記，定義などを紹介する．
- 3 章: LWR 問題を解くための BKW アルゴリズムを解析する．
  - 3.1 節: BKW アルゴリズムを紹介する．
  - 3.2 節: アルゴリズムの計算量，必要サンプル数を解析する．
  - 3.3 節: 計算量を最小化するパラメータ a を求める．
- 4 章: サンプル増幅法を用いた場合の，LWR 問題を解くための BKW アルゴリズムを解析する．
  - 4.1 節: サンプル増幅法の適用方法を説明する．
  - 4.2 節: サンプル増幅法適用時のアルゴリズムの計算量，必要増幅サンプル数を解析する．
  - 4.3 節: 計算量を最小化するパラメータ a を求める．
- 5 章: サンプル増幅法におけるパラメータ β の解析を行い，必要なサンプル数 m をより少なくするための最適値を求める．
- 6 章: 計算量最小時における，サンプル増幅法を用いた場合と用いない場合の計算量，必要サンプル数などを計算する．
- 7 章: 本論文をまとめる．

2. 準備

2.1 表記・定義

- $i := \sqrt{-1}$
- ln は自然対数とし，log は底が 2 の対数とする．
- $\boldsymbol{s} \xleftarrow{U} \mathcal{S}$: $\boldsymbol{s}$ は集合 $\mathcal{S}$ から一様にランダムに生成されたベクトル
- $\langle \boldsymbol{a_j}, \boldsymbol{s} \rangle_q := \langle \boldsymbol{a_j}, \boldsymbol{s} \rangle \pmod q$
- $\lceil x \rfloor$: $x \in \mathbb{R}$ に最も近い整数 (最も近い整数が 2 つある

場合は，小さい方の整数を返す．)

- $\mathrm{Hw}(\boldsymbol{x})$: ベクトル $\boldsymbol{x}$ のハミング重み
- $\theta_p := e^{\frac{2\pi i}{p}}$
- W : ランベルトの W 関数 [11]

2.2 LWR 問題

定義 1. (LWR オラクル $\mathcal{O}_{\boldsymbol{s},p}$) n, q を自然数とする．ベクトル $\boldsymbol{s} \in \mathbb{Z}_q^n$ と *Learning with Rounding (LWR)* オラクル $\mathcal{O}_{\boldsymbol{s},p}$ は以下のサンプルを出力する．

$$\left\{ (\boldsymbol{a}, c) = \left(\boldsymbol{a}, \left\lceil \frac{p}{q} \langle \boldsymbol{a}_j, \boldsymbol{s} \rangle_q \right\rfloor \right) \;\middle|\; \boldsymbol{a} \xleftarrow{U} \mathbb{Z}_q^n \right\}.$$

定義 2. (LWR 問題)．*LWR* 問題とは，*LWR* オラクル $\mathcal{O}_{\boldsymbol{s},p}$ から得た m 個のサンプル $(\boldsymbol{a}_j, c_j)$ からベクトル $\boldsymbol{s}$ を求める問題である．

2.3 サンプル増幅法に用いるハッシュ関数

本研究では，サンプル増幅法における線形結合に用いるハッシュ関数を上中谷ら [10], Lyubashevsky ら [8] と同様にして定義する．$x = (x_1, ..., x_N) \in \{0,1\}^N$ と $A \xleftarrow{U} \mathbb{Z}_q^{n \times N}$: の j 列目の列ベクトル $\boldsymbol{a}_j$ を入力として，$\mathbb{Z}_q^n$ 上のベクトルを出力するハッシュ関数を以下のように定義する．

$$h_A(x) = \sum_{j=1}^{N} x_j \boldsymbol{a}_j \tag{1}$$

3. BKW アルゴリズムの解析

本章では，本研究が対象とする LWR 問題を解くための BKW アルゴリズムについて紹介する．このアルゴリズムにおいて，計算量を最適化するパラメータ a の最適値を求め，またその時のサンプル数及び計算量のオーダーを求める．

3.1 Duc らのアルゴリズム [9]

本節では，LWR 問題を解くための Duc ら [9] のアルゴリズムを紹介する．そのアルゴリズムは

- ステップ 1: サンプル簡約 (Sample reduction)，
- ステップ 2: 仮説検定 (Hypothesis testing)，
- ステップ 3: 後退代入 (Back substitution)

の 3 つに分けることができる．LWE 問題と LWR 問題は類似しており，そのアルゴリズムは，LWE 問題を解くための BKW アルゴリズムのステップ 3 の尤度関数が LWE 問題を解く場合の BKW アルゴリズムのものと異なっているのみである．アルゴリズムの概要については，Algorithm 1 のとおりである．なお，簡単のため，以下では $ab = n$ のときのみを考える．

