付録 5

格子問題等の困難性に関する調査

暗号技術調査 (暗号解析評価) ワーキンググループ

2015 年 3 月

目次

第 1 章

調査の目的

公開鍵暗号の安全性は, 素因数分解の困難性や離散対数問題の困難性などさまざまな数学的問題に依存している.「暗号技術調査ワーキンググループ (暗号解析評価)」ではこれまで, 素因数分解の困難性及び離散対数問題等の困難性に関する調査を行ってきたが, 量子計算機が実現しても安全性が保たれると期待されている「耐量子計算機暗号」を支える数学的問題の困難性の中でも, 特に近年活発に研究されてきている, 格子に係る数学的問題等に注目して調査を行った.

1.1 委員構成

2013 年度及び 2014 年度における「暗号技術調査ワーキンググループ (暗号解析評価)」の委員構成は表 1.1 の通りである.

表 1.1 暗号技術調査ワーキンググループ (暗号解析評価) の委員構成 (2013–2014 年度)

主査	高木 剛	国立大学法人九州大学 マス・フォア・インダストリ研究所 教授
委員	青木 和麻呂	日本電信電話株式会社 NTT セキュアプラットフォーム研究所 主任研究員
委員	石黒 司[*1]	株式会社 KDDI 研究所 情報セキュリティ G 研究員
委員	太田 和夫	国立大学法人電気通信大学 大学院 情報理工学研究科 総合情報学専攻 (セキュリティ情報学コース) 教授
委員	草川 恵太	日本電信電話株式会社 NTT セキュアプラットフォーム研究所 研究員
委員	國廣 昇	国立大学法人東京大学大学院 新領域創成科学研究科複雑理工学専攻 准教授
委員	下山 武司	株式会社富士通研究所 ソーシャルイノベーション研究所 セキュアコンピューティング研究部 主任研究員
委員	安田 雅哉	株式会社富士通研究所 ソーシャルイノベーション研究所 セキュアコンピューティング研究部

1.2 調査の概要

各章の執筆担当者及び調査内容は表 1.2 の通りである.

[*1] 2013 年度まで

表 1.2　章構成と執筆分担

章	担当	内容
第 1 章	事務局	調査の目的, 調査の概要など
第 2 章	石黒 司 委員[*1]	一般的な攻撃に関する総論
第 3 章	下山 武司 委員 安田 雅哉 委員	各問題について以下の項目を記述 (1) 公開鍵方式からの帰着, 証明の有無, 追加の問題・制約など
第 4 章	草川 恵太 委員	(2) 攻撃や量子アルゴリズム - General な攻撃との関係
第 5 章	國廣 昇 委員	- 固有の攻撃 - 量子アルゴリズムとの関係

第 2 章から第 5 章までの調査内容をまとめると, 下記の通りとなる.

第 2 章　格子に関する研究は非常に多岐にわたるため, SVP (近似版を含む) のうち, 近似因子が次元の多項式で表される場合に適用される, 4 つの解読アルゴリズム (LLL, BKZ, 篩, ボロノイセル) の計算量等に関する概説を行った. SVP (Shortest Vector Problem) は, ランダム帰着の元で NP 困難問題であることが示されている問題であり, パラメータを適切に取れば, 本問題を効率的に解くことは困難であると予想されている. 実際の計算機環境における解析に関しては, 計算機実験 (SVP Challenge, Lattice Challenge, Ideal Lattice Challenge) が良く知られており, 日本の研究者らの実験結果も記録されてきている.

第 3 章　LWE (Learning with Errors) 問題は, Machine Learning (機械学習理論) から派生した問題で, GapSVP (the decision version of the shortest vector problem) 及び SIVP (the shortest independent vectors problem) の困難性に関する仮定のもとで解くことが難しいことが知られており, パラメータを適切に取れば, 本問題を効率的に解くことは困難であると予想されている. 現在までに完全準同型暗号スキームをはじめとした, 様々な公開鍵暗号スキームのベースがこの LWE 問題をベースとして提案されており, 今後も安全な暗号を構成する上で重要な要素となると考えられる. 現在までに知られている LWE 問題を解く最良アルゴリズムは指数時間の計算量を持っている. ただし, 実際の LWE 問題をベースとした暗号スキームの構成の際には, BKZ アルゴリズムなどの格子縮約アルゴリズムに対し耐性を持つようにパラメータ設定を行う必要があり, 安全でかつ演算機能等の要件を満足するような LWE パラメータを選択するための, 統一的な方法は知られておらず, 今後の課題となっている. また, LWE 問題に対する攻撃実験評価に関する結果もあまり知られていないため, 今後は計算機実験に関する研究も非常に重要になると思われることから, 安全性理論評価はもちろん攻撃実験評価の視点からも, 今後の動向に注意する必要がある.

第 4 章　LPN 問題は機械学習理論や符号理論から派生した問題であり, 誤り確率が十分大きい場合の LPN 問題を多項式時間で効率的に解くことは困難であると予想されている. 共通鍵や公開鍵の分野で多くの方式が LPN 問題に基づいて提案されている. LWE 問題と比較した場合, 利点としては, ハードウェア構成との相性が良い点や誤差のサンプリングが容易である点が挙げられる. 一方, 欠点として, 鍵や暗号文のサイズが大きくなりやすい点や発展的な応用が少ない点が挙げられる. 暗号方式のパラメータ設定の際には, 4.2 節で挙げたさまざまなアルゴリズムを考慮する必要がある. アルゴリズムの高速化について盛んに研究されており, 動向を注視する必要がある.

また, 攻撃に用いられるアルゴリズムの研究は理論的なものが多く, 攻撃実験報告は小さいパラメータに対して行ったものが多い. そのため, 攻撃実験に関する研究もこれから非常に重要である.

第 5 章 ACD 問題は, 2001 年に Howgrave-Graham により導入された問題であり, パラメータを適切に選ぶことにより, 効率的に解くことが困難であると予想されている. ACD 問題は, 複数 ACD 問題や GACD 問題など, いくつかの拡張問題をもつ. ACD 問題を素因数分解を直接的に経由しないで解くアルゴリズムには, 大別すると, 組み合わせ論に基づく方法と格子理論に基づく方法がある. 組み合わせ論に基づくアルゴリズムを用いた場合では, 指数関数時間の計算量が必要であるが, 全数探索アルゴリズムの平方根の計算量で解を求めることができる. 格子理論に基づくアルゴリズムを用いた場合では, 法に対して解がある制限よりも小さいときには, 多項式時間で解くことができるものの, 十分大きいときには, 解くことができない. ACD 問題を安全性の根拠としてもつ, 完全準同型暗号方式が提案されている. 適切にパラメータが設定された状況では, 攻撃に成功するのに指数関数時間が必要であるが, 理論上の解析であるため数値実験により安全性の検証をする必要がある.

1.3 更新履歴

表 1.3 更新履歴

更新日時	主な更新内容
2013 年度	•初版.
2014 年度	•2.1.3 節. 計算機実験に関する記録の更新. •3.1.3 節の追加. •3.2.2 節の最後.「■近年の攻撃研究の動向」の追加. •4.2 節. 代表的な暗号方式を追加 (旧 4.3-4.5 節から移動した文書有り). •4.3 節 (旧 4.2 節). いくつかコメントを追加. •5.1.3 節. 5.1.3.1 節及び 5.1.3.2 節の追加. •5.1.4 節の追加. •5.5 節の追加.

第 2 章

一般的な攻撃に関する総論

格子に関する困難性問題の中でベースとなる問題は格子の最短ベクトル問題 (SVP) である. 本章では, この格子の最短ベクトル問題の定義と, それに関連するアルゴリズムについてまとめる. 更に, 実際の計算機環境における解析の現状についてまとめる. 最短ベクトル問題は, 格子暗号における重要な困難性問題の一つであり, この問題が解けると, 次章以降で説明する LWE 問題などの格子問題も解けるため計算量解析がとりわけ重要である.

2.1 準備

本章で使用する記号・用語を以下にまとめる. $\boldsymbol{b}_i = (b_1, b_2, \ldots, b_n) \in \mathbb{R}^n$ を n 個の一次独立なベクトルとする $(1 \leq i \leq n)$. $\boldsymbol{b}_i$ を列ベクトルとする行列を $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) \in \mathbb{R}^{n \times n}$ とする. この時,

$$\mathcal{L}(\mathrm{B}) = \mathcal{L}(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) = \left\{ \sum_{1 \leq i \leq n} x_i \boldsymbol{b}_i, x_i \in \mathbb{Z} \right\}$$

を格子とする. また, B を格子基底と呼ぶ. 本章では格子の次元を n とする. ベクトル $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ のノルム (長さ) を $||\boldsymbol{v}|| = (\sum_{1 \leq i \leq n} v_i^2)^{1/2}$ とする. また, 基底 B の最短ベクトルかつ非零ベクトルのノルムを $\lambda_1(\mathrm{B})$ あるいは単に λ_1 と表す. 格子 B のグラムシュミット直交化基底を $\mathrm{B}^* = (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, \boldsymbol{b}_n^*)$ とする. $\boldsymbol{b}_i^*$ は, $\boldsymbol{b}_1^* = \boldsymbol{b}_1$ として, $2 \leq i \leq n$ について以下のように帰納的に定義される.

$$\boldsymbol{b}_i^* = \boldsymbol{b}_i - \sum_{1 \leq j \leq i-1} \mu_{i,j} \boldsymbol{b}_j^*, \quad \mu_{i,j} = \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle}{||\boldsymbol{b}_j^*||}$$

$\mu_{i,j}$ をグラムシュミット係数とよぶ. 基底 $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n), i \in \{1, 2, \ldots, n\}$ における直交射影 $\pi_i : \mathbb{R}^n \to \mathbb{R}^n$ を $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{i-1})$ が生成する部分空間の直交補空間への射影写像とし, $\pi_i(\boldsymbol{v}) = \sum_{1 \leq i \leq n} a_i \boldsymbol{b}_i^*$ と表す. $i \leq j$ となる基底ベクトル $\boldsymbol{b}_j$ に対して $\pi_i(\boldsymbol{b}_j) = \boldsymbol{b}_j^{(i)}$ と表す. また, 格子の射影部分格子を $\mathcal{L}_{[j,k]} = \mathcal{L}((\boldsymbol{b}_i^{(j)})_{j \leq i \leq \min(j+k-1, n)})$ とする.

2.2 最短ベクトル問題 (SVP)

格子の最短ベクトル問題を SVP(Shortest Vector Probrem) とよぶ. これはある格子の基底が与えられた時に, その格子上のベクトルの中で長さが最小となる非零ベクトルを探索する問題である. 一般に, 最短ベクトルは必ずしも一つではないため, 最短ベクトルの中の一つのベクトルを見出せば SVP の解となる. また, 長さが最短ベクトルの α 倍以下となるベクトルのうちの一つを探索する問題を近似版最短ベクトル問題 (α-SVP) とよぶ. 以下にそれぞれ詳細な定義を示す.

定義 2.1 (最短ベクトル問題 (SVP)) 格子 $\mathcal{L}(\mathrm{B})$ が与えられて, 格子に含まれるベクトル $\boldsymbol{v} \in \mathcal{L}(\mathrm{B})$ のうちでノルムが最小の非零ベクトル (つまり, $|\boldsymbol{v}| = \lambda_1$) の一つを求める問題を最短ベクトル問題 (SVP) と呼ぶ.

最短ベクトルのノルムについて以下の定理が知られている.

定理 2.2 (ミンコフスキーの第 1 定理) 格子 $\mathcal{L}(\mathrm{B})$ に対して最短ベクトルのノルムは, $\sqrt{n}(\mathrm{vol}(\mathcal{L}(\mathrm{B})))^{\frac{1}{n}}$ 未満となる.

また, より精緻な見積りとしてガウスヒューリスティックスが知られている. ガウスヒューリスティックスによって格子 $\mathcal{L}(\mathrm{B})$ の最短ベクトルのノルムは $GH(\mathcal{L}(\mathrm{B})) = (1/\sqrt{\pi})\Gamma(\frac{n}{2}+1)^{\frac{1}{n}} \cdot |\det(\mathcal{L}(\mathrm{B}))^{\frac{1}{n}}|$ 程度と見積もられる. ここで, $\Gamma(x)$ はガンマ関数を表す. 最短ベクトル問題は, 上記の通り厳密解を求める問題として定義されている. 一方, 暗号アルゴリズムでは最短ベクトルの近似解を求める問題の困難性をベースとして構成される場合もある. 以下に近似版最短ベクトル問題 (α-SVP) を定義する.

定義 2.3 (近似版最短ベクトル問題 (α-SVP)) 格子 $\mathcal{L}(\mathrm{B})$ が与えられて, 格子に含まれるベクトル $\boldsymbol{v} \in \mathcal{L}(\mathrm{B})$ のうちでノルムが $||\boldsymbol{v}|| < \alpha\lambda_1$ となるベクトルの一つを求める問題を近似版最短ベクトル問題 (α-SVP) と呼ぶ. また, α を近似因子と呼ぶ.

2.3 求解アルゴリズムと計算量

SVP は Ajtai によって, ランダム帰着の元で NP 困難問題であることが示されている [Ajt98]. α-SVP については, 近似因子 $1 < \alpha < \sqrt{2}$ となる範囲ではランダム帰着の元で NP-困難であることが Micciancio[Micci98] によって示され, 任意の定数 α の元での NP 困難性が Khot によって証明されている [Kho05, Kho10]. 一方, 近似因子が格子の次元 n の多項式となる場合, すなわち $\alpha = poly(n)$ の場合の NP 困難性については証明されておらず, 重要な研究課題となっている. 本節では, SVP, α-SVP それぞれについて求解アルゴリズムを解説する.

■α-SVP　α-SVP を解くアルゴリズムとして, LLL[LLL82], BKZ[Sch87] アルゴリズムがある. LLL アルゴリズムは, Lenstra, Lenstra, Lovász によって提案されたアルゴリズムである. LLL アルゴリズムは格子の基底を入力とし, LLL 簡約基底とよばれる入力された基底と同じ格子を張る別の基底を求めるアルゴリズムである. この LLL 簡約基底は, 基底ベクトルのノルムに制約がある格子基底となっており, 以下のように定義される.

定義 2.4 (簡約基底) 格子基底を B とする. このとき B^* のグラムシュミット係数 $\mu_{i,j}(1 \leq j < i \leq n)$ が $|\mu_{i,j}| < \frac{1}{2}$ を満足するとき, B は簡約基底という.

定義 2.5 (δ-LLL 簡約基底) 格子基底を $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ とし, $\delta \in (0.25, 1]$ とする. 格子 B が簡約基底であり, かつ

$$\delta||\boldsymbol{b}_{i-1}^*||^2 \leq ||\boldsymbol{b}_i^*||^2 + \mu_{i,i-1}^2||\boldsymbol{b}_{i-1}^*||^2$$

という条件を満足するとき, B は δ-LLL 簡約基底という. また, この条件を Lovász 条件とよぶ.