ステップ 1: 長さ n のベクトル $\boldsymbol{a}_j$ を a 等分して長さ b のブロックに分割する．$l = 0, \ldots, a-2$ の順にしてガウスの消去法と同様に，第 $a-l$ ブロックを $\boldsymbol{0}$ にしていくことで，最終的に次元 n の LWR 問題を次元 b の LWR 問題へと簡約化する．その際に，第 $a-l$ ブロックを $\boldsymbol{0}$ にできないサンプルが最大で $\frac{q^b-1}{2}$ 個存在する．よってステップ 1 で出力される最悪の場合の (最小の) サンプル数を m' とおくと，

$$m' = m - (a-1)\frac{q^b - 1}{2}$$

となる．

ステップ 2: ステップ 1 で簡約化された LWR 問題の解を以下の尤度関数を用いて推測する．その尤度関数はステップ 1 で出力された m' 個のサンプル $(\overline{\boldsymbol{a}}_j, \overline{c}_j)$ を用いた，

$$f(\boldsymbol{y}) := \sum_{j=1}^{m'} \mathbb{1}_{\{\overline{\boldsymbol{a}}_j, \boldsymbol{y}\}} \theta_p^{\overline{c}_j}$$

を離散フーリエ変換して得られる

$$\hat{f}(\boldsymbol{z}) := \sum_{j=1}^{m'} \theta_p^{-(\langle \overline{\boldsymbol{a}}_j, \boldsymbol{z} \rangle \frac{p}{q} - \overline{c}_j)}$$

である．である．ここで，

$$\mathbb{1}_{\{\overline{\boldsymbol{a}}_j, \boldsymbol{y}\}} = \begin{cases} 1 & (\overline{\boldsymbol{a}}_j = \boldsymbol{y}) \\ 0 & (\overline{\boldsymbol{a}}_j \neq \boldsymbol{y}) \end{cases}$$

である．この尤度関数を全ての $\boldsymbol{y} \in \mathbb{Z}_q^b$ について総当たりで計算し，最大となる入力を求めその結果を部分的な解 $\boldsymbol{s}_{(1,b)}$ として出力する．

ステップ 3: 次の部分的な解 $\boldsymbol{s}_{(b+1,2b)}$ を求めるために $\boldsymbol{s}_{(1,b)}$ を利用して c_j を修正し，ステップ 1 に戻る．

上記のステップ 1, 2, 3 を a 回繰り返し，部分的な解を結合することで，$\boldsymbol{s}$ を求めることができる．

Algorithm 1 LWR 問題に対する BKW アルゴリズム [9]

input: $ab = n$ を満たす自然数 a, b
　　自然数 m

ステップ 1: サンプル整形

1: m 個のサンプル $(\boldsymbol{a}_j, c_j)$ を LWR オラクル $\mathcal{O}_{\boldsymbol{s},p}$ から得る．(その集合を $\mathcal{S}$ とする．)
2: **for** $l = 0$ to $a-2$ **do**
3: 　$\mathcal{S}' \leftarrow \phi$ (ϕ : 空集合)
4: 　**repeat**
5: 　　$\mathcal{S}$ からサンプル $(\boldsymbol{a}, c)$ を取り出す．
6: 　　**if** $\boldsymbol{a}$ の第 $a-l$ ブロックが $\boldsymbol{0}$ **then**
7: 　　　$\mathcal{S}' \leftarrow \mathcal{S}' \cup (\boldsymbol{a}, c)$
8: 　　**else if** $\mathcal{T}^l$ に $\boldsymbol{a}$ の第 $a-l$ ブロックの値と同じ $\pm\boldsymbol{a}'$ が存在する **then**
9: 　　　$\mathcal{S}' \leftarrow \mathcal{S}' \cup (\boldsymbol{a} \mp \boldsymbol{a}', c \mp c')$
10: 　　**else**
11: 　　　$\mathcal{T}^l \leftarrow \mathcal{T}^l \cup (\boldsymbol{a}, c)$
12: 　　**end if**
13: 　**until** $\mathcal{S} == \phi$
14: 　$\mathcal{S} \leftarrow \mathcal{S}'$
15: **end for**

ステップ 2: 仮設検定

1: $f(\boldsymbol{y}) := \sum_{j=1}^{|\mathcal{S}|} \mathbb{1}_{\{\overline{\boldsymbol{a}}_j = \boldsymbol{y}\}} \theta_p^{c_j}$ の離散フーリエ変換 $\hat{f}(\boldsymbol{z})$ を計算
2: return argmax $\mathrm{Re}(\hat{f}(\boldsymbol{z}))$

ステップ 3: 後退代入

1: $\boldsymbol{s}_{(1,b)}$ を利用して c_j を修正し，ステップ 1 に戻る．

3.2 サンプル数と計算量の解析

本節では，上中谷ら [10] が，Duc ら [9] の LWE 問題対して行ったのと同様にして，LWR 問題を解くための BKW アルゴリズムの対してサンプル数と計算量についての解析を行い，以下の定理を示す．

定理 3. (BKW アルゴリズムのサンプル数と計算量) a, b は $ab = n$ を満たす自然数とする．$\mathcal{O}_{\boldsymbol{s},p,\chi}$ の *LWR* 問題に対して，

- サンプル数：$m = \mathrm{poly}(q^{n/a}, (R_{q,p})^{-2^a})$
- 計算時間：$t = \mathrm{poly}(q^{n/a}, (R_{q,p})^{-2^a})$

で解くことができるアルゴリズムが存在する．ただし，$R_{q,p}$ は以下のように定義された関数である．

$$R_{q,p} := \frac{\sin\left(\frac{\pi}{p}\right)}{q\sin\left(\frac{\pi}{pq}\right)} \tag{2}$$

定理 3 を証明するために，以下の補題 4，5 を利用する．

補題 4. ([9] の Theorem 23.) *LWR* 問題に対して *BKW* アルゴリズムが解を出力しない確率，すなわち $\mathrm{argmax}_{\boldsymbol{z}}\mathrm{Re}\left(\hat{f}(\boldsymbol{z})\right) \neq \boldsymbol{s}_{(1,b)}$ となる確率を ϵ_f とすると，*LWR* 問題を解くのに必要なサンプル数を $\hat{m}$ は

$$\hat{m} = 8\ln\left(\frac{q^b}{\epsilon_f}\right)\left((R_{q,p})^{2^{a-1}} - \left(\frac{3}{p}\right)^{2^{a-1}}\right)^{-2} + (a-1)\frac{q^b-1}{2} \tag{3}$$

となる．

補題 5. p が十分に大きい時，以下が成り立つ．

$$\left((R_{q,p})^{2^{a-1}} - \left(\frac{3}{p}\right)^{2^{a-1}}\right)^{-2} \simeq (R_{q,p})^{-2^a}$$

Proof. 上式の両辺の逆数を取り，$X =$ (右辺) $-$ (左辺) とおき，テイラー展開より，

$$X = 2\left(\frac{3}{p}\right)^{2^{a-1}} - O\left(\frac{1}{p^{2^a}}\right)$$

が成りたつ． □

Proof. (定理 3 の証明) 上中谷ら [10] が LWE 問題に対して解析した定理 12 と同様に下記の通りに証明できる．

以下では， $\boldsymbol{s}_{(1,b)}$ を解読するのに掛かる計算量を考える．補題 4 より，今，サンプル数 m は，$m = \hat{m}$ となる．よって，ステップ 1 によって出力されるサンプル数 m' は $m' = \hat{m} - (a-1)\frac{q^b-1}{2}$ である．

ステップ 1 では，長さ n の $\hat{m}$ 個のサンプルに対して $a-1$ 回演算を行うため，計算量は $t_1 = O(amn)$ である．ステップ 2 では $f(\boldsymbol{z})$ の最大値を総当たりで調べるため，計算時間は $t_2 = O(m'nq^b)$ である．ステップ 3 では m' 個のサンプルを修正するだけなので，の計算時間は $t_3 = O(m')$ である．

以上のことと，補題 5 より，s の全成分を求めるために必要な計算時間は $t = \mathrm{poly}(q^b, (R_{q,p})^{-2^a})$ となる． □

3.3 最小計算量の導出

本節では，BKW アルゴリズムの計算量を最小化する a の最適値を考える．またその最適な a の下での，BKW アルゴリズムの計算量を考える．ただし，ここで，$ab = n$ であり b については $b = n/a$ として導かれるため考慮しない．

補題 6.

$$\alpha_{\mathrm{lwr}} := \frac{\pi}{p\sqrt{6}} \tag{4}$$

とおいた時，p $(q > p)$ が十分大きい時，

$$\left((R_{q,p})^{2^{a-1}} - \left(\frac{3}{p}\right)^{2^{a-1}}\right)^{-2} \simeq \exp(\alpha_{\mathrm{lwr}}^2 2^a) \tag{5}$$

が成り立つ．

Proof. テイラー展開より，以下のようにかける．

$$R_{q,p} - \exp\left(-\alpha_{\mathrm{lwr}}^2\right) = \frac{\pi^2}{6p^2q^2} + O\left(\frac{1}{p^4}\right)$$

よって，$R_{q,p} \simeq \exp(-\alpha_{\mathrm{lwr}}^2)$ と近似できる．よって，これを補題 5 の式に代入することで，式 (5) が得られる □

定理 7. *(*最適なパラメータ a*) LWR* 問題において，計算量を最小化する，最適なパラメータ a は以下のように求められる．

$$a = \frac{1}{\ln 2}W\left(\frac{n\ln q\ln 2}{\alpha_{\mathrm{lwr}}^2}\right) \tag{6}$$

ここで，W はランベルトの W 関数である [11]

Proof. 定理 3 に補題 6 を適用することで，計算量のオーダーは，$\mathrm{poly}(q^{n/a}, \exp(\alpha_{\mathrm{lwr}}^2 2^a))$ となり，

$$\exp(\alpha_{\mathrm{lwr}}^2 2^a) = q^{n/a} \tag{7}$$

の時最小となると考えられる．ここで，

$$\begin{aligned} &\exp(\alpha_{\mathrm{lwr}}^2 2^a) = q^{n/a} \\ \Leftrightarrow\ & a = \frac{1}{\ln 2}W\left(\frac{n\ln q\ln 2}{\alpha_{\mathrm{lwr}}^2}\right) \end{aligned} \tag{8}$$

となる． □

また，ランベルトの W 関数の性質から，n あるいは q, p が十分に大きい時，最適な a は以下のように近似できる．

$$a \simeq \frac{1}{\ln 2}\left(\ln\left(\frac{n\ln q\ln 2}{\alpha_{\mathrm{lwr}}^2}\right) - \ln\ln\left(\frac{n\ln q\ln 2}{\alpha_{\mathrm{lwr}}^2}\right)\right)$$