LLL 簡約アルゴリズムを用いると, LLL 簡約基底を求めることができ, 基底ベクトルがノルムの大きさが小さい方から順番に整列される. このとき, $||\boldsymbol{b}_1|| \leq (\frac{2}{\sqrt{3}})^n\lambda_1$ となることが証明されているため, 近似因子 $\alpha = (\frac{2}{\sqrt{3}})^n$ における α-SVP の解とすることができる.

LLL アルゴリズムの概要を以下に示す. 入力は, 格子基底 $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ とし δ-LLL 簡約基底を出力する. LLL アルゴリズムは $\boldsymbol{b}_1$ から順に $\boldsymbol{b}_n$ に向かって簡約を行う. まず, $\boldsymbol{b}_j$ を簡約基底の条件を満足するために $k < j$ に対

して, $\boldsymbol{b}_j = \boldsymbol{b}_j - \lceil \mu_{j,k} \rfloor \boldsymbol{b}_k$ を計算し, $\boldsymbol{b}_j$ に合わせて $\mu_{j,k}$ を再計算する. 次に, $\boldsymbol{b}_j$ が Lovász 条件を満足しない場合には $\boldsymbol{b}_j$ と $\boldsymbol{b}_{j-1}$ を入れ替え, $j = j - 1$ として上記を繰り返す. この処理によって $j = 1$ から $j = n$ まで $\boldsymbol{b}_j$ を簡約する. LLL アルゴリズムは多項式回のループで停止することが示されており, 計算量は $O(n^4 \log(\max_{1 \leq i \leq n} ||\boldsymbol{b}_i||^2))$ となる. また, 出力される基底の第一ベクトルのノルムは $||\boldsymbol{b}_1|| \leq (\frac{2}{\sqrt{3}})^n \lambda_1$ となることが証明されている [LLL82]. 計算機実験上はこの見積りよりも短いベクトルが出力されることが多く, 特に小さい次元の場合には LLL アルゴリズムを用いて最短ベクトルを求めることができる.

LLL を改良したアルゴリズムとして BKZ アルゴリズムが Schnorr 等によって提案されている. BKZ アルゴリズムは BKZ 簡約基底を出力するアルゴリズムである. BKZ 簡約基底は LLL 簡約基底よりも広い定義となっており, 以下のように定義される.

定義 2.6 (β-BKZ 簡約基底) 格子基底を $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ とし，$\beta \in [2, n]$ とする. 格子 B が LLL 簡約基底であり, かつ $1 \leq j \leq n$ について $||\boldsymbol{b}_j^*|| = \lambda_1(\mathcal{L}_{[j,\beta]})$ を満足するとき, B は β-BKZ 簡約基底という.

β-BKZ 簡約基底は LLL 簡約基底を拡張したものであり, $\beta = 2$ の場合には LLL 簡約基底そのものになる. BKZ アルゴリズムの概要を以下に示す. BKZ アルゴリズムの入力は, LLL 簡約基底 $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ とし β-BKZ 簡約基底を出力する. まず, $i = 1, 2, \ldots, n-1$ について $\pi_i(\boldsymbol{b})$ が $\mathcal{L}_{[i,\beta]}$ で最短ベクトルとなるような $\boldsymbol{b} \in \mathcal{L}(\mathrm{B})$ を探索する. このようなベクトルは次節で説明する SVP を解くアルゴリズムを用いて求めることができる. 次にこの $||\pi_i(\boldsymbol{b})|| < ||\boldsymbol{b}_i^*||$| となる場合には基底 B にベクトル $\boldsymbol{b}$ を i 番目に挿入し基底 $\mathrm{B}' = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_i, \boldsymbol{b}, \boldsymbol{b}_{i+1}, \ldots, \boldsymbol{b}_n)$ を構成する. これに LLL 簡約基底を適用し, 新たな基底とする. 新たな基底に対して上記を繰り返し, 基底が更新されなくなるまで繰り返すことによって基底簡約を行う. BKZ アルゴリズムの停止性や計算量は証明されていないが, 計算機実験上は高速に動作し, LLL アルゴリズムよりも大きな次元に対して適用することができる. BKZ アルゴリズムを改良したアルゴリズムとして BKZ2.0 アルゴリズム [CN11, AN12] が提案されており, より大きな次元の α-SVP が解けることが示されている. また, ランダムに短いベクトルを生成して基底に挿入し, そこに BKZ アルゴリズムを適用することによって基底を簡約する RSR アルゴリズムも提案されている [Sch03, BL06].

■SVP　SVP を解くアルゴリズムとして以下のいくつかの種類のアルゴリズムが提案されている. 代表的な求解手法として, 格子基底簡約アルゴリズム, 列挙アルゴリズム, ボロノイセルアルゴリズム, 篩アルゴリズムがある.

格子基底簡約アルゴリズムは, 上記で説明した LLL, BKZ アルゴリズムなどの基底簡約アルゴリズムであり, 格子基底に適用することによって SVP を解くことができる. 代表的な格子基底簡約アルゴリズムとして LLL アルゴリズム [LLL82], BKZ アルゴリズム [Sch87], L^2 アルゴリズム [NV05, NV06], BKZ2.0[GNR10, AN12] がある.

列挙アルゴリズムは, 所謂全数探索で可能性のある係数の総当り探索を行い, 最短ベクトルを見つけるアルゴリズムである. 格子ベクトル $\boldsymbol{v} \in \mathcal{L}(\mathrm{B})$ は, 基底ベクトル $\boldsymbol{b}$ を用いて, $\boldsymbol{v} = \sum_{1 \leq i \leq n} u_i \boldsymbol{b}_i$ と表せる. したがって, 可能性のある全ての係数 $[u_1, u_2, \ldots, u_n]$ を列挙することによって最短ベクトルを見つける事ができる. 列挙アルゴリズムは, Schnorr によって示され [Sch94], 更に探索範囲を削減する枝刈り列挙 ([SH95, GNR10, MV09]) アルゴリズムが提案されている. 現時点で最も高速な枝刈り列挙アルゴリズムは Gama, Nguyen, Regev によって提案された Extream Pruning Enumeration アルゴリズムである [GNR10]. このアルゴリズムの時間計算量は $2^{O(n)}$ である. 列挙アルゴリズムは特に比較的小さい次元において高速に SVP を解くことができるため, BKZ アルゴリズムの内部関数としても用いられている. 列挙アルゴリズムの計算量を表 2.1 に示した. 列挙アルゴリズムは並列化が容易であることから, GPU 上での高速実装や, クラウドコンピューティングを用いた大規模並列計算によって大きな次元の SVP の求解報告がなされている [SchPD11].

Micciancio によってボロノイセルアルゴリズムが提案されている [MV10]. ボロノイセルアルゴリズムは決定的アル

表 2.1 列挙アルゴリズムの計算量

アルゴリズム	時間	空間	文献
ENUM	$2^{O(n^2)}$	$O(n)$	文献 [Sch94]
Extream Pruning Enumeration	$2^{O(n)}$	$O(n)$	文献 [GNR10]

表 2.2 篩アルゴリズムの計算量

アルゴリズム	時間計算量	空間計算量	文献
AKS Sieve	$O(2^{5.90n})$	$O(2^{2.95n})$	文献 [AKS01]
AKS Sieve without perturbation	$O(2^{0.41n})$	$O(2^{0.21n})$	文献 [NS08]
List Sieve	$O(2^{3.199n})$	$O(2^{1.325n})$	文献 [MV10]
Gauss Sieve	$O(2^{0.52n})$	$O(2^{0.21n})$	文献 [MV10]
List Sieve Birthday	$O(2^{2.465n})$	$O(2^{1.233n})$	文献 [PS09]
NV Sieve	$O(2^{0.3836n})$	$O(2^{0.2557n})$	文献 [NS08, WLTB10]

ゴリズムであり, $2^{O(n)}$ の時間計算量, 空間計算量となることが示されている. しかし, 現在のところボロノイセルアルゴリズムを利用した実装例は知られていない.

篩アルゴリズムは SVP を解く確率的アルゴリズムである. 2001 年に Ajtai 等によって AKS Sieve[AKS01] が提案され, それ以降, より計算量を削減したアルゴリズムが提案されている [NS08, BN07, AJ08, MV10, PS09, WLTB10]. 一般に篩アルゴリズムの時間・空間計算量は $2^{O(n)}$ である. 現在, 理論上最も高速な篩アルゴリズムは NV Sieve であり, 時間計算量は $O(2^{0.3836n})$, 空間計算量は $O(2^{0.2557n})$ となっている. 篩アルゴリズムの計算量を表 2.2 に示した.

2.4 計算機実験

本章では, 計算機実験によって実際に解かれた SVP についてまとめる. 現在, ダルムシュタット工科大学によって SVP に関するコンテストが開催されている. このコンテスによって統一された問題設定においてアルゴリズム・実装性能の評価が可能となっている. しかし実験環境, 計算機環境についての制限はないため, アルゴリズムや実装手法以外にも, 計算機性能や実験規模などが異なることに注意する必要がある.

SVP Challenge[SVPC] はランダムに与えられた格子基底に対して SVP を解き, より大きい次元について, より短いベクトルを求めることによって順位が競われている. コンテストのサイトには, 実際に解かれたベクトルが掲載されている. ただし, 掲載されているベクトルは必ずしも最短のベクトルではないことに注意されたい. Lattice Challenge[LC] は与えられた格子基底について α-SVP を解き, SVP チャレンジと同様により大きい次元, より短いベクトルを解くことが競われている. Ideal Lattice Challenge[ILC] は, イデアル格子と呼ばれる, 暗号で用いられることが多い特殊な格子 [HPS98, GGH12, Gen09] に対する SVP, α-SVP の問題が掲載されている. コンテストに掲載されている問題の設定については文献 [Pla13] を参照にされたい.

α-SVP に対する実験結果を表 2.3 に表す. 現在, α-SVP の求解は BKZ2.0 アルゴリズム [GNR10], あるいはその改良方式 [CN11, AN12] が用いられており, 825 次元までの α-SVP が解かれている. 詳細なアルゴリズム, 計算機環境についてはそれぞれの文献を参照されたい. また, SVP に対する実験結果を 2.4 に示す. SVP Challenge の結果として Kashiwabara らの RSR アルゴリズムの改良手法 [Kashi13], BKZ2.0[GNR10] が有効であることが示されており, 最も大きな次元に対する求解は Kashiwabara らによる RSR アルゴリズムの改良方式などである [Kashi13]. 彼らの手法は,

表 2.3　q-ary lattice に対する Approx-SVP の求解 (Lattice Challenge[LC])

	次元	ノルム	アルゴリズム	時期	文献
Chen, Nguyen	825	120.37	BKZ2.0 の改良	2013-3	
Aono, Naganuma	825	122.38	BKZ2.0 の改良	2012-10	文献 [AN12]
Chen, Nguyen	800	106.60	BKZ2.0	2013-3	文献 [CN11]
Aono, Naganuma	800	117.69	BKZ2.0 の改良	2012-10	文献 [AN12]
Chen, Nguyen	775	100.14	BKZ2.0 の改良	2013-3	文献 [CN11]
Aono, Naganuma	775	106.68	BKZ2.0 の改良	2012-10	文献 [AN12]
Chen, Nguyen	750	87.76	BKZ2.0	2013-3	文献 [CN11]
Chen, Nguyen	725	80.65	BKZ2.0	2013-3	文献 [CN11]
Aono, Naganuma	725	83.61	BKZ2.0 の改良	2012-9	文献 [AN12]
Chen, Nguyen	700	72.46	BKZ2.0	2013-3	文献 [CN11]
Aono, Naganuma	700	76.17	BKZ2.0 の改良	2012-9	文献 [AN12]

表 2.4　SVP の求解 (SVP Challenge[SVPC])

	次元	ノルム	アルゴリズム	時期	文献
Kashiwabara, Teruya	140	3025	RSR アルゴリズムの改良	2015-1	
Kashiwabara, Teruya	138	3077	RSR アルゴリズムの改良	2014-12	
Kashiwabara, Teruya	134	2976	RSR アルゴリズムの改良	2014-7	文献 [Kashi14]
Kashiwabara, Fukase	132	3012	RSR アルゴリズムの改良	2014-4	文献 [Kashi14]
Aono, Nguyen	130	2883	BKZ2.0 + Randomized ENUM	2014-10	
Kashiwabara, Fukase	130	3025	RSR アルゴリズムの改良	2013-11	文献 [Kashi13]
Kashiwabara, Fukase	128	2984	RSR アルゴリズムの改良	2013-9	文献 [Kashi13]
Aono, Nguyen	126	2855	BKZ2.0 + Extreme pruning	2014-9	
Kashiwabara, Teruya	126	2897	RSR アルゴリズムの改良	2014-8	
Aono	126	2906	BKZ2.0 + Extreme pruning	2014-7	
Kashiwabara, Fukase	126	2944	RSR アルゴリズムの改良	2013-9	文献 [Kashi13]
Chen, Nguyen	126	2969	BKZ2.0 + Randomized ENUM	2013-4	文献 [CN11]
Chen, Nguyen	124	2884	BKZ2.0 + Randomized ENUM	2013-3	文献 [CN11]
Chen, Nguyen	122	2913	BKZ2.0 + Randomized ENUM	2013-3	文献 [CN11]
Kashiwabara, Fukase	120	2756	BKZ2.0 の改良	2013-3	文献 [AN12]
Aono, Naganuma	120	2830	BKZ2.0 の改良	2013-9	文献 [Kashi13]

短いベクトルの統計的な情報から, 最短ベクトルの分布を予測し高速に短いベクトルを生成するように改良している.

Ideal Lattice に対する実験結果を表 2.5–2.6 に表す. Ideal Lattice Challenge においては 128 次元の SVP が解かれている [IKMT13]. 彼らの手法は, 篩アルゴリズムの一つである Gauss Sieve アルゴリズムの並列化によって 84 台の計算機を用いて 128 次元の SVP を求めている. Gauss Sieve アルゴリズムはイデアル格子の性質を用いて次元が 2 の冪乗となる場合に高速化できることが示されている. 更に, イデアル格子のいくつかの次元において Gauss Sieve を高速

表 2.5 Ideal-SVP(< 1.05 Gaussian heuristic) の求解 (Ideal Lattice Challenge[ILC])

	次元	ノルム	アルゴリズム	時期	文献
Ishiguro, Kiyomoto, Miyake, Takagi	128	2959	Gauss Sieve の改良	2013-4	文献 [IKMT13]
Ishiguro, Kiyomoto, Miyake, Takagi	108	2669	Gauss Sieve の改良	2013-4	文献 [IKMT13]

表 2.6 Approx-SVP($n \det^{1/n}$) の求解 (Ideal Lattice Challenge[ILC])

	次元	ノルム	アルゴリズム	時期	文献
Wang, Aono, Hayashi, Takagi	500	507596	Progressive BKZ	2015-1	文献 [WAHT15]

化できる条件も見つかっているが, 一般のイデアル格子の性質を用いた高速化手法は, 他の求解手法も含めて見つかっていないため, 格子暗号の安全性を議論する上で重要な研究課題となっている.

第 2 章の参照文献

[Ajt98] M. Ajtai, “The Shortest Vector Problem in L^2 is NP-hard for Randomized Reductions (Extended Abstract),” In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, STOC’98, pp. 10–19. ACM, 1998.

[AD97] M. Ajtai and C. Dwork, “A Public-key Cryptosystem with Worst-case/average-case Equivalence,” In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing*, STOC’97, pp. 284–293. ACM, 1997.

[AKS01] M. Ajtai, R. Kumar and D. Sivakumar, “A Sieve Algorithm for the Shortest Lattice Vector Problem,” In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, STOC 2001, pp. 601–610. ACM, 2001.

[AN12] 青野 良範, 長沼 健 “BKZ2.0 アルゴリズムの実装と改良,” 信学技報, vol. 112, no. 211, ISEC2012-45, pp. 15–22, 2012.

[AJ08] V. Arvind and P. S. Joglekar, “Some Sieving Algorithms for Lattice Problems,” In *Proceedings of the IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science*, FSTTCS’08, volume 2 of *LIPIcs*, pp. 25–36. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2008.

[BN07] J. Blömer and S. Naewe, “Sampling Methods for Shortest Vectors, Closest Vectors and Successive Minima,” *Journal of Theoretical Computer Science*, volume 410, issue 18, pp. 1648–1665, 2009.

[CN11] Y. Chen and N. Nguyen, “BKZ 2.0: Better Lattice Security Estimates,” In *Proceedings of the 19th Annual International Conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT’11, Springer LNCS 7073, pp. 1-20, 2011.

[FK15] M. Fukase and K. Kashiwabara, “An Accelerated Algorithm for Solving SVP Based on Statistical Analysis,” Journal of Information Processing Vol.23 No.1 pp. 67-80, 2015.

[GGH12] S. Garg, C. Gentry and S. Halevi, “Candidate Multilinear Maps from Ideal Lattices,” Cryptology ePrint Archive, Report 2012/610, 2012.

[GNR10] N. Gama, P. Nguyen and O. Regev, “Lattice Enumeration Using Extreme Pruning,” In *Proceedings of the 29th Annual International Conference on Theory and Application of Cryptographic Techniques*, Eurocrypt’10, Springer LNCS 6110, pp. 257–278, 2010.

[Gen09] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” In *Proc of the 41st Annual ACM Symposium on Theory of Computing*, STOC 2009, pp. 169–178. ACM, 2009.

[HPS98] J. Hoffstein, J. Pipher and J. Silverman, “NTRU: A Ring-based Public Key Cryptosystem,” In *Algorithmic Number Theory*, Springer LNCS 1423, pp. 267–288, 1998.

[LLL82] A. Lenstra, H. Lenstra and L. Lovász, “Factoring Polynomials with Rational Coefficients,” *Mathema-*

tische Annalen, volume 261, issue 4, pp. 515–534, 1982.

[BL06] J. Buchmann and C. Ludwig, "Practical Lattice Basis Sampling Reduction," In *Proceedings of the 7th International Symposium*, ANTS-VII, Springer LNCS 4076, pp. 222–237, 2006.

[IKMT13] T. Ishiguro, S. Kiyomoto, Y. Miyake and T. Takagi, "Parallel Gauss Sieve Algorithm: Solving the SVP Challenge over a 128-Dimensional Ideal Lattice," Cryptology ePrint Archive, Report 2013/388, 2013.

[Kashi13] 柏原 賢二, "格子の最短ベクトル問題の新しいアルゴリズム," 第 5 回暗号及び情報セキュリティと数学の相関ワークショップ, CRISMATH2013, 2013. `http://www.risec.aist.go.jp/events/2013/1226-ja.html`.

[Kashi14] K. Kashiwabara, "A fast algorithm for the shortest vector problem," Workshop "Post-Quantum Cryptography: Recent Results and Trends," November 2014. `http://www.isit.or.jp/lab2/2014/10/20/pqworkshop-2/`

[Kho05] S. Khot, "Hardness of Approximating the Shortest Vector Problem in Lattices," *Journal of the ACM*, Vol. 52, No. 5, pp. 789–808, Springer, 2005.

[Kho10] S. Khot, "Inapproximability Results for Computational Problems on Lattices," *The LLL Algorithm–Survey and Applications*, pp. 453–473, Springer, 2010.

[Micci98] D. Micciancio, "The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant," In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS'98, pp. 92–98. IEEE Computer Society, 1998.

[MV10] D. Micciancio and P. Voulgaris, "A Deterministic Single Exponential Time Algorithm for Most Lattice Problems Based on Voronoi Cell Computations," In *Proceedings of the 42nd ACM Symposium on Theory of Computing*, STOC 2010, pp. 351–358. ACM, 2010.

[MV09] D. Micciancio and P. Voulgaris, "Faster Exponential Time Algorithms for the Shortest Vector Problem," In *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA 2010, volume 65, pp. 1468–1480. SIAM, 2010.

[NV05] P. Q. Nguyen and T. Vidick, "Floating-point LLL Revisited," In *Proceedings of the 24th Annual Eurocrypt Conference*, Springer LNCS 3495, pp. 215–233, 2005.

[NV06] P. Q. Nguyen and T. Vidick, "LLL on the Average," In *Proceedings of the 7th International Symposium*, ANTS-VII, Springer LNCS 4076, pp. 238–256, 2006.

[NS08] P. Q. Nguyen and D. Stehlé, "Sieve Algorithms for the Shortest Vector Problem Are Practical," *Journal of Mathematical Cryptology*, volume 2, pp. 181–207, 2008.

[ILC] T. Plantard and M. Schneider, Ideal Lattice Challenge, `http://www.latticechallenge.org/ideallattice-challenge/`.

[Pla13] T. Plantard and M. Schneider, "Creating a Challenge for Ideal Lattices," Cryptology ePrint Archive, Report 2013/039, 2013.

[PS09] X. Pujol and D. Stehlé, "Solving the Shortest Lattice Vector Problem in Time $2^{2.465n}$," Cryptology ePrint Archive, Report 2009/605, 2009.

[SchPD11] M. Schneider, "Computing Shortest Lattice Vectors on Special Hardware," PhD thesis, Technische Universität Darmstadt, 2011.

[ScheP11] M. Schneider, "Sieving for Shortest Vectors in Ideal Lattices," Cryptology ePrint Archive, Report

2011/458, 2011.

[LC] R. Lindner, M. Rueckert, P. Baumann and L. Nobach, Lattice Challenge, `http://www.latticechallenge.org/`.

[SVPC] M. Schneider and N. Gama, The SVP Challenge, `http://www.latticechallenge.org/svp-challenge/`.

[Sch87] C.-P. Schnorr, "A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms," *Journal of Theoretical Computer Science*, volume 53, issue 2-3, pp. 201–224, 1987.

[Sch94] C.-P. Schnorr, "Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems," *Journal of Mathematical programming*, pp. 181–191. Springer, 1993.

[SH95] C.-P. Schnorr and H. H. Horner, "Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction," In *Proceedings of the 14th annual international conference on Theory and application of cryptographic techniques*, Eurocrypt'95, Springer LNCS 921, pp. 1–12, 1995.

[Sch03] C.-P. Schnorr, "Lattice reduction by random sampling and birthday methods," In *Proceedings of the 20th Annual Symposium on Theoretical Aspects of Computer Science*, STACS 2003, Springer LNCS 2607, pp. 145–156. 2003.

[WLTB10] X. Wang, M. Liu, C. Tian and J. Bi, "Improved Nguyen-Vidick Heuristic Sieve Algorithm for Shortest Vector Problem," Cryptology ePrint Archive, Report 2010/647, 2010.

[WAHT15] Y. Wang, Y. Aono, T. Hayashi and T. Takagi, "A New Progressive BKZ Algorithm," SCIS2015, 3E3-5, 2015.

第 3 章

LWE

近年, 2005 年に Regev[Reg05] によって紹介された LWE (Learning with Errors) 問題の計算量困難性に依存した暗号技術がこれまで数多く提案されている. 本章では, 主に LWE 問題を用いた様々な暗号技術へのアプリケーションの紹介と, LWE 問題の計算量困難性についての調査結果を述べる (本章をまとめるにあたり, 文献 [Reg] を主に参考にした).

3.1 LWE の概説

3.1.1 LWE とは

LWE 問題とは, Machine Learning (機械学習理論) から派生した, 解くことが難しいとされている問題の一種である. 簡単に説明すると, 秘密情報 $\vec{s} \in \mathbb{F}_q^n$ に関するランダムな線形 “近似値” の列が与えられたときに, その秘密情報 $\vec{s}$ を復元する問題のことをいう. 具体的な数値例として, 変数 $\vec{s} = (s_1, s_2, s_3, s_4)$ に関する線形近似値の列

$$\begin{cases} 14s_1 + 15s_2 + 5s_3 + 2s_4 \approx 8 \pmod{17} \\ 13s_1 + 14s_2 + 14s_3 + 6s_4 \approx 16 \pmod{17} \\ 6s_1 + 10s_2 + 13s_3 + s_4 \approx 12 \pmod{17} \\ 10s_1 + 4s_2 + 12s_3 + 16s_4 \approx 12 \pmod{17} \\ 9s_1 + 5s_2 + 9s_3 + 6s_4 \approx 9 \pmod{17} \\ 3s_1 + 6s_2 + 4s_3 + 5s_4 \approx 16 \pmod{17} \\ \vdots \\ 6s_1 + 7s_2 + 16s_3 + 2s_4 \approx 3 \pmod{17} \end{cases}$$

が与えられたとする (ただし, 各線形方程式の誤差は ± 1 程度とする). このとき, 上記の方程式の列の解 $\vec{s} = (s_1, s_2, s_3, s_4)$ を求めるのが LWE 問題の例である (実際, 上記の数値例では, $\vec{s} = (0, 13, 9, 11) \in \mathbb{F}_{17}^4$ が解となる). ここで注意しておかなくてはいけない事は, 上記の線形方程式で誤差がない場合は, ガウスの消去法 (または掃出し法ともいう) を用いれば多項式時間で簡単に解を求めることができる点である. つまり, 与えられる誤差の度合いが LWE 問題をより難しくしている. ここで, LWE 問題の定義を与えておく.

定義 3.1 (LWE 問題 [Reg05]) サイズパラメータ $n \geq 1$, 剰余パラメータ $q \geq 2$, $\mathbb{F}_q$ 上の誤差に関する確率分布 χ が与えらたとする. このとき, $A_{\vec{s},\chi}$ を

$$A_{\vec{s},\chi} = \left\{ (\vec{a}, \langle \vec{a}, \vec{s} \rangle + e) \in \mathbb{F}_q^n \times \mathbb{F}_q \mid \vec{a} \leftarrow \mathbb{F}_q^n, e \leftarrow \chi \right\}$$

で定義される確率分布とする (ただし, $\vec{a}$ は $\mathbb{F}_q^n$ 上一様ランダムに選ばれた元とし, $\langle \vec{a}, \vec{s} \rangle$ は 2 つのベクトル間の内積値とする). 秘密情報 $\vec{s} \in \mathbb{F}_q^n$ に対し, $A_{\vec{s},\chi}$ からサンプリングされた任意個数の元が与えられた時に, 秘密情報 $\vec{s}$ を求める問題を LWE 問題という.

上記で定義した LWE 問題は, ランダム線形符号の復号問題, または, 格子上ランダムな bounded distance decoding (BDD) 問題として見なすことができる. さらに, $q = 2$ のとき, LWE 問題は learning parity with noise (LPN) 問題に対応する (LPN 問題については, 第 4 章で説明). 上記の定義において, 確率分布 χ としてガウス分布を用いる場合がほとんどであったが, 近年では一様分布を用いた場合の研究も進み始めている [DQ13, MP13].

またこの節で, 上記で定義した LWE の変形問題である ring-LWE 問題も紹介しておく (以下の定義では, 2 べき整数 n の場合しか説明しないが, 近年では一般の整数 n を用いた ring-LWE 問題も紹介され, 色々な暗号方式を構成する際に応用されている. 参考文献として [LPR13] を参照することを勧める).

定義 3.2 (ring-LWE 問題 [LPR10]) n を 2 べき整数とし, q を $q \equiv 1 \bmod 2n$ を満たす素数とする. また, R_q を環 $\mathbb{F}_q[x]/(x^n + 1)$ と定め, R_q 上の誤差に関する確率分布 χ を固定しておく. ただし, 写像 $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \mapsto (a_0, a_1, \ldots, a_{n-1})$ より環 R_q は n-次元ベクトル空間 $\mathbb{F}_q^n$ と同一視することができ, R_q の元を $\mathbb{F}_q^n$ の元として見なすことができる. ring-LWE 問題では, $\vec{a} \bullet \vec{s}$ を R_q 上の乗算とした時, 秘密情報 $\vec{s} \in R_q \simeq \mathbb{F}_q^n$ に対して, 集合

$$\left\{ (\vec{a}, \vec{b} = \vec{a} \bullet \vec{s} + \vec{e}) \in R_q \times R_q \mid \vec{a} \leftarrow R_q, \vec{e} \leftarrow \chi \right\}$$

からサンプリングされた m 個の元が与えられた時に, 秘密情報 $\vec{s}$ を求める問題を ring-LWE 問題と呼ぶ.

通常の LWE 問題に比べて, ring-LWE 問題は格子ベースの暗号スキームをより効率的にすることができ, 近年では ring-LWE 問題をベースとした (主に準同型) 暗号スキームが数多く提案されている.

3.1.2 LWE の一般的な利点 (アプリケーション)

一般的に, LWE 問題は暗号技術の様々な分野に応用することが可能で, これまでに様々な研究者によって提案されている. 代表的な応用例として以下のものが知られている.

- 公開鍵暗号スキームの構成
  - 選択平文攻撃に対して安全な方式 [Reg05, KTX07, PVW08]
  - 選択暗号文攻撃に対して安全な方式 [PW08, Pei09]
- 紛失通信プロトコル [PVW08]
- identity-based encryption (IBE) スキームの構成 [GPV08, CHKP10, ABB10]
- leakage-resilient 暗号の構成 [AGV09, ACPS09, DGK10, GKPV10]

さらに, 2009 年の Gentry[Gen09] の完全準同型暗号の構成に関する結果以降では, 特に ring-LWE 問題ベースの (完全 or somewhat) 準同型暗号スキームが数多く提案されており, 代表的な完全準同型暗号スキームに関するものとして, [SV11, BGV12, GHS12a, GHS12b, GHPS12] の結果が知られている.

3.1.3 代表的な LWE ベースの暗号方式

ここでは, LWE 問題をベースとした代表的な暗号方式をいくつか紹介する.