この値を定理 3 の a に代入し，式 (5)，式 (7) を用いることで，以下の系が導かれる．

系 8. (最適なサンプル数と計算量) a, b は $ab = n$ を満たす自然数とする．$\mathcal{O}_{\boldsymbol{s},p}$ の *LWR* 問題に対し，

- サンプル数：$m = q^{O(n/\log n)}$
- 計算量：$t = q^{O(n/\log n)}$

で解くことができるアルゴリズムが存在する．

上の系は，α_{lwr} が $O(1)$ より小さい時において成立する．

3.4 LWR 問題と LWE 問題の解読計算量の比較

3.3 節の解析により，LWR 問題を BKW アルゴリズムで求解するための最小計算量は $\mathrm{poly}(q^b, \exp(\alpha_{\mathrm{lwr}}^2 2^a))$ である．一方で，上中谷ら [10] は，LWE 問題を BKW アルゴリズムで求解するための最小計算量を，$\alpha_{\mathrm{lwe}} = \frac{\sqrt{2}\pi\sigma}{q}$ とし，$\mathrm{poly}(q^b, \exp(\alpha_{\mathrm{lwe}}^2 2^a))$ と見積もっている．このため，式 (4) における $\alpha_{\mathrm{lwr}} = \alpha_{\mathrm{lwe}}$ とすることで，BKW アルゴリズムによる同一の解読計算量を有する LWR 問題と LWE 問題には，

$$2\sqrt{3}p\alpha = 1 \tag{9}$$

の関係式が成立することが示される．ここで，α は LWE 問題における相対エラーであり，LWE 問題の法 q と標準偏差 σ により，$\alpha = \sigma/q$ と定義される．

4. 提案手法

本章では，LWE 問題に対してサンプル増幅法を行った既存研究 [9], [10] を LWR 問題に適用し，LWR 問題を解くためのサンプル増幅法を用いた BKW アルゴリズム提案し，そのアルゴリズムに必要な計算量などを解析する．

4.1 サンプル増幅法

本節では，LWR 問題を解く為の BKW アルゴリズムへのサンプル増幅法の適用方法を説明する．まず，準備として，LWR 問題が以下のように置き換えられることを示す．

定義 9. (LWR オラクル $\mathcal{O}'_{\boldsymbol{s},p,\chi}$) n, q を自然数とする．ベクトル $\boldsymbol{s} \in \mathbb{Z}_q^n$ と *Learning with Rounding (LWR)* オラクル $\mathcal{O}'_{\boldsymbol{s},p,\chi}$ は以下のサンプルを出力する．

$$\left\{ (\boldsymbol{a}, c) = \left(\boldsymbol{a}, \frac{p}{q}\langle \boldsymbol{a_j}, \boldsymbol{s} \rangle_q + \xi \right) \;\middle|\; \boldsymbol{a} \xleftarrow{U} \mathbb{Z}_q^n,\ \xi \leftarrow \chi \right\}.$$

ただし，ノイズ ξ の分布 χ は以下の特性関数により定義される．

$$\phi_\chi(t) = \mathbb{E}\left[e^{it\xi}\right] = \frac{\sin\left(\frac{t}{2}\right)}{q\sin\left(\frac{t}{2q}\right)} \tag{10}$$

系 10. *LWR* オラクル $\mathcal{O}'_{\boldsymbol{s},p,\chi}$ の *LWR* 問題を解くことができるアルゴリズムは，*LWR* オラクル $\mathcal{O}_{\boldsymbol{s},p}$ の *LWR* 問題を解くことができる．

Proof. 今，LWR オラクル $\mathcal{O}_{\boldsymbol{s},p}$ からサンプル

$$(\boldsymbol{a}, c) = \left(\boldsymbol{a}, \left\lceil \frac{p}{q}\langle \boldsymbol{a_j}, \boldsymbol{s} \rangle_q \right\rfloor \right)$$

を受け取ったとする．$\overline{\xi}$ を以下のように定義すると，

$$\overline{\xi} = \left\lceil \frac{p}{q}\langle \boldsymbol{a}, \boldsymbol{s} \rangle_q \right\rfloor - \frac{p}{q}\langle \boldsymbol{a}, \boldsymbol{s} \rangle_q$$

Duc ら [9] の Lemma 19. より，$\overline{\xi}$ の従う分布 χ の特性関数は式 (10) の特性関数となることが求められる． □

よって，以下では，LWR オラクル $\mathcal{O}'_{\boldsymbol{s},p,\chi}$ の LWR 問題を解くことを考える．

定理 11. (サンプル増幅法) $w \in \mathbb{N}$, 定数 $\beta \in \mathbb{R}$ $(\beta > 1)$ とする．*LWR* オラクル $\mathcal{O}'_{\boldsymbol{s},p,\chi}$ から $m = wq^{\beta n/w}$ 個のサンプルを与えられた場合は，*LWR* オラクル $\mathcal{O}'_{\boldsymbol{s},p,\chi_w}$ から無制限にサンプルを与えられた場合に置き換えられる．ここで，分布 χ_w は，以下の特性関数により定義される．

$$\phi_{\chi_w}(t) = \mathbb{E}\left[e^{it\xi}\right] = \left(\frac{\sin\left(\frac{t}{2}\right)}{q\sin\left(\frac{t}{2q}\right)} \right)^w \tag{11}$$

Proof. まず，サンプル増幅により得た「増幅」サンプルと，LWR オラクルから得た「純粋な」サンプルが統計的に識別不可であることを，上中谷ら [10] の補題 17 の導出と同様にして証明する．LWR オラクルにクエリすることで得た m 個のサンプル $(\boldsymbol{a}_j, c_j)$ に対し，式 (1) と同様にハッシュ関数

$$\begin{cases} h_A(\boldsymbol{x}) = & \sum_{j=1}^m x_j \boldsymbol{a}_j \pmod q \\ h_c(\boldsymbol{x}) = & \sum_{j=1}^m x_j c_j \pmod p \end{cases} \tag{12}$$

と定義する．$j = 1, \ldots, M$ に対して，集合 $\mathcal{X} = \{x \in \{0,1\}^m | Hw(x) = w\}$ からランダムに選ばれた x_j を入力として，$(\hat{\boldsymbol{a}}_j, \hat{c}_j) = (h_A(\boldsymbol{x}_j), h_c(\boldsymbol{x}_j))$ を生成し，これを M 個の新しいサンプルとする．M 個のサンプルを入力として LWE 問題を解くアルゴリズムを動かしたとき，正しい解を出力すれば 1 を，出力しなければ 0 を出力する述語を g とする．上中谷ら [10] の補題 17 と同様にして，

$$\begin{aligned} &|\Pr[g((\hat{\boldsymbol{a}_1}, \hat{c}_1), \ldots, (\hat{\boldsymbol{a}}_{\boldsymbol{M}}, \hat{c}_M)) = 1] \\ &\quad -\Pr[g((\boldsymbol{a_1}, c_1), \ldots, (\boldsymbol{a_M}, c_M)) = 1]| \\ &\leq Mq^{-\frac{(\beta-1)n}{2}} \quad (:= \Delta_n \text{とする.}) \end{aligned} \tag{13}$$

となる．よって，$M < q^{-(\beta-1)n/2}$ となるように β を定めることで，n が十分大きいとき，Δ_n は指数的に 0 に近づく．(β の適切な取り方については，5 章を参照されたい．) よって，$m = wq^{\beta n/w}$ 個のサンプル (a_j, c_j) から生成した M 個のサンプル $(\hat{\boldsymbol{a}}_j, \hat{c}_j)$ を入力した場合と M 個のサンプル $(\boldsymbol{a}_j, c_j)$ を入力した場合の誤差は指数的に 0 になっていく．

次に，χ が χ_w と置き換わることを示す．式 (12) を以下のように変形することで，$\hat{c}_j$ は以下のようにかける，

$$\begin{aligned} \hat{c}_j &= \sum_{j \in \{j | x_j = 1\}} \left(\frac{p}{q}\langle \boldsymbol{a_j}, \boldsymbol{s} \rangle_q + \xi_j \right) \\ &= \frac{p}{q}\langle \hat{\boldsymbol{a}}_{\boldsymbol{j}}, \boldsymbol{s} \rangle_q + \sum_{j \in \{j | x_j = 1\}} \xi_j \pmod p \end{aligned}$$

ここで，$\hat{\xi}_j := \sum_{j \in \{j | x_j = 1\}} \xi_j$ と定義した時，ξ_j はそれぞれ独立同分布であることと，式 (10) から，その特性関数は，以下のように求められる．

$$\mathbb{E}\left[e^{it\hat{\xi}}\right] = \mathbb{E}\left[e^{it\left(\sum_{j\in\{j|x_j=1\}}\xi_j\right)}\right] = \prod_{j\in\{j|x_j=1\}}\mathbb{E}\left[e^{it\xi_j}\right] = \left(\frac{\sin\left(\frac{t}{2}\right)}{q\sin\left(\frac{t}{2q}\right)}\right)^w \quad \square$$

4.2 サンプル数と計算量の解析

前節の定理 11 より，サンプル増幅法を用いた場合は，ノイズの分布が異なる LWR オラクルを用いた場合に帰着できることが示された．よって， 3.2 節と同様にして，LWR 問題に対する BKW アルゴリズムにサンプル増幅法を適用した場合の必要なサンプル数及び計算量を求めることができ，以下の定理が示せる．

定理 12. *(サンプル増幅法を用いた場合のサンプル数と計算量)* $a, b, w \in \mathbb{N}$，$ab = n$ を満たす．また，$\beta \in \mathbb{R}$ が Δ_n を十分に小さくする様な β であるとする．*LWR* オラクル $\mathcal{O}_{\boldsymbol{s},p}$ の *LWR* 問題に対して，

- サンプル数*:* $m = wq^{\beta n/w}$,
- 計算量*:* $t = \mathrm{poly}(q^b, \exp(\alpha_{\mathrm{lwr}}^2 w 2^a))$