3.1.3.1 [Reg05] による公開鍵暗号方式

LWE 問題をベースとした公開鍵暗号として, [Reg05] で提案された方式が代表的である. [Reg05] の暗号方式の構成のためには, 以下の 4 つのパラメータが必要である:

- n: 安全性パラメータ
- m: LWE サンプルの個数 ($m = 1.1 \cdot n \log q$ となる整数を選ぶ)
- q: 剰余パラメータ (q として $n^2 \leq q \leq 2n^2$ を満たす素数を選ぶ)
- $\alpha > 0$:ノイズパラメータ ($\alpha = 1/\left(\sqrt{n}\log^2 n\right)$)

以下に具体的な暗号方式の構成を示す:

秘密鍵の生成 一様ランダムに $\vec{s} \leftarrow \mathbb{F}_q^n$ を選ぶ.

公開鍵の生成 秘密鍵 $\vec{s}$, 剰余パラメータ q, ノイズパラメータ α を持つ LWE 分布から生成した m 個のサンプル $(\vec{a}_i, b_i)_{i=1}^m \leftarrow A_{\vec{s},\chi}^m$ を公開鍵とする (つまり各 i に対し, $\vec{a} \leftarrow \mathbb{F}_q^n$ で $e_i \leftarrow \chi = D_{\mathbb{Z},\alpha q}$ と選び, $b_i = \langle \vec{a}_i, \vec{s} \rangle + e_i \in \mathbb{F}_q$ と構成する).

暗号化 集合 S を $\{1, 2, \ldots, m\}$ の中から一様ランダムに選んだ部分集合とする (例えば, $S = \{1, m\}$). このとき, 平文ビットが 0 の暗号文を $\left(\sum_{i\in S} \vec{a}_i, \sum_{i\in S} b_i\right)$ とし, 平文ビットが 1 の暗号文を $\left(\sum_{i\in S} \vec{a}_i, \lfloor \frac{q}{2} \rfloor + \sum_{i\in S} b_i\right)$ とする.

復号 暗号文 $(\vec{a}, b)$ に対し, $b - \langle \vec{a}, \vec{s} \rangle \in \mathbb{F}_q$ が $\lfloor \frac{q}{2} \rfloor$ より 0 に近い場合, 復号結果として 0 を出力し, それ以外の場合は 1 を出力する.

復号の正当性について, $(\vec{a}, b) = \left(\sum_{i\in S} \vec{a}_i, \sum_{i\in S} b_i\right)$ の場合 (つまり, 平文 0 に対応する暗号文の場合),

$$b - \langle \vec{a}, \vec{s} \rangle = \sum_{i\in S} (b_i - \langle \vec{a}_i, \vec{s} \rangle) = \sum_{i\in S} e_i$$

なので, $-\frac{q}{4} < \sum_{i\in S} e_i < \frac{q}{4}$ であれば復号に成功する (つまり, 復号として 0 が出力される). 各ノイズ e_i は標準偏差が αq のガウス分布 $\chi = D_{\mathbb{Z},\alpha q}$ から選ばれているので, $\sum_{i\in S} e_i$ の標準偏差は高々 $\sqrt{m}\alpha q$ となる. ここで, 各パラメータの選択方法から $\sqrt{m}\alpha q < q/\log n$ なので, 非常に高い確率で復号に成功することが分かる (平文ビットが 1 の暗号文に対しても同様の議論が成り立つ). また, 上記の暗号方式の安全性については, LWE 仮定の下で CPA 安全であることが証明されている [Reg09, Section 5].

ここで紹介した [Reg05] による暗号方式は, 公開鍵サイズが $(mn \log q) = \widetilde{O}(n^2)$ で, 暗号文サイズも平文サイズの $O(n \log q) = \widetilde{O}(n)$ 倍に増加するため, 決して効率的ではない (より効率的な方式としては [PVW08] などを参照).

■パラメータ設定について 上記で構成した [Reg05] による公開鍵暗号方式の具体的なパラメータ設定例が [MR09] で示されている. パラメータ設定例として, $(n, m, q, \alpha) = (136, 2008, 2003, 0.0065)$, $(192, 1500, 16381, 0.0009959)$, $(233, 1042, 32749, 0.000217)$ などが挙げられており, これらの各パラメータ設定は格子ベース暗号の安全性を測る root Hermite factor δ の値が 1.01 程度になるように設定されている (root Hermite factor δ については後述の 3.2.2 節を参照).

3.1.3.2 [BV11] による somewhat 準同型暗号方式 ([LNV11] で少し改良)

近年, 効率的な LWE ベースの暗号方式を得るために, [LPR10] で紹介されている ring-LWE 問題 (定義 3.5 を参照) の困難性に依存した方式がいくつか提案されている. 以下では, [BV11] で提案されている somewhat 準同型暗号方式を紹介する (somewhat 準同型暗号とは暗号化したまま限定回の加算と乗算が可能な暗号方式). [BV11] の somewhat

準同型暗号方式の構成のために, 以下の 4 つのパラメータが必要である:

- n: 2 べき整数で, 暗号方式を構成する基礎的な環 $R = \mathbb{Z}[x]/(x^n + 1)$ を定義する (n が 2 べき整数の場合のみ, 多項式 $x^n + 1$ は $\mathbb{Z}$ 上既約となることに注意).
- q: $q \equiv 1 \bmod 2n$ を満たす素数で, 暗号文空間の基礎環 $R_q = \mathbb{F}_q[x]/(x^n + 1)$ を定義する.
- t: 条件 $t < q$ を満たす整数で, 暗号方式の平文空間 $R_t = (\mathbb{Z}/t\mathbb{Z})[x]/(x^n + 1)$ を定義する.
- σ: ノイズを与えるためのガウス分布の標準偏差.

そこで, [BV11] の somewhat 準同型暗号方式は以下のように構成される (少しだけ改良された方式として [LNV11] も参照): また, 以下の構成では, 定義 3.5 と同じように $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \to (a_0, a_1, \ldots, a_{n-1})$ より環 R を $\mathbb{Z}^n$ と同一視する (同様に, $R_q \simeq \mathbb{F}_q^n$ と同一視することが可能).

鍵生成　まず, $R \ni s \leftarrow \chi = D_{\mathbb{Z}^n,\sigma}$ を選び, 一様ランダムに $p_1 \in R_q$ を取り, 小さなエラー $e \leftarrow \chi$ を固定する ([BV11] では $s \leftarrow \chi$ を一様ランダムに選択するのに対し, [LNV11] では一様ランダムには選択しない点だけが異なる). そこで, 公開鍵を $\mathsf{pk} = (p_0, p_1)$ とし (ただし, $p_0 = -(p_1 s + te)$ とする), 秘密鍵を $\mathsf{sk} = s$ とする.

暗号化　平文情報 $m \in R_t$ と公開鍵 $\mathsf{pk} = (p_0, p_1)$ に対し, まず $R \ni u, f, g \leftarrow \chi$ を選び, 暗号文を

$$\mathsf{Enc}(m, \mathsf{pk}) = (c_0, c_1) = (p_0 u + tg + m, p_1 u + tf),$$

と定義する. ただし, 条件 $t < q$ より, 上記の数式では元 $m \in R_t$ を環 R_q の元として見なして計算する. つまり, 上記の暗号文は $(R_q)^2$ の元として表現される.

準同型暗号演算 (暗号加算・暗号乗算)　上記の暗号アルゴリズムでは暗号文として $(R_q)^2$ の元を出力するが, 以下で定義する暗号乗算では暗号文の長さを長くする操作であるため, ここでは任意の長さの暗号文に対する暗号加算・乗算を定義する; 2 つの暗号文 $\mathsf{ct} = (c_0, c_1, \ldots, c_\xi)$ and $\mathsf{ct}' = (c'_0, c'_1, \ldots, c'_\eta)$ が与えられているとする.

- まず, 暗号加算 "$\dot{+}$" は, 以下のように各成分ごとの加算

$$\mathsf{ct} \dot{+} \mathsf{ct}' = (c_0 + c'_0, c_1 + c'_1, \ldots, c_{\max(\xi,\eta)} + c'_{\max(\xi,\eta)})$$

  で与えられる. 同様に, 暗号減算も各成分ごとの減算で与えられる.

- 次に, 暗号乗算 "$*$" は以下で与えられる:

$$\mathsf{ct} * \mathsf{ct}' = (\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{\xi+\eta})$$

  ただし, z を変数としたとき, 各 $\hat{c}_i$ は以下の関係式から計算可能である:

$$\sum_{i=0}^{\xi+\eta} \hat{c}_i z^i = \left(\sum_{i=0}^{\xi} c_i z^i\right) \cdot \left(\sum_{j=0}^{\eta} c'_j z^j\right)$$

復号　任意の長さの暗号文 $\mathsf{ct} = (c_0, c_1, \ldots, c_\xi)$ に対して, 復号は

$$\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) = [\tilde{m}]_q \bmod t \in R_t,$$

で計算できる. ただし, $\tilde{m} = \sum_{i=0}^{\xi} c_i s^i \in R_q$ であり, $[\tilde{m}]_q$ は元 $\tilde{m}$ の各係数の $[-q/2, q/2)$ への剰余とする. また, $\vec{s} = (1, s, s^2, \ldots)$ としたとき, この復号処理を $\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) = [\langle \mathsf{ct}, \vec{s} \rangle]_q \bmod t$ と書き直すこともできる.

復号の正当性については, 上記の暗号アルゴリズムで得られる暗号文 $\mathsf{ct} = (c_0, c_1)$ に対し, 関係式 $p_0 + p_1 s = -te$ が成り立つので

$$\langle \mathsf{ct}, \vec{s} \rangle = (p_0 u + tg + m) + s \cdot (p_1 u + tf) = m + t \cdot (g + sf - ue)$$

が環 R_q 上で成り立つ. ここで, 元 $m+t\cdot(g+sf-ue)$ を環 R の元と見なしたとき, その各係数が $[-q/2,q/2)$ 内に収まっている限り, $[\langle \mathsf{ct},\vec{s}\rangle]_q = m+t\cdot(g+sf-ue)$ が環 R 上で成立する (元 $e,f,g,u\leftarrow\chi$ が十分小さなノイズとして選択されていることに注意). この場合, 剰余 mod$t$ の操作で正しい復号結果 $m\in R_t$ が得られる. また, 暗号加算・暗号乗算された暗号文について, 2 つの暗号文 $\mathsf{ct}_1,\mathsf{ct}_2$ に対し,

$$\begin{cases} \langle \mathsf{ct}_1 \dot{+} \mathsf{ct}_2,\vec{s}\rangle = \langle \mathsf{ct}_1,\vec{s}\rangle + \langle \mathsf{ct}_2,\vec{s}\rangle \\ \langle \mathsf{ct}_1 * \mathsf{ct}_2,\vec{s}\rangle = \langle \mathsf{ct}_1,\vec{s}\rangle \cdot \langle \mathsf{ct}_2,\vec{s}\rangle \end{cases}$$

が成り立つので, 暗号文のノイズが十分小さい限り, 準同型演算が可能な暗号方式となっている. 具体的には, 暗号文 $\mathsf{ct}_1,\mathsf{ct}_2$ が平文情報 $m_1,m_2\in R_t$ に対応しているとき, 各暗号文のノイズが小さい場合に限り

$$\begin{cases} \mathsf{Dec}(\mathsf{ct}_1 \dot{+} \mathsf{ct}_2,\mathsf{sk}) = m_1+m_2 \\ \mathsf{Dec}(\mathsf{ct}_1 * \mathsf{ct}_2,\mathsf{sk}) = m_1\times m_2 \end{cases}$$

が成立する.

また, この暗号方式の安全性については, 定義 3.5 で与えられた ring-LWE 問題を少し変形した以下の問題の計算量困難性に依存する (以下は [LNV11] を引用):

定義 3.3 (polynomial-LWE 問題 [BV11], [LNV11]) パラメータ (n,q,t,σ) が与えられた時, polynomial-LWE 問題 $\mathsf{PLWE}_{n,q,\chi}$ とは, 次の 2 つの分布を識別することである:

1. 一様ランダムに $(R_q)^2$ の元 (a_i,b_i) をサンプリングする.
2. 一様ランダムに $s\leftarrow\chi=D_{\mathbb{Z}^n,\sigma}$ を選び, 一様ランダムに $a_i\leftarrow R_q$ をサンプリングし, $e_i\leftarrow\chi$ を選び $b_i=a_is+e_i$ とする. このとき, $(a_i,b_i)\in(R_q)^2$ をサンプリングする.

上記で構成した somewhat 準同型暗号方式の安全性については, 具体的には上記の polynomial-LWE 問題の計算量困難性仮定の下で KDM 安全 (key dependent message security) であることが証明されている [BV11].

■パラメータ設定について 上記で構成される somewhat 準同型暗号方式に関して, [LNV11, Table 1] で具体的なパラメータ設定例が挙げられている. 表 3.1 で, [LNV11, Table 1] の中で代表的なパラメータ設定例を示すと共に, そのパラメータ設定に対する distinguishing attack による攻撃計算量の見積もりも示しておく. また, distinguishing attack による攻撃原理とその攻撃計算量評価については, 後述の 3.2.2 節で説明する (具体的には, 表 3.1 の distinguishing attack の攻撃計算量は式 (3.3) から算出した値である).

表 3.1 [BV11] による somewhat 準同型暗号方式のパラメータ設定例とその安全性レベル (詳細は [LNV11, Table 1] を参照, δ は各パラメータに対する root Hermite factor で詳細は 3.2.2 節を参照)

パラメータ (n,q,t,σ)	暗号乗算の深さ	distinguishing attack の攻撃計算量
$(2048, 52\text{-bit}, 128, 8)$	1	2^{198} $(\delta=1.0041)$
$(4096, 86\text{-bit}, 128, 8)$	2	2^{250} $(\delta=1.0035)$
$(4096, 118\text{-bit}, 128, 8)$	3	2^{149} $(\delta=1.0048)$
$(4096, 150\text{-bit}, 128, 8)$	4	2^{92} $(\delta=1.0062)$
$(16384, 338\text{-bit}, 128, 8)$	9	2^{243} $(\delta=1.0035)$

3.2 LWE 問題の困難性について

ここでは, LWE 問題の困難性に簡単について説明する. ここでは, 他の格子問題への帰着という理論的な困難性に関するものと, 実際の攻撃実験による困難性評価に関するものの 2 つの面による結果を説明する.

3.2.1 他の格子問題への帰着とその困難性

文献 [Reg] でも説明されているように, 以下に挙げる 3 つの理由から現在 LWE 問題を解くことは難しいと信じられている.

(A) まず, LWE 問題を解く, 知られているものの中で最良のアルゴリズムは指数時間アルゴリズムである (量子アルゴリズムを用いた場合でさえも難しい).

(B) 3.1.1 節で説明したように, LWE 問題は LPN 問題の一般化であり, LPN 問題自体が格子理論において解くのが困難な問題と予想されている. さらに, LPN 問題はランダム線形バイナリ符号の復号問題として定式化可能であり, LPN 問題を効率的に解くこと自体符号理論におけるブレークスルーである (LPN 問題については, 第 4 章を参照).