で解くことができるアルゴリズムが存在する．

Proof. サンプル増幅法を用いた場合に，式 (2) で定義される $R_{q,p}$ を以下で定義される $R_{q,p,w}$ に置き換えることで，サンプル増幅法を用いない場合に帰着することができる．

$$R_{q,p,w} := \phi_{\chi_w}\left(\frac{2\pi}{p}\right) = \left(\frac{\sin\left(\frac{\pi}{p}\right)}{q\sin\left(\frac{\pi}{pq}\right)}\right)^w$$

(ここで，ϕ_{χ_w} は式 (11) で定義される特性関数である．) つまり，サンプル増幅法において，LWR 問題を解くのに必要な「増幅後」のサンプル数を $\hat{M}$ とおくと，補題 3 の導出と同様にして、下記の通りに求められるのである．

$$\hat{M} = 8\ln\left(\frac{q^b}{\epsilon_f}\right)\left((R_{q,p,w})^{2^{a-1}} - \left(\frac{3}{p}\right)^{2^{a-1}}\right)^{-2} + (a-1)\frac{q^b-1}{2} \tag{14}$$

また，補題 6 と同様にして，p が十分に大きい時，以下が成立する．

$$\left((R_{q,p,w})^{2^{a-1}} - \left(\frac{3}{p}\right)^{2^{a-1}}\right)^{-2} \simeq (R_{q,p,w})^{-2^a} \simeq \exp(w\alpha_{\mathrm{lwr}}^2 2^a)$$

定理 3 の $R_{q,p}$ に上式右辺を代入し，定理 11，系 10 を適用することで証明できる． $\square$

4.3 最小計算量の導出

次に， 3.3 節と同様にして，サンプル増幅法を用いた場合のパラメータ a の最適値を考える．

式 (8) の導出と同様にして，定理 12 におけるパラメータ a の最適値は，

$$a = \frac{1}{\ln 2}W\left(\frac{n\ln q\ln 2}{w\alpha_{\mathrm{lwr}}^2}\right) \tag{15}$$

となる．今，サンプル数は $m = wq^{\beta n/w}$ であることから，最小の m とその時の w をそれぞれ $\tilde{m}, \tilde{w}$ とすると，

$$\begin{cases}\tilde{m} &= e\beta n\ln q\\ \tilde{w} &= \beta n\ln q\end{cases} \tag{16}$$

である．この $\tilde{w}$ を式 (15) に代入すると，以下のようになる，

$$\tilde{a} = \frac{1}{\ln 2}W\left(\frac{\ln 2}{\beta\alpha_{\mathrm{lwr}}^2}\right) \tag{17}$$

また，ランベルトの W 関数 [11] の性質より，α_{lwr}^2 が十分に小さい時，以下のように近似できる．

$$\tilde{a}' \simeq \frac{1}{\ln 2}\left(\ln\left(\frac{\ln 2}{\beta\alpha_{\mathrm{lwr}}^2}\right) - \ln\ln\left(\frac{\ln 2}{\beta\alpha_{\mathrm{lwr}}^2}\right)\right) \tag{18}$$

よって，以上より，以下の系が導かれる．

系 13. (サンプル増幅法を用いた場合の，最小サンプル数と計算量) a, b は $ab = n$ を満たす自然数とする．$\mathcal{O}_{\boldsymbol{s},p}$ の *LWR* 問題に対し，サンプル増幅法を用いることで，

- サンプル数：$m = \tilde{m} = e\beta n\ln q$
- 計算量：$t = q^{O(n/\tilde{a}')}$

で解くアルゴリズムが存在する．ただし，$\tilde{a}'$ は式 (18)，a_{lwr} は式 (4) のとおりである．

$\alpha_{\mathrm{lwr}} = 1/n^{\Omega(1)}$ の場合，

5. 最適なパラメータ β の解析

本節では，定理 12 における β について，サンプル数を更に最小化する最適値を初めて解析する．この最適値の解析は，LWE 問題の場合にも同様にして適用可能である．この β の設定については，LWE 問題において，Duc ら [9] は $\beta = 1$ としていたがそれでは式 (13) の右辺を小さくすることができないために誤りであり，上中谷ら [10] は $\beta = 2$ と固定している．

以下では，m, w は，m を最小とするように式 (16) により設定されていて $m = \tilde{m}, w = \tilde{w}$ とする．計算量を最小化するパラメータ a は式 (17) により与えられるが，より正確に，$a \in \mathbb{N}$ であることより，

$$a = \left\lfloor\frac{1}{\ln 2}W\left(\frac{\ln 2}{\beta\alpha^2}\right)\right\rfloor \tag{19}$$

とする．この時，$a \le \frac{1}{\ln 2}W\left(\frac{\ln 2}{\beta\alpha^2}\right)$ が成り立っているため，式 (8) の式変形と同様の変形を下から行うことで，

$$\exp(\alpha_{\mathrm{lwr}}^2 w 2^a) \le q^{n/a}$$

が成り立つことが示せる．式 (14) に上式を代入することで，

表 1　BKW アルゴリズムに必要なサンプル数 $\hat{m}$ と計算量 $\mathcal{C}$

				[増幅無し]			[$\beta=2$]				[$\beta=\tilde{\beta}$]				
	n	q	p	a	$\log(\hat{m})$	$\log(\mathcal{C})$	a	$\log(\hat{m})$	$\log(\mathcal{C})$	$\log(\Delta_n)$	a	$\log(\hat{m})$	$\log(\mathcal{C})$	β	$\log(\Delta_n)$
type (a)	64	$\approx 2^{29}$	733	24	82.64	92.2	13	8.84	123.4	-795.7	14	8.29	124.7	1.16	-25.5
	80	$\approx 2^{31}$	1151	25	95.01	102.1	14	9.13	162.0	-1063.9	15	8.57	161.8	1.14	-20.1
	96	$\approx 2^{32}$	1663	26	99.93	108.1	15	9.36	202.3	-1345.1	16	8.79	201.9	1.13	-10.2
	112	$\approx 2^{33}$	2287	28	137.68	144.7	16	9.56	243.9	-1637.3	17	8.98	211.2	1.12	-29.8
	128	$\approx 2^{34}$	3023	29	149.12	159.9	17	9.72	253.2	-1973.6	18	9.14	254.9	1.12	-13.7
type (b)	64	9461	13	12	68.79	75.8	3	8.07	281.8	-145.2	4	7.80	216.9	1.53	-12.6
	80	14867	13	12	85.62	92.3	3	8.34	365.1	-194.0	4	8.07	283.1	1.52	-13.0
	96	21611	13	12	117.66	124.0	3	8.56	465.8	-230.3	4	8.28	351.7	1.52	-13.3
	112	29717	13	13	124.88	134.1	3	8.74	555.0	-282.3	4	8.47	422.4	1.52	-13.6
	128	39241	13	13	139.93	147.2	3	8.90	646.3	-335.7	4	8.63	494.9	1.51	-13.8

$$\hat{M} \leq 8\ln\left(\frac{q^{n/a}}{\epsilon_f}\right) q^{n/a} + (a-1)\frac{q^{n/a}-1}{2} \tag{20}$$

と書ける．q, n が十分大きい場合に，式 (20) は以下のように近似できる．

$$\hat{M} \leq 8\ln\left(\frac{q^{n/a}}{\epsilon_f}\right) q^{n/a}$$

上式のを $\hat{M}$ を，式 (13) の M に代入すると，式 (13) の右辺 Δ_n は以下のように評価できる．

$$\Delta_n \leq \left(8\ln\left(\frac{q^{n/a}}{\epsilon_f}\right)\right) \cdot q^{n(\frac{1}{a}-\frac{(\beta-1)}{2})}$$

ここで，上式の右辺の上界を ϵ_d $(\ll 1)$ とおき，以下のように β を評価することができる．

$$\left(8\ln\left(\frac{q^{n/a}}{\epsilon_f}\right)\right) \cdot q^{n(\frac{1}{a}-\frac{(\beta-1)}{2})} < \epsilon_d$$

$$\Leftrightarrow \quad \beta > 1 + \frac{2}{a} + 2\frac{\ln\left(\frac{8}{\epsilon_d}\ln\left(\frac{q^{n/a}}{\epsilon_f}\right)\right)}{n\ln q} \tag{21}$$

ただし，上式において，a は β に依存していることに注意が必要である．

この評価式を満たす中で β をできるだけ小さくすることで，必要なサンプル数 $\hat{m}$ を小さくすることができる．また，式 (17) より，β を小さくすることで，(a の整数化により無効化される場合はあるが，) a が大きくなり，つまり $b = n/a$ が小さくなり．影響計算量も小さくなることが期待できる．

6. 実験

サンプル増幅法を用いた場合の BKW アルゴリズムかかる計算量を計算し，**表 1** に載せた．その計算量は，Duc ら [9] の定理 17 と同様に計算でき，$\mathcal{C} = c_1 + c_2 + c_3 + c_4$ とおくと，以下のようにして計算できる．

$$\mathcal{C} = \frac{1}{4}(a-2)(a-1)(2b+1)(q^b-1) + nq^b\log(q) + \sum_{j=0}^{a-1} m'_{j,\epsilon_f}\left(\frac{a-1-j}{2}(n+2)+2\right) \tag{22}$$

ただし，

$$m'_{j,\epsilon_f} := 8\ln\left(\frac{q^b}{\epsilon_f}\right)\left((R_{q,p,w})^{2^{a-1-j}} - \left(\frac{3}{p}\right)^{2^{a-1-j}}\right)^{-2}$$

である．

6.1 概要

n, q, p については，Duc ら [9] の Table 2. における設定方法と同じである．つまりここで，type (a) のパラメータについては，

$$q = \text{nextprime}(\lceil(2\sigma n)^3\rceil), \quad p = \text{nextprime}(\lceil\sqrt[3]{q}\rceil)$$

type (b) については，

$$p = 13, \quad q = \text{nextprime}(\lceil 2\sigma np\rceil)$$

であり，上記の両方において，

$$\sigma = \frac{n^2}{\sqrt{2\pi n}(\log(n))^2}$$

である．これらは，Alwen ら [3] Corollary 4.2 に基づいており，type (a) は，$\text{LWR}_{n,m,q,p}$ 仮定を保つ中で，q に対する計算量の割合 (Efficiency) を最大化するパラメータであり，type (b) は，$\text{LWR}_{n,m,q,p}$ 仮定を保つ中で，ノイズの分散の大きさに対する q の割合 (Modulus to error ratio) を最小とするパラメータである．しかしここで，Duc [9] らと同様にして，Alwen [3] らの条件から m については除外していることに注意する必要がある．