(C) さらに最も重要なこととして, GapSVP (the decision version of the shortest vector problem) や SIVP (the shortest independent vectors problem) のような標準的な格子問題の最悪ケースの困難性に関するある仮定のもとで, LWE 問題は困難であることが知られている [Reg05, Pei09].

ここで, 上記の (A) と (C) の点について具体的に説明した定理を挙げておく.

定理 3.4 ([Reg09] における Theorem 1.1) n, q を 2 つの整数とし, $\alpha \in (0,1)$ は $\alpha q > 2\sqrt{n}$ を満たすとする. もし $\mathsf{LWE}_{n,q,\bar{\Phi}_\alpha}$(3.2.2 節の定義 3.5 を参照) を解く効率的なアルゴリズムが存在するなら, 最悪時の因子 $\gamma = \tilde{O}(n/\alpha)$ を持つ GapSVP_γ と SIVP_γ を効率的に解くことができる量子アルゴリズムが存在する. ただし, Φ_α は平均値が 0 で標準偏差が $\frac{\alpha}{\sqrt{2\pi}}$ を持つ確率分布で, $\bar{\Phi}_\alpha$ は Φ_α を離散化した確率分布とする.

別の言い方をすると, 上記の定理は GapSVP と SIVP を効率的に解く量子アルゴリズムが存在しないなら, LWE 問題を効率的に解くアルゴリズムは存在しないことを示している. また一方で, 任意の多項式因子 γ を持つ GapSVP_γ と SIVP_γ を解く多項式時間を持つ量子アルゴリズム [NC00] は存在しないと予想されており, このことから LWE 問題を解くことは困難であると予想されている.

ちなみに GapSVP_γ 問題とは, n 次元格子 L と与えらえた値 $d > 0$ に対し, $\lambda_1(L)$ を各々 L の最小ベクトルの長さ, $\lambda_n(L)$ を n 個の一次独立なベクトル集合に含まれる最大ベクトル長の最小値, $\gamma = \gamma(n)$ を 1 以上の近似因子として, $\lambda_1(L) \leq d$ なら Yes を, $\lambda_1(L) > \gamma(n)d$ なら No を返す問題であり, SIVP_γ とは, 同じく L に対して, 長さ $\gamma(n) \cdot \lambda_n(L)$ 以下の n 個の一次独立なベクトルを求める問題である.

その他, 安全性証明に関連する結果として, 文献 [LMSV12] では, ring-LWE 問題をベースとした Somewhat Homomorphic Encryption スキーム (演算回数に制約がある準同型暗号スキームで, 完全準同型暗号スキームの構成要素) が IND-CCA1 を満たすことが示されている.

3.2.2 LWE 問題の困難性の実験評価

Lindner と Peikert [LP11] は, LWE 問題の困難性について NTL ライブラリ (具体的には, NTL ライブラリ内の BKZ アルゴリズムを利用) を用いて実際の攻撃実験を行い, その困難性評価指標を定めている. ここでは, 彼らの困難性評価指標について, 簡単にまとめておく. まず, 彼らが評価対象とした decision version の LWE 問題を以下で正確に定義する.

定義 3.5 (decision version, $\mathsf{LWE}_{n,q,\chi}$) 定義 3.1 で与えたように, $n \geq 1$ と $q \geq 2$ と, $\mathbb{F}_q$ 上の確率分布 χ を考える (ただし, 文献 [LP11] では, 確率分布 χ は $\mathbb{Z}$ 上の標準偏差 σ を持つ離散ガウス分布 $D_{\mathbb{Z},\sigma}$ から生成されたものにしている). このとき, 秘密情報 $\vec{s} \in \mathbb{F}_q^n$ に対し, 定義 3.1 で紹介した $A_{\vec{s},\chi}$ からランダムにサンプリングされた元 $(\vec{a}, \langle \vec{a}, \vec{s} \rangle + e)$ と, $\mathbb{F}_q^n \times \mathbb{F}_q$ 上の一様分布で得られる元とを区別する問題を $\mathsf{LWE}_{n,q,\chi}$ と定義する.

上記で定義した $\mathsf{LWE}_{n,q,\chi}$ 問題に対して, 文献 [LP11] で Lindner-Peikert は 2 つの効率的な攻撃手法を紹介している.

- distinguishing attack (Micciancio-Regev[MR07] が提案)
- decoding attack (Lindner-Peikert 自身が文献 [LP11] で提案)

文献 [LP11] によると, decoding attack よりも distinguishing attack の方が常に効率的であるが, 実際の攻撃評価結果 [LP11, Figure 4 in Section 6] を比べてみると, $\varepsilon = 2^{-32}$ または $\varepsilon = 2^{-64}$ 程度の実用的なレベルの advantage を想定した場合には, 上記 2 つの攻撃の効率性は同程度であったという結果を得たとのこと.

■Distinguishing attack **による攻撃原理** そこで, 以下では $\mathsf{LWE}_{n,q,\chi}$ 問題に対する distinguishing attack の攻撃原理を少し紹介しておく. 秘密情報 $\vec{s} \in \mathbb{F}_q^n$ に対し, 集合 $A_{\vec{s},\chi}$ からランダムにサンプリングされた元

$$\vec{a}_i \in \mathbb{F}_q^n,\ b_i = \langle \vec{a}_i, \vec{s} \rangle + e_i \in \mathbb{F}_q \tag{3.1}$$

を数多く (ここでは m 個) 集めることで, 以下の情報を得ることができる (ここでは, すべてのベクトルは n-次元の行ベクトルで表記したとする):

$$\mathbf{A} = (\vec{a}_1^T, \vec{a}_2^T, \ldots, \vec{a}_m^T) \in \mathbb{F}_q^{n \times m}, \vec{b} = (b_1, b_2, \ldots, b_m) \in \mathbb{F}_q^m, \vec{e} = (e_1, e_2, \ldots, e_m) \in \mathbb{Z}^m$$

すると, 上記の記法を用いると, 関係式 (3.1) から

$$\vec{b} = \vec{s} \cdot \mathbf{A} + \vec{e} \pmod{q}$$

という関係式を得ることができる. そこで, $\mathbb{F}_q^n \times \mathbb{F}_q$ 上の一様分布で得られる元と区別するために, 攻撃者はまず (scaled な) 双対格子

$$\Lambda^{\perp}(\mathbf{A}) := \left\{ \vec{v} \in \mathbb{Z}^m \mid \vec{v} \cdot \mathbf{A}^T \equiv 0 \pmod{q} \right\}$$

の最短ベクトル $\vec{v} \neq \vec{0} \in \mathbb{Z}^m$ を見つけたとする. ここで, その攻撃者は内積値 $\langle \vec{v}, \vec{b} \rangle \pmod{q}$ が 0 に十分近いかどうかで $\mathbb{F}_q^n \times \mathbb{F}_q$ 上一様分布にサンプリングされた元かどうか判定することができる. その理由は, ベクトル $\vec{v}$ は $\vec{v} \cdot \mathbf{A}^T \equiv 0 \pmod{q}$ を満たすので,

$$\langle \vec{v}, \vec{b} \rangle \equiv \langle \vec{v}, \vec{s} \cdot \mathbf{A} + \vec{e} \rangle \equiv \langle \vec{v}, \vec{s} \cdot \mathbf{A} \rangle + \langle \vec{v}, \vec{e} \rangle \equiv \langle \vec{v}, \vec{e} \rangle \pmod{q}$$

となる. さらに, ベクトル $\vec{e} \in \mathbb{Z}$ の各成分 e_i は $\chi = D_{\mathbb{Z},\sigma}$ からサンプリングされた元なので, そのサイズは σ 程度となり, 上記の内積値 $\langle \vec{v}, \vec{b} \rangle$ のサイズはおよそ $\sigma \cdot ||\vec{v}||$ 程度となることが分かる. よって, 攻撃者は十分小さなベクトル $\vec{v} \in \Lambda^{\perp}(\mathbf{A})$ を見つけることができた場合, 上記の内積値の小ささを測ることで, $\mathbb{F}_q^n \times \mathbb{F}_q$ 上一様にサンプリングされた元か $A_{\vec{s},\chi}$ からサンプリングされた元か区別することができる.

■Distinguishing attack **に対する解読計算量評価** さらに, 文献 [MR07] によると, advantage ε を持つ攻撃者は双対格子 $\Lambda^{\perp}(\mathbf{A})$ から長さ $c \cdot q/\sigma$ を持つ格子元を見つけることができた場合, distinguishing attack を成功することができると示している (詳細は, [LP11, Section 6] を参照). ただし, $c \approx \sqrt{\log_2(1/\varepsilon)/\pi}$ とする. また一方, 格子縮約アルゴリズムはある格子の中からかなり短い格子元を出力するアルゴリズムで, その格子縮約アルゴリズムがどのくらい短い格子元を出力することが可能かを図る指標として, *root Hermite factor* という指標がよく用いられる (root Hermite factor の説明については, [GN08] を参照). d-次元の格子 L に対して,

$$\delta := \left(\frac{||\vec{b}_1||}{|\det(L)|^{1/d}} \right)^{1/d}$$

の値を格子縮約アルゴリズムの root Hermite factor と呼ぶ. ただし, 格子縮約アルゴリズムを出力される格子基底を $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_d\}$ とし, その長さを $||\vec{b}_i||$ と表す (さらに, $||\vec{b}_1|| \leq ||\vec{b}_2|| \leq \cdots$ と仮定). そこで, distinguishing attack を用いて, $\mathsf{LWE}_{n,q,\chi}$ 問題を解くためには, 攻撃に利用する格子縮約アルゴリズムの root Hermite factor δ は

$$c \cdot q/\sigma = \delta^m \cdot |\det(\Lambda^{\perp}(\mathbf{A}))|^{1/m} = \delta^m \cdot q^{n/m}$$

の条件を満たす必要がある. さらに, distinguishing attack に最適な格子次元 $m = \sqrt{n \log_2(q)/\log_2(\delta)}$ を想定した場合, 上記の関係式から

$$c \cdot q/\sigma = 2^{2\sqrt{n \log_2(q) \log_2(\delta)}} \tag{3.2}$$

という n, q, σ の関係式を新たに得ることができる.

一方, BKZ アルゴリズムは効率的な格子縮約アルゴリズムであることが知られている. そこで, Lindner-Peikert [LP11] は NTL ライブラリで実装済みの BKZ アルゴリズムを利用した場合の distinguishing attack の計算量 T_{BKZ} に対して,

$$\log_2(T_{\mathrm{BKZ}}) = \frac{1.8}{\log_2(\delta_{\mathrm{BKZ}})} - 110 \tag{3.3}$$

という見積もり値を示している. ただし, ここでの δ_{BKZ} は BKZ アルゴリズムの root Hermite factor で, その指標値は BKZ アルゴリズムのブロックサイズに関するパラメータにより定まる (ブロックサイズが大きくなるほど root Hermite factor は小さくなるため, distinguishing attack の計算量 T_{BKZ} は増大する). 表 3.2[*1] に, 文献 [DPSZ12, Appendix D] で示されている T_{BKZ} と δ_{BKZ} の関係式を示した表を紹介しておく. 表 3.2 から分かることは, BKZ アルゴリズムを利用した攻撃に対して $\mathsf{LWE}_{n,q,\chi}$ 問題のセキュリティレベルを 80-bit 程度以上に保つためには, root Hermite factor $\delta = 1.0066$ に対し, 関係式 (3.2) を満たすように $n, q, \chi = D_{\mathbb{Z},\sigma}$ のパラメータを選択する必要があることを示している. しかし, Lindner-Peikert による見積もり攻撃評価 (3.3) は, NTL ライブラリ実装による BKZ アルゴリズムに関するもので, すでに最新の実装結果ではないことに注意. 現在知られている BKZ アルゴリズムは, Chen-Nguyen ら [CN11] が実装した BKZ 2.0 というアルゴリズムが代表的で, 彼ら自身のアルゴリズム評価によると, 80-bit セキュリティを得るためには, BKZ アルゴリズムの root Hermite factor が 1.0050 程度以下を想定する必要があることを示している.

表 3.2 $\log_2(T_{\mathrm{BKZ}})$ と δ_{BKZ} の関係 [DPSZ12, Appendix D]

$\log_2(T_{\mathrm{BKZ}})$	80	100	128	192	256
δ_{BKZ}	1.0066	1.0059	1.0052	1.0041	1.0034

[*1] 表 3.2 における $\log_2(T_{\mathrm{BKZ}})$ の 192 は元論文では 196 と記載されているが, 誤植であろうと考えられる.

■近年の攻撃研究の動向 [BG14] では LWE 問題の特殊な場合に有効な攻撃手法を提案している. 具体的には, 定義 3.1 で紹介した LWE 問題において, 秘密情報 $\vec{s} \in \mathbb{F}_q^n$ と取り方として, $\vec{s} \leftarrow \{-1, 0, 1\}^n$ と限定する binary-LWE 問題について考察している. この binary-LWE 問題に対して, [BG14] では 3.2.2 節で少し紹介した decoding attack をベースとした攻撃手法を提案している. より具体的には, binary-LWE 問題を inhomogeneous short integer solution(ISIS) 問題に帰着させて解く手法を示しており (ISIS 問題: $(\mathbf{A}, \vec{v})$ が与えられた時, $\vec{v} \equiv \mathbf{A}\vec{y} \pmod q$ を満たす短い整数ベクトル $\vec{y}$ を見つける問題), 通常の攻撃よりも非常に効率的であることを理論的かつ実験的にも示している.

3.2.3 アプリケーションのためのパラメータ設定について

LWE 問題を用いた暗号技術応用において, LWE 問題の困難性を十分保ちながら暗号プロトコルなどを正しく動作させるためのパラメータ設定は一般的にかなり難しい問題である. ここでは, これまで知られている LWE 問題におけるパラメータ設定の代表例を挙げておく：

- Lindner-Peikert らは, [LP11, Section 3] で Micciancio[Mic10] が概要を示した LWE 問題ベースの公開鍵暗号方式の具体的な構成方法を示し, さらに彼らは [LP11, Section 6] でその暗号方式に対する具体的なパラメータ例を [LP11, Figure 3] に示している. また近年では, 青野らは表 [ABPW13, Table 2] において [LP11] で挙げたパラメータの安全性を再評価する一方で, LWE ベースの proxy re-encryption(PRE) スキームの具体的なパラメータを [ABPW13, Table 1] で示し, その各パラメータの安全性を [ABPW13, Table 3] で評価している.
- LWE 問題をベースとした準同型暗号方式に関しては, AES 回路を暗号化したまま行うために, Gentry-Halevi-Smart ら [GHS12b] が [BGV12] で提案されたレベル付き完全準同型暗号の具体的なパラメータ設定方法を示している. 一方, 完全準同型暗号ではなく限定回の加算と乗算が可能な somewhat 準同型暗号の具体的なパラメータとして, Lauter-Naehrig-Vaikuntanathan ら [LNV11] が [BV11] で提案された somewhat 準同型暗号を利用して, 平均・標準偏差・ロジスティック回帰などの統計計算を暗号化したまま行うための具体的なパラメータを表 [LNV11, Table 1] で示している.

3.3 まとめ

LWE (Learning with Errors) 問題は, Machine Learning(機械学習理論) から派生した問題で, GapSVP 及び SIVP の困難性に関する仮定のもとで解くことが難しいことが知られており, 本問題を効率的に解くことは困難であると予想されている. 現在までに完全準同型暗号スキームをはじめとした, 様々な公開鍵暗号スキームのベースがこの LWE 問題をベースとして提案されており, 今後も安全な暗号を構成する上で重要な要素となると考えられる. 現在までに知られている LWE 問題を解く最良アルゴリズムは指数時間の計算量を持っている. ただし, 実際の LWE 問題をベースとした暗号スキームの構成の際には, BKZ アルゴリズムなどの格子縮約アルゴリズムに対し耐性を持つようにパラメータ設定を行う必要があり, 安全でかつ演算機能等の要件を満足するような LWE パラメータを選択するための, 統一的な方法は知られておらず, 今後の課題となっている. また, LWE 問題に対する攻撃実験評価に関する結果もあまり知られていないため, 今後は計算機実験に関する研究も非常に重要になると思われることから, 安全性理論評価はもちろん攻撃実験評価の視点からも, 今後の動向に注意する必要がある.

第 3 章の参照文献

[ABB10] S. Agrawal, D. Boneh and X. Boyen, “Efficient Lattice (H)IBE in the Standard Model,” In *Advances in Cryptology–EUROCRYPT 2010*, Springer LNCS 6110, pp. 553–572, 2010.

[ABPW13] Y. Aono, X. Boyen, L. T. Phong and L. Wang, “Key-Private Re-Encryption under LWE,” In *Progress in Cryptology–INDOCRYPT 2013*, Springer LNCS 8250, pp. 1–18, 2013.

[ACPS09] B. Applebaum, D. Cash, C. Peikert and A. Sahai, “Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems,” In *Advances in Cryptology–CRYPTO 2009*, Springer LNCS 5677, pp. 595–618, 2009.

[AGV09] A. Akavia, S. Goldwasser and V. Vaikuntanathan, “Simultaneous Hardcore Bits and Cryptography against Memory Attacks,” In *Theory of Cryptography–TCC 2009*, Springer LNCS 5444, pp. 474–495, 2009.

[BG14] S. Bai and S. D. Galbraith, “Lattice Decoding Attacks on Binary LWE,” In *–Australasian Conference on Information Security and Privacy–ACISP 2014*, Springer LNCS 8544, pp. 322–337, 2014.

[BGV12] Z. Brakerski, C. Gentry and V. Vaikuntanathan, “(Leveled) fully homomorphic encryption without bootstrapping,” In *Innovations in Theoretical Computer Science–ITCS 2012*, ACM, pp. 309–325, 2012.

[BV11] Z. Brakerski and V. Vaikuntanathan, “Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages,” In *Advances in Cryptology–CRYPTO 2011*, Springer LNCS 6841, pp. 505–524, 2011.

[CHKP10] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert, “Bonsai Trees, or How to Delegate a Lattice Basis,” Journal of Cryptology, **25**(4) (2012), pp. 601–639 (Preliminary version was presented at EUROCRYPT 2010), 2012.

[CN11] Y. Chen and P. Q. Nguyen, “BKZ 2.0: Better Lattice Security Estimates,” In *Advanecs in Cryptology–ASIACRYPT 2011*, Springer LNCS 7073, pp. 1–20, 2011.

[DGK10] Y. Dodis, S. Goldwasser, Y. Kalai, C. Peikert and V. Vaikuntanathan, “Public-Key Encryption Schemes with Auxiliary Inputs,” In *Theory of Cryptography–TCC 2010*, Springer LNCS 5978, pp. 361–381, 2010.

[DPSZ12] I. Damgård, V. Pastro, N. P. Smart and S. Zakarias, “Multiparty Computation from Somewhat Homomorphic Encryption,” In *Advances in Cryptology–CRYPTO 2012*, Springer LNCS 7417, pp. 643–662, 2012.

[DQ13] N. Döttling and J. Müller-Quade, “Lossy Codes and a New Variant of the Learning-With-Errors Problem,” In *Advances in Cryptology–EUROCRYPT 2013*, Springer LNCS 7881, pp. 18–34, 2013.

[GN08] N. Gama and P. Q. Nguyen, "Predicting Lattice Reduction," In *Advances in Cryptolog–EUROCRYPT 2008*, Springer LNCS 4965, pp. 31–51, 2008.

[Gen09] C. Gentry, "Fully homomorphic encryption using ideal lattices," In *Proc. 41st ACM Symp. on Theory of Computing–STOC 2009*, ACM, pp. 169–178, 2009.

[GHS12a] C. Gentry, S. Halevi and N. P. Smart, "Fully Homomorphic Encryption with Polylog Overhead," In *Advances in Cryptology–EUROCRYPT 2012*, Springer LNCS 7237, pp. 465–482, 2012.

[GHS12b] C. Gentry, S. Halevi and N. P. Smart, "Homomorphic Evaluation of the AES Circuit," In *Advances in Cryptology–CRYPTO 2012*, Springer LNCS 7417, pp. 850–867, 2012.

[GHPS12] C. Gentry, S. Halevi, C. Peikert and N. P. Smart, "Ring Switching in BGV-Style Homomorphic Encryption," In *Security and Cryptography for Networks–SCN 2012*, Springer LNCS 7485, pp. 19–37, 2012.

[GKPV10] S. Goldwasser, Y. Kalai, C. Peikert and V. Vaikuntanathan, "Robustness of the Learning with Errors Assumption," In *Innovation in Computer Science–ICS 2010*, Tsinghua University, pp. 230–240, 2010.

[GPV08] C. Gentry, C. Peikert and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," In *Proc. 40th ACM Symp. on Theory of Computing–STOC 2008*, ACM, pp. 197–206, 2008.

[KTX07] A. Kawachi, K. Tanaka and K. Xagawa, "Multi-bit Cryptosystems Based on Lattice Problems," In *Public Key Cryptography–PKC 2007*, Springer LNCS 4450, pp. 315–329, 2007.

[LMSV12] J. Loftus, A. May, N. P. Smart, F. Vercauteren, "On CCA-Secure Somewhat Homomorphic Encryption," In *Selected Areas in Cryptology–SAC 2011*, LNCS 7118, pp. 55–72. 2012.

[LNV11] K. Lauter, M. Naehrig and V. Vaikuntanathan, "Can homomorphic encryption be practical?," In *ACM workshop on Cloud computing security workshop–CCSW 2011*, ACM, pp. 113–124, 2011.

[LP11] R. Lindner and C. Peikert, "Better Key Sizes (and Attacks) for LWE-Based Cryptography," In *RSA Conference on Topics in Cryptology–CT-RSA 2011*, Springer LNCS 6558, pp. 319–339, 2011.

[LPR10] V. Lyubashevsky, C. Peikert and O. Regev, "On Ideal Lattices and Learning with Errors over Rings," In *Advances in Cryptology–EUROCRYPT 2010*, Springer LNCS 6110, pp. 1–23, 2010.

[LPR13] V. Lyubashevsky, C. Peikert and O. Regev, "A Toolkit for Ring-LWE Cryptography," In *Advances in Cryptology–EUROCRYPT 2013*, Springer LNCS 7881, pp. 35–54, 2013.

[Mic10] D. Micciancio, "Duality in Lattice Cryptography," Invited talk at Public Key Cryptography–PKC 2010.

[MP13] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with Small Parameters," In *Advances in Cryptology–CRYPTO 2013*, Part I, Springer LNCS 8042, pp. 21–39, 2013.

[MR07] D. Micciancio and O. Regev, "Worst-Case to Average-Case Reduction Based on Gaussian measures," SIAM J. Computing **37**(1) (2007), pp. 267–302, 2007.

[MR09] D. Micciancio and O. Regev, "Lattice-based Cryptography," Post–Quantum Crytography, Springer, pp. 147–191, 2009.

[NC00] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[Pei09] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problems: extended abstract," In *Proc. 41st ACM Symp. on Theory of Computing–STOC 2009*, ACM, pp. 333–342, 2009.

[PVW08] C. Peikert, V. Vaikuntanathan and B. Waters, "A Framework for Efficient and Composable Oblivious Transfer," In *Advances in Cryptology–CRYPTO 2008*, Springer LNCS 5157, pp. 554–571, 2008.

[PW08] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications," In *Proc. 40th ACM Symp. on Theory of Computing–STOC 2008*, ACM, pp. 187–196, 2008.

[Reg05] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, **56**(6) (2009), pp. 1–40 (Preliminary version was presented at STOC 2005), 2009.

[Reg] O. Regev, "The Learning with Errors Problem," survey paper, available at `http://www.cims.nyu.edu/~regev/papers/lwesurvey.pdf`.

[Reg09] O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," (2009), available at `http://www.cims.nyu.edu/~regev/papers/qcrypto.pdf`.

[SV11] N. P. Smart and F. Vercauteren, "Fully homomorphic SIMD operations," Designs, Codes and Cryptography, April 2014, Volume 71, Issue 1, pp. 57–81, 2014.

第 4 章

LPN

本章では, Learning with Parity Noise (LPN) 問題を用いた様々な暗号技術へのアプリケーションの紹介と, LPN 問題や符号に関連する問題の困難性についての調査結果を述べる.

4.1 Learning Parity with Noise (LPN) 問題の概説

4.1.1 LPN 問題とは

LPN 問題とは誤差付きの線型方程式を解けるかどうかという問題である. 1993 年に, Blum, Furst, Kearns, Lipton [BFKL93] が困難と思われる問題として挙げ, 定式化を行った. 第 3 章において, この問題を一般化した LWE 問題を既に扱っている.

以下では $\mathbb{F}_q$ で位数が q の有限体を表す. Ber_τ でパラメータ τ のベルヌーイ分布を表すことにする. (確率 τ で 1, 確率 $1-\tau$ で 0 となる $\mathbb{F}_2$ 上の分布である.) また, 自然数 $k \geq 1$ について, Ber_τ^k で, Ber_τ から独立に k 個サンプルを取ったときの $\mathbb{F}_2^k$ 上の分布を表す.

■LPN 問題: $\mathbb{F}_2$ 上の分布 χ および $\vec{s} \in \mathbb{F}_2^n$ について, オラクル $\mathcal{O}_{\vec{s},\chi}$ を以下で定義する. (1) $\vec{a}$ を $\mathbb{F}_2^n$ からランダムに選び, (2) e を分布 χ に従い選び, (3) $b = \vec{s} \cdot \vec{a}^\top + e$ と計算し, (4) $(\vec{a}, b)$ を出力する. 定義より, このオラクルは第 3 章定義 3.1 で定義される分布 $A_{\vec{s},\chi}$ からのサンプル $(\vec{a}, b) \in \mathbb{F}_2^{n+1}$ を返す. また, オラクル $\mathcal{U}$ を $(\vec{a}, b) \leftarrow \mathbb{F}_2^{n+1}$ とランダムな組を出力するオラクルとして定義する.

定義 4.1 (探索版 LPN 問題) 探索版 LPN 問題とは, オラクル $\mathcal{O}_{\vec{s},\chi}$ へのアクセスが可能なときに, $\vec{s}$ を出力する問題である.

特に $\chi = \mathsf{Ber}_\tau$ のとき, $\mathsf{LPN}_{n,\tau}$ 問題と呼ぶ. また $\mathsf{LPN}_{n,\tau}$ 問題でオラクルからのサンプル数が $m = m(n)$ に制限されるものを, $\mathsf{LPN}_{n,m,\tau}$ 問題と呼ぶ.

定義 4.2 (探索版 LPN 仮定) $\mathbb{F}_2$ 上の確率分布 χ について, 敵 $\mathcal{A}$ の優位性を

$$\mathsf{Adv}_{\mathcal{A}}(n) = \Pr_{\vec{s} \leftarrow \mathbb{F}_2^n}[\mathcal{A}^{\mathcal{O}_{\vec{s},\chi}}(1^n) = \vec{s}]$$

で定義する. 任意の多項式時間の敵 $\mathcal{A}$ について, その優位性が無視できるとき, 探索版 LPN 仮定が成立するという.

暗号プリミティブや暗号プロトコルの安全性証明のために, 判定版 LPN 仮定を用いることも多い. 判定版 LPN 問題と判定版 LPN 仮定は以下で定義される.

定義 4.3 (判定版 LPN 問題) 判定版 LPN 問題とは, オラクル $\mathcal{O}_{\vec{s},\chi}$ またはオラクル $\mathcal{U}$ へのアクセスが与えられたときに, どちらのオラクルにアクセスしているかを判定する問題である.

定義 4.4 (判定版 LPN 仮定) $\mathbb{F}_2$ 上の確率分布 χ について, 敵 $\mathcal{A}$ の優位性を

$$\mathsf{Adv}_{\mathcal{A}}(n) = \left| \Pr_{\vec{s}\leftarrow\mathbb{F}_2^n}[\mathcal{A}^{\mathcal{O}_{\vec{s},\chi}}(1^n) = 1] - \Pr[\mathcal{A}^{\mathcal{U}}(1^n) = 1] \right|$$

で定義する. 任意の多項式時間の敵 $\mathcal{A}$ について, その優位性が無視できる関数であるとき, 判定版 LPN 仮定が成立するという.

探索版 LPN 問題にはランダム自己帰着が存在する [BFKL93]. すなわち, ランダムに選ばれた $\vec{s} \in \mathbb{F}_2^n$ について探索版 LPN 問題を解けるならば, 任意の $\vec{s} \in \mathbb{F}_2^n$ について探索版 LPN 問題を解くことが出来る.

Katz, Shin, Smith [KSS10] によれば, [BFKL93, Reg09] と同様に判定版 LPN 仮定を探索版 LPN 仮定に帰着することが出来る.

定理 4.5 ([KSS10]) 判定版 $\mathsf{LPN}_{n,\tau}$ 仮定を破る t ステップ, m 回のクエリ, 優位性 δ の敵が存在すると仮定する. このとき, 探索版 $\mathsf{LPN}_{n,\tau}$ 仮定を破る t' ステップ, m' 回のクエリ, 優位性 δ' の敵が存在する. ここで,

$$t' = O(\delta^{-2} tn \log n),\ m' = O(\delta^{-2} m \log n),\ \delta' \geq \delta/4.$$

■変種:　以上に列挙した LPN 問題・仮定では, 基礎となる体として $\mathbb{F}_2$ を用いていた. 体を $\mathbb{F}_q$ に変更した LPN 問題・仮定が用いられることもある. 特に q を素数とした場合には LWE 問題と非常によく似た問題・仮定となるが, 誤差分布 χ の定義が異なることが多い.

LWE 問題では剰余環 $\mathbb{Z}_q$ を用いている. 応用の観点からは, 誤差分布 χ からのサンプル x の絶対値が高い確率で小さいことが重視される.

一方, LPN 問題では有限体 $\mathbb{F}_q$ を用いている. また, 符号からの要求としてハミング重みを考えることが多いため, 誤差分布 χ は 0 を取る確率が大きいことが求められる. たとえば, ベルヌーイ分布の一般化として, 確率 τ で 0 を確率 $1-\tau$ で $\mathbb{F}_q \setminus \{0\}$ のランダムな値を取る分布が用いられる. これは格子問題と符号問題のアナロジーとして考えることができる.

4.1.2　LPN 問題の拡張

4.1.2.1　復号問題

オラクルからのサンプル数を固定し $m = m(n)$ とする. $\mathsf{LPN}_{n,m,\tau}$ 問題での m 個のサンプル $(\vec{a}_1, b_1), (\vec{a}_2, b_2), \ldots, (\vec{a}_m, b_m)$ を行列・ベクトル表示して,

$$\boldsymbol{A} = [\vec{a}_1^\top \vec{a}_2^\top \cdots \vec{a}_m^\top] \in \mathbb{F}_2^{n\times m},\ \vec{b} = \vec{s}\cdot\boldsymbol{A} + \vec{e}$$

とする. 符号理論の観点からは, ランダム行列 $\boldsymbol{A}$ を生成行列とする線形符号の受信語 $\vec{b}$ から元のメッセージ $\vec{s}$ を復元する問題と捉えることができる.

4.1.2.2　シンドローム復号問題

先ほど挙げた復号問題の “双対” として, シンドローム復号問題が挙げられる. シンドローム復号問題 $\mathsf{SD}_{k,m,w}$ とは,

$$\boldsymbol{H} = [\vec{h}_1^\top \vec{h}_2^\top \cdots \vec{h}_m^\top] \in \mathbb{F}_2^{k\times m},\ \vec{u} \in \mathbb{F}_2^k$$

および自然数 w が与えられた時に, $\vec{e}\cdot\boldsymbol{H}^\top=\vec{u}$ かつハミング重みが w 以下となる $\vec{e}\in\mathbb{F}_2^m$ を求める問題である.

$\boldsymbol{H}$ として $\boldsymbol{A}$ で生成される符号のパリティ検査行列を取り, $\vec{u}$ として $\vec{b}\cdot\boldsymbol{H}^\top(=\vec{e}\cdot\boldsymbol{H}^\top)$ をとれば, $\mathsf{LPN}_{n,m,\tau}$ 問題や復号問題をシンドローム復号問題 $\mathsf{SD}_{m-n,m,O(\tau m)}$ に変換可能である.

4.1.2.3 Exact-LPN 問題

誤差分布として, $\vec{e}\leftarrow\mathsf{Ber}_\tau^m$ ではなく, ハミング重みが丁度 w のものだけを考える. このように誤差分布を変えた問題を Exact-LPN 問題と呼ぶ.

4.1.2.4 Sparse-LPN 問題

一部の暗号方式では, $\vec{s}$ のハミング重みが小さい, すなわち, 疎 (sparse) であることを要求する. Applebaum ら [ACPS09] は $\vec{s}$ を誤差分布である χ^n から選んだ場合の LPN 問題と $\vec{s}$ を $\mathbb{F}_2^n$ からランダムに選んだ場合の問題とが等価であることを示している.

4.1.2.5 Subspace-LPN 問題

Pietrzak [Pie12a] は, 敵のオラクルへのクエリを強めた問題として, 以下の Subspace-LPN 問題を考察した. LPN 仮定で定義されたオラクルを $\mathcal{O}_{\vec{s},\chi}$ から以下で定義される $\mathcal{O}'_{\vec{s},\chi}$ に変更する. 二つの Affine 関数 $\phi_a(\vec{a})=\vec{a}\boldsymbol{X}_a+\vec{x}_a$, $\phi_s(\vec{s})=\vec{s}\boldsymbol{X}_s+\vec{x}_s$, $(\boldsymbol{X}_a,\boldsymbol{X}_s\in\mathbb{F}_2^{n\times n},\vec{x}_a,\vec{x}_s\in\mathbb{F}_2^n,)$ をクエリとして受け取り, $\mathrm{rank}(\boldsymbol{X}_a^\top\boldsymbol{X}_s)\geq d+\delta$ ならば, $\vec{a}\leftarrow\mathbb{F}_2^n$ および $b=\phi_s(\vec{s})\cdot\phi_a(\vec{a})^\top+e$ を出力する.

Pietrzak は, $2^{-\delta+1}$ が無視できるならば, 新しいオラクル $\mathcal{O}'_{\vec{s},\chi}$ を用いた Subspace-LPN 問題は, 次元 d の LPN 問題と困難性が等価であることを示した.

4.1.2.6 Toeplitz-LPN 問題

Gilbert, Robshaw, Seurin [GRS08] が認証プロトコルの効率化のために導入した.

行列 $\boldsymbol{A}=\{a_{i,j}\}\in\mathbb{F}_2^{n\times m}$ が Toeplitz 行列であるとは, 任意の i,j について $a_{i-1,j-1}=a_{i,j}$ が成立することである. Toeplitz 行列を表現するには左端の列ベクトルおよび最も上の行ベクトルがあれば良い. そのため $\boldsymbol{A}$ の表現は $n+m-1$ ビットで可能である.

復号問題の節で, 探索版 LPN 問題でのサンプル $(\vec{a}_1,b_1),(\vec{a}_2,b_2),\ldots,(\vec{a}_m,b_m)$ を行列・ベクトル表示して,

$$\boldsymbol{A}=[\vec{a}_1^\top\vec{a}_2^\top\cdots\vec{a}_m^\top]\in\mathbb{F}_2^{n\times m},\ \vec{b}=\vec{s}\cdot\boldsymbol{A}+\vec{e}$$

を考えた. オラクル $\mathcal{O}$ (および $\mathcal{U}$) を変更し, $\boldsymbol{A}$ が必ず Toeplitz 行列になる場合の LPN 問題を考える. これを Toeplitz-LPN 問題と呼ぶ.

4.1.2.7 Ring-LPN 問題

Heyse, Kiltz, Lyubashevsky, Paar, Pietrzak [HKL+12] は, Ring-LPN 問題を定義した. この問題は ring-LWE 問題 (定義 3.2) と同様に定義される.

定義 4.6 (探索版 Ring-LPN 問題) 適当な n 次の $\mathbb{F}_q$ 係数多項式 $f(x)$ を考え, 環 $R_q=\mathbb{F}_q[x]/(f(x))$ を固定する. R_q 上の確率分布 χ を固定する.

R_q 上の誤差分布 χ および $s\in R_q$ について, オラクル $\mathcal{O}_{\vec{s},\chi}$ を以下で定義する. (1) a を R_q からランダムに選び, (2) e を分布 χ に従い選び, (3) $b=sa+e$ と計算し, (4) $(a,b)\in R_q^2$ を出力する.

探索版 Ring-LPN 問題とは, オラクル $\mathcal{O}_{s,\chi}$ へのアクセスが可能なときに, $s \in R_q$ を出力する問題である.

4.2 LPN 問題のアプリケーション

90 年代から様々な応用が提案されている.

擬似乱数生成器 Blum, Furst, Kearns, Lipton [BFKL93] による疑似乱数生成器が有名である. Fischer, Stern [FS96] の構成や Appelbaum, Cash, Peikert, Sahai [ACPS09] による構成も知られている

共通鍵による両側認証 Hopper と Blum によって, 後に HB プロトコルと呼ばれる認証プロトコルが提案された [HB01]. 多くの変種が提案されており, 現在も研究が続けられている.

共通鍵暗号 Gilbert, Robshaw, Seurin [GRS08] による LPN-C と呼ばれる IND-CPA 安全な共通鍵暗号方式がある. Applebaum, Cash, Peikert, Sahai [ACPS09] は, LPN-C の変種が KDM-CPA 安全であることを示した. また Applebaum, Harnik, Ishai [AHI11] は ACPS09 の共通鍵方式が RKA-CPA 安全であることを示し, OT への応用を考察している. Applebaum [App13] は ACPS09 の共通鍵方式が RKA-KDM-CPA 安全であることを示し, このような方式を用いれば, Free-XOR 構成を用いた Yao's GC が標準モデルで安全であることを示した.

署名 大別して二つのタイプがある.

- Fiat-Shamir 変換によるもの: Stern の認証方式や Veron の認証方式に Fiat-Shamir 変換を施すことによって得られる署名である. 署名長の観点から効率が悪く実用には向いていない.
- Full-Domain Hash によるもの: CFS 署名が知られている.

今までのところ標準モデルでの安全性証明は行われていない.

公開鍵暗号 大きく分けて二つの系統がある.

- Alekhnovich 暗号: Alekhnovich [Ale11] 暗号は LPN 仮定のみから IND-CPA 安全性を証明可能な方式である. IND-CCA2 版は Döttling, Müller-Quade, Nasciment [DMQN12] によって構成されている.
- McEliece 暗号または Niederreiter 暗号: McEliece [McE78] および Niederreiter [Nie86] によって提案された暗号である. Li, Deng, Wang [LDW94] が「Niederreiter 暗号の OW-CPA 性は McEliece 暗号の OW-CPA 性と等価である」ことを示している.
  - McEliece 暗号の派生: Kobara, Imai [KI01] は McEliece 暗号用のパディング方法を提案し, その方式がランダムオラクルモデルで ND-CCA2 安全であることを示した. Nojima, Imai, Kobara, Morozov [NIKM08] は McEliece 暗号の変種が標準モデルで IND-CPA 安全でああることを示した. McEliece 暗号を基にした IND-CCA2 暗号については [DDMQN12] や Persichetti [Per13] に構成が見られる.
  - Niederreiter 暗号の派生: 標準モデルで IND-CCA2 安全な Niederreiter ベースの暗号として, Freeman, Goldreich, Kiltz, Rosen, Segev の構成 [FGK+13] や, Mathew, Vasant, Venkatesan, Rangan の構成 [MVVR12] が知られている.

紛失転送 McEliece 暗号を用いた紛失転送プロトコルが提案されている [DvdGMQN12, DNdS12, DNMQ12].

以下では, LPN 仮定に基づく公開鍵暗号方式の例として Alekhnovich 暗号を取りあげる. また, 追加の仮定が必要であるが Alekhnovich 暗号よりも効率が良い公開鍵暗号方式の例として McEliece 暗号を取り上げる.

4.2.1 Alekhnovich 暗号 [Ale11]

Alekhnovich は [Ale11] で 2 つ公開鍵暗号方式を提案している. ここではシンプルな 1 つ目の暗号方式を取り上げる. パラメータを以下とする.

- n: 安全性パラメータ
- m: LPN サンプルの個数 (例: $m = 2n + 1$)
- $\tau > 0$: 誤差パラメータ (例: $\tau = n^{-1/2-\epsilon}$)

このとき Alekhnovich 暗号は以下で構成される:

秘密鍵の生成: ランダムに $\vec{e} \leftarrow \mathsf{Ber}_\tau^m$ を選ぶ.

公開鍵の生成 ランダムに $\boldsymbol{A} \leftarrow \mathbb{F}_2^{n\times m}$ を選ぶ. ランダムに $\vec{s} \leftarrow \mathbb{F}_2^n$ を選ぶ. $\vec{b} = \vec{s}\boldsymbol{A} + \vec{e} \in \mathbb{F}_2^m$ を計算し, $\boldsymbol{B} = \binom{\boldsymbol{A}}{\vec{b}}$ とする. $\boldsymbol{M} \in \mathbb{F}_2^{(m-n-1)\times m}$ を $\ker(\boldsymbol{B}^\top)$ の基底とし, 公開鍵を $\boldsymbol{M}$ とする.

暗号化 平文が 0 の場合, $\vec{t} \leftarrow \mathbb{F}_2^{m-n-1}$ と $\vec{f} \leftarrow \mathsf{Ber}_\tau^m$ をランダムに選び, $\vec{c} = \vec{t}\boldsymbol{M} + \vec{f} \in \mathbb{F}_2^m$ を出力する.
平文が 1 の場合, ランダムに $\vec{c} \leftarrow \mathbb{F}_2^m$ を選び出力する.

復号 暗号文 $\vec{c} \in \mathbb{F}_2^m$ について, $\delta = \langle \vec{c}, \vec{e} \rangle$ を計算する. δ を出力する.

復号の正当性について以下考察する. 平文が 1 の場合, 復号は確率 $1/2$ で成功する.
一方, 平文が 0 の場合, $\vec{e} \in \mathrm{Span}(\boldsymbol{B})$ および $\vec{t}\boldsymbol{M} \in \ker(\boldsymbol{B}^\top)$ より $\vec{t}\boldsymbol{M}\vec{e}^\top = 0$ であることに注意すると,

$$\langle \vec{c}, \vec{e} \rangle = \vec{t}\boldsymbol{M} \cdot \vec{e}^\top + \vec{f}\vec{e}^\top = \langle \vec{f}, \vec{e} \rangle$$

なので, $\langle \vec{f}, \vec{e} \rangle = 0$ であれば復号に成功する. 誤り確率を評価すると, $\Pr[\langle \vec{f}, \vec{e} \rangle = 1] \approx (1-\tau)^{\tau m} = o(1)$ となり, $1 - o(1)$ の確率で復号に成功する. また, 上記の暗号方式の安全性については, 判定版 LPN 仮定の下で CPA 安全であることが証明される.

ここで紹介した暗号方式は, 1 ビット暗号であり, 復号誤りの確率も高いため実用的ではない. 効率的な方式としては 2 つ目の Alekhnovich 暗号や次に挙げる McEliece 暗号を参考にされたい.

4.2.2 McEliece 暗号

以下では, S_m で m 次対称群を表し, $\mathrm{GL}_n(\mathbb{F}_q)$ で n 次の $\mathbb{F}_q$ 要素正則行列全体がなす群を表す.

- n: 安全性パラメータ
- m: サンプルの個数
- τ: 誤差パラメータ (例: $\tau = cn$)
- t: 誤り訂正符号の誤り訂正能力 ($t = \Omega(\tau m)$)

鍵生成: 誤り訂正能力が t である (m, n)-線形符号の生成行列 $\boldsymbol{G}$ を生成する. $\boldsymbol{S} \leftarrow \mathrm{GL}_n(\mathbb{F}_2)$ をランダムに選ぶ. $\boldsymbol{P} \leftarrow S_m$ をランダムに選ぶ. $\boldsymbol{M} = \boldsymbol{SGP}$ とする.
公開鍵を $\boldsymbol{M}$ とし, 秘密鍵を $(\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{P})$ とする.

暗号化: 平文を $\vec{v} \in \mathbb{F}_2^n$ とする. 乱数 $\vec{e} \leftarrow \mathsf{Ber}_\tau^m$ を選び, 暗号文 $\vec{c} = \vec{v}\boldsymbol{M} + \vec{e}$ を計算する.

復号: $\hat{\vec{v}} = \vec{c}\boldsymbol{P}^{-1}$ を計算する. $\hat{\vec{v}}$ を誤り訂正符号で訂正し復号すると $\vec{v}' = \vec{v}\boldsymbol{S}$ を得る. $\vec{v} = \vec{v}'\boldsymbol{S}^{-1}$ を出力する.

復号の正当性は以下で確認される. $\vec{c} = \vec{v}\boldsymbol{M} + \vec{e}$ として, $\hat{\vec{v}} = \vec{c}\boldsymbol{P}^{-1}$ を計算すると,

$$\hat{\vec{v}} = \vec{v}\boldsymbol{M}\boldsymbol{P}^{-1} + \vec{e}\boldsymbol{P}^{-1} = \vec{v}\boldsymbol{S}\boldsymbol{G} + \vec{e}\boldsymbol{P}^{-1}$$

を得る. $\vec{v}\boldsymbol{S}\boldsymbol{G}$ は符号語であり, $\vec{e}\boldsymbol{P}^{-1}$ は誤りであり. $\vec{e}\boldsymbol{P}^{-1}$ の重みが t 以下であれば, 誤り訂正符号の復号により, $\vec{v}' = \vec{v}\boldsymbol{S}$ を得る. よって, 高い確率で復号に成功する.

平文 $\vec{v}$ および $\boldsymbol{M}$ がランダムであれば, 暗号文 $\vec{c}$ は LPN 仮定の下で疑似ランダムである. $\boldsymbol{M}$ が疑似ランダムであることを言うためには, McEliece 仮定と呼ばれる仮定が必要となる.

定義 4.7 (McEliece 仮定) $[m(n), n]_{q(n)}$-符号のクラス $\mathcal{C}$ を固定する. 敵 $\mathcal{A}$ の優位性を

$$\mathsf{Adv}_{\mathcal{A}}(n) = \left| \Pr_{\boldsymbol{S}\leftarrow \mathrm{GL}_n(\mathbb{F}_q), \boldsymbol{G}\leftarrow\mathcal{C}, \boldsymbol{P}\leftarrow S_m}[\mathcal{A}(1^n, \boldsymbol{M} = \boldsymbol{S}\boldsymbol{G}\boldsymbol{P}) = 1] - \Pr_{\boldsymbol{M}\leftarrow\mathbb{F}_q^{n\times m}}[\mathcal{A}(1^n, \boldsymbol{G}) = 1] \right|$$

で定義する. 任意の多項式時間の敵 $\mathcal{A}$ について, その優位性が無視できる関数であるとき, McEliece 仮定が成立するという.

左側の敵は McEliece 暗号の公開鍵 (または Niederreiter 暗号の公開鍵の双対) を受け取っている. そのため, この仮定は, McEliece 暗号の公開鍵はランダムな同サイズの行列と見分けが付かないということを意味する.

Faugère, Gauthier-Umaña, Otmani, Perret, Tillich [FGOPT13] は元となる Goppa 符号 (または Alternant 符号) のレートが高い場合には, McEliece 仮定を破るアルゴリズムを提案している. 暗号として用いる場合には, パラメータ設定によって彼らの攻撃を避けることが可能である.

■McEliece 暗号の変種の安全性について: 二元 Goppa 符号を用いた場合, 鍵サイズが大きくなることが知られている. そのため, 元となる符号を変更し, 鍵サイズや暗号文サイズを小さくする研究が進められてきた. しかし, 符号が特殊な場合には多くの方式が破られている. McEliece 暗号やその変種を用いる場合には, 符号の選定やパラメータの設定おいて, より一層の注意が必要である.

Bernstein, Lange, Peters が [BLP10] および [BLP11a] で q 元-Goppa 符号を用いた q 元-McEliece 暗号についてパラメータの提案を行っている.

■パラメータ設定について: Bernstein, Lange, Peters は [BLP10] および [BLP11a] で q 元-Goppa 符号を用いた q 元-McEliece 暗号についてパラメータの提案を行っている. 具体的なチャレンジ問題も入手可能である. [*1] たとえば 128-bit 安全性を考える際には, $(q, n, m, \tau m) = (2, 2325, 3009, 57)$ といったパラメータを提案している.

LPN 問題をベースとした暗号方式を実際に構成する際には, 4.3 節で挙げる各種のアルゴリズムに耐性を持つよう, パラメータ設定を行う必要がある. たとえば, Damgård と Park [DP12] は Alekhnovich 暗号の変種として公開鍵暗号を提案し, Bernstein と Lange の攻撃 [BL12] を元にしたパラメータ設定 (表 4.1) を行っている.

4.3 LPN 問題に対する評価

サンプル数を固定した場合, $\boldsymbol{A}$ および $\vec{b}$ の最悪時を考えると NP 困難になることが Berlekamp, McEliece, van Tilborg [BMvT78] によって示されている. また, Håstad [Hås01] により近似版 LPN 問題の NP 困難性も示されている.

[*1] http://pqcrypto.org/wild-challenges.html.

表 4.1 Damgård と Park によるパラメータ設定の例 ([DP12] より)

セキュリティレベル	n	τ
80-bit	9000	0.0044
112-bit	21000	0.0029
128-bit	29000	0.0024
196-bit	80000	0.0015
256-bit	145000	0.0011

しかし平均時の困難性についてはよく分かっていない. そのため LPN 問題を解くための提案されたアルゴリズムについて調査を行った.

$\mathsf{LPN}_{n,m,\tau}$ 問題を解くための素朴な方法として, 総当たり法がある. 閾値 $d \geq 1$ を固定する. $\vec{s} \in \mathbb{F}_2^n$ の候補ごとに, $\vec{e} = \vec{b} - \vec{s}\boldsymbol{A}$ を計算し, $\vec{e}$ のハミング重みが $(1+1/d)\tau m$ 以下であれば $\vec{s}$ を解として出力するというものである. Chernoff の補題から $\vec{e} \leftarrow \mathsf{Ber}_\tau^m$ としたとき, $d \geq 1$ について $\Pr[Hw(\vec{e}) \leq (1+1/d)\tau m] \leq \exp(-\tau m/3d^2)$ である. 従ってこの方法を用いると, 時間 $O(2^n)$ で圧倒的な確率で $\mathsf{LPN}_{n,m,\tau}$ 問題を解くことが可能である.

以降では, $O(2^n)$ 以下の時間で解を求めるアルゴリズムについて考察する. 現在では, 大別して 3 つのアルゴリズムが知られている.

1. Blum, Kalai, Wasserman [BKW03] の BKW アルゴリズム,
2. Arora, Ge [AG11] の「再線形化」アルゴリズム,
3. シンドローム復号問題として解くアルゴリズム

である.

4.3.1 BKW アルゴリズムおよびその改良

Blum, Kalai, Wasserman [BKW03] は BKW アルゴリズムと呼ばれるアルゴリズムを提案した.

基本アイデアは以下である. オラクルからのサンプル $(\vec{a}, b)$ が常に $\vec{a} = (1, 0, \ldots, 0)$ という形であれば, $b = s_1 + e$ となる. このようなサンプルを大量に集めれば, s_1 を多数決法で求めることが出来る. 一般に $\vec{u}_j$ を j 番目の単位ベクトルとして, $(\vec{u}_j, b)$ という形のサンプルを集めれば s_j を多数決法で求められる. そこでオラクル $\mathcal{O}_{\vec{s},\tau}$ からのサンプルを用いて, 上記のようなサンプルを生成することを目指す.

■BKW アルゴリズムの概要: $(t-1)k < n \leq tk$ を満たす適当な自然数 t, k を固定する. 以下では,

$$A_{\vec{s},\delta,i} := \{\vec{a} \leftarrow \mathbb{F}_2^{n-ik} \times \{0\}^{ik},\ e \leftarrow \mathsf{Ber}_{(1+\delta)/2} : (\vec{a}, \vec{s}\cdot\vec{a}^\top + e)\}$$

というオラクルを考える. $A_{\vec{s},\delta,i}$ から得たサンプル $(\vec{a}, b)$ は $\vec{a}$ の末尾から ik 個の要素が必ず 0 である. $i = 0$, $\delta = 1-2\tau$ とすれば, $A_{\vec{s},\delta,i} = \mathcal{O}_{\vec{s},\tau}$ となる.

基本アルゴリズムは以下である.

1. $A_{\vec{s},\delta,i}$ からのサンプルを L_0 個用意する.
2. $i = 0, 1, \ldots, t-2$ について, サイズ L_i の $A_{\vec{s},\delta,i}$ からのサンプルを用いて, $O(L_i)$ 時間でサイズ $L_{i+1} = L_i - 2^k$ の $A_{\vec{s},\delta^2,i+1}$ からのサンプルを構成する.
   - サンプル $(\vec{a}, b) \in L_i$ について, $\vec{a} = (a_1, a_2, \ldots, a_{n-ik}, 0, \ldots, 0) \in \mathbb{F}_2^n$ の $(a_{n-(i+1)k+1}, a_{n-(i+1)k+2}, , \ldots, a_{n-ik}) \in$

$\mathbb{F}_2^k$ に従って分類を行う.
- 各組で代表を一つとり, それを $(\vec{a}^*, b^*)$ とする.
- 各組の代表以外の要素 $(\vec{a}, b)$ を $(\vec{a} \oplus \vec{a}^*, b \oplus b^*)$ で置き換える.
- 全組をまとめてサイズ $L_i - 2^k$ の $A_{\vec{s},\delta^2,i+1}$ からのサンプルとする.

最終的に, サイズ $L_{t-1} = L - (t-1)2^k$ の $A_{\vec{s},\delta^{2^{t-1}},t-1}$ からのサンプルが得られる.

3. 得られた L_{t-1} 個の $A_{\vec{s},\delta^{2^{t-1}},t-1}$ からのサンプルを用いて, s_j を投票で決める.
   - $j = 1, 2, \ldots, n-(t-1)k$ について, $\vec{u}_j$ を $\mathbb{F}_2^n$ の標準基底 j 番目の単位ベクトルとする. サンプル $\{(\vec{a}_i, b_i)\}_{i=1,2\ldots,m}$ から ℓ 個のベクトルを $\vec{a}_{i_1} + \vec{a}_{i_2} + \cdots + \vec{a}_{i_\ell} = \vec{u}_j$ となるようにうまく選ぶ. このとき, $b_{i_1} + b_{i_2} + \cdots + b_{i_\ell} = s_j + e_{i_1} + \cdots + e_{i_\ell}$ となり, 誤差が 0 になる確率は $\Pr[e_{i_1} + e_{i_2} + \cdots + e_{i_\ell} = 0] > 1/2 + (1-2\delta^{2^{t-1}})^\ell/2$ で与えられる. 適当な回数この試行を行い, s_j を多数決投票で決めれば良い.

Blum らの見積もりでは, サンプル数および計算ステップ数は $\delta = 1-2\tau$ として, $\mathrm{poly}\left(\delta^{-2^t}, 2^k\right)$ であった. $\tau < 1/2$ を定数とし, $t = \frac{1}{2}\log n$, $k = 2n/\log n$ とすれば, $2^{O(n/\log n)}$ を得る.

■LF アルゴリズム: Levieil と Fouque [LF06] は BKW アルゴリズムの一部アルゴリズムを改良し LF アルゴリズムを提案した.

簡単のために $n = tk$ を仮定する. BKW アルゴリズムでは基本アルゴリズムのステップ 3 において $\vec{s}$ の各要素を 1 ビットずつ決定している. ステップ 3 において得られたサンプルは, $A_{\vec{s},\delta^{2^{t-1}},t-1}$ からのサンプルであるため, $((a_1, a_2, \ldots, a_k, 0, \ldots, 0), b)$ という形をしている. このとき, $b = \sum_{i=1}^k a_i s_i + e$ となり, サンプルに影響を与えるのは, $\vec{s}$ の k ビット分である. LF アルゴリズムでは, $s_1, s_2, \ldots, s_k$ を総当りで計算する.

Levieil と Fouque は BKW アルゴリズムおよび LF アルゴリズムが必要とするサンプル数および計算ステップ数を, 以下のように詳細に解析した.

定理 4.8 $n = tk$ とし, $\delta = 1-2\tau$ とする.

- BKW アルゴリズムはクエリ数 $m = 20\ln(4n)2^k\delta^{-2^t}$, ステップ数 $t = O(ntm)$, メモリ量 $M = nm$, 成功確率 $\theta = 1/2$ で $\mathsf{LPN}_{n,m,\tau}$ 問題を解く.
- LF アルゴリズムはクエリ数 $m = (8k+200)\delta^{-2^t} + (t-1)2^k$, ステップ数 $t = O(ntm)$, メモリ量 $M = nm + k2^k$. 成功確率 $\theta = 1/2$ で $\mathsf{LPN}_{n,m,\tau}$ 問題を解く.

彼らの報告によれば, LF アルゴリズムと一部のヒューリスティクな手法を用いて $n = 99$, $\tau = 1/4$, $m = 10000$ の LPN 問題を CPU: Pentium 4 (3GHz), RAM: 1GB のマシンで解くことが可能である.

■Kirchner の指摘: Kirchner [Kir11] はランダムに選ばれた $\vec{s}$ よりは Ber_τ に従って選ばれる誤りベクトル $\vec{e}$ の方が, ハミング重みが小さくバリエーションが少ないことに着目した. LPN 問題を Sparse-LPN 問題に置き換えた上で問題を解くことを提案している.

Kirchner の手法は以下のようにまとめられる.

1. Applebaum ら [ACPS09] と同様の手法を用いて, $\mathcal{O}_{\vec{s},\chi}$ というオラクルを $\vec{e}' \leftarrow \mathsf{Ber}_\tau^n$ とランダムに選んだ場合の $\mathcal{O}_{\vec{e}',\chi}$ というオラクルに変換する.
2. BKW アルゴリズムや LF アルゴリズムと同様に基本アルゴリズムのステップ 1, 2 を行い, $A_{\vec{e}',\delta^{2^{t-1}},t-1}$ からのサンプルを得る.
3. ステップ 3 で, k ビットを決定する際に, $\vec{e}'$ の該当部分の重みが少ないことを考慮して総当りを行う.

一般の $\vec{s}$ であれば, 総当りに必要な回数は 2^k となる. 一方, $\vec{e}'$ はスパースであることが期待される. $d \geq 1$ を固定し k が十分に大きいとする. このとき, 圧倒的な確率の下で, ハミング重みは $(1+1/d)\tau k$ 以下である. よって, $\vec{e}'$ の候補数は $\binom{k}{(1+1/d)\tau k}$ 以下となり, 総当りに必要な回数が削減される.

■Ring-LPN 問題への応用: Bernstein と Lange [BL12] は Levieil と Fouque の高速化手法および Kirchner のアイデアを用いることにより, Ring-LPN 問題の解法が高速化できることを示している.

■GJL アルゴリズム: Guo, Johansson, Löndahl [GJL14] は, covering codes と呼ばれる符号を用いて Kirchner の手法の高速化を提案している. Kirchner の手法ではステップ 3 で, $A_{\vec{e}',\delta^{2^{t-1}},t-1}$ からのサンプル $\{(\vec{a}_i, b_i)\}$ が得られる