[増幅無し] の場合は a については式 (6) の a に床関数を施し整数化して計算し，$\hat{m}$ は式 (3), $\mathcal{C}$ は式 (22), により計算した．サンプル増幅ありの場合は，a については，[$\beta=2$] の場合は式 (19) を用いて計算し，[$\beta=\tilde{\beta}$] の場合は，式 21 を満たす条件中で β を最小にするようにして a, β を数値計算により設定した．$\hat{m}$ は式 (16), $\mathcal{C}$ は式 (22), そして，Δ_n は式 (13) で定義されているように，$\Delta_n = \hat{M}\cdot q^{-\frac{(\beta-1)n}{2}}$ である．ここで，$\hat{M}$ は式 (14) により計算する．また，$\epsilon_f = 0.001, \epsilon_d = 2^{-3}$ としている．

6.2 結果

サンプル数については，[増幅無し] の場合に比べて $[\beta = 2]$, $[\beta = \tilde{\beta}]$ の場合の $\hat{m}$ は明らかに少なくなることが分かる．また，$[\beta = \tilde{\beta}]$ の場合，結果の全てにおいて $\hat{\beta} < 2$ であり，$\hat{m} = e\beta n \ln q$ であることからも明らかであるが，$\beta = 2$ の時よりも必要なサンプル数 $\hat{m}$ が少なくなっていることが確認できる．また，それと同時に Δ_n についても全て ϵ_d よりも小さくなっており，式 (13) の右辺は十分に収束する様な β に設定できていることが確認できる．

計算量 $\mathcal{C}$ については，今回計算したパラメータでは，type (a)，type (b) ともにサンプル増幅法を用いた場合の方が大きくなることが確認された．このことは，どちらの場合も計算量のオーダーが $q^{n/a}$ であることより，式 (8), (15) を比べることで，$w > 1$ であれば計算量のオーダーが大きくなることからも確認できる．

7. まとめ

本研究では，LPN 問題・LWE 問題で使用されていた BKW アルゴリズムにおけるサンプル増幅法の手法を初めて LWR 問題に適用した．サンプル増幅法におけるパラメータである β の詳細な解析することにより，必要とするサンプル数を従来の方法より少なくすることができることを示した．この解析は，LPN 問題，LWE 問題におけるサンプル増幅法にも適用可能である．また，BKW アルゴリズムによる同一の解読計算量を持つ LWR 問題と LWE 問題に対して，LWR 問題の法 p と LWE 問題の相対エラー $\alpha = \sigma/q$ が漸近的には $2\sqrt{3}p\alpha = 1$ の関係式を満足することを導出した．この結果は，LWR 問題に基づく暗号アルゴリズムの設計及び安全性評価に応用することができる．

参考文献

[1] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, *Journal of the ACM (JACM)*, Vol. 56, No. 6, p. 34 (2009).

[2] Banerjee, A., Peikert, C. and Rosen, A.: Pseudorandom functions and lattices, *Advances in Cryptology–EUROCRYPT 2012*, pp. 719–737 (2012).

[3] Alwen, J., Krenn, S., Pietrzak, K. and Wichs, D.: Learning with rounding, revisited, *Advances in Cryptology–CRYPTO 2013*, Springer, pp. 57–74 (2013).

[4] Boneh, D., Lewi, K., Montgomery, H. and Raghunathan, A.: Key homomorphic PRFs and their applications, *Advances in Cryptology–CRYPTO 2013*, Springer, pp. 410–428 (2013).

[5] Cheon, J. H., Kim, D., Lee, J. and Song, Y. S.: Lizard: Cut off the Tail! Practical Post-Quantum Public-Key Encryption from LWE and LWR., *IACR Cryptology ePrint Archive*, Vol. 2016, p. 1126 (2016).

[6] Blum, A., Kalai, A. and Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model, *Journal of the ACM (JACM)*, Vol. 50, No. 4, pp. 506–519 (2003).

[7] Albrecht, M. R., Cid, C., Faugere, J. C., Fitzpatrick, R. and Perret, L.: On the complexity of the BKW algorithm on LWE, *Designs, Codes and Cryptography*, Vol. 74, No. 2, pp. 325–354 (2013).

[8] Lyubashevsky, V.: The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem, *APPROX-RANDOM*, Springer, pp. 378–389 (2005).

[9] Duc, A., Tramer, F. and Vaudenay, S.: Better algorithms for LWE and LWR, *34th Annual International Conference*, Part I, Vol. 9056, No. EPFL-CONF-207733, Sofia, Bulgaria, the Theory and Applications of Cryptographic Techniques, Springer, pp. 173–202 (2015).

[10] 上中谷健，國廣昇，高安敦：最小サンプルで LWE 問題を解くための BKW アルゴリズム，*SCIS*, Vol. 2D4, No. 5 (2016).

[11] Corless, R. M., Gonnet, G. H., Hare, D. E., Jeffrey, D. J. and Knuth, D. E.: On the LambertW function, *Advances in Computational mathematics*, Vol. 5, No. 1, pp. 329–359 (1996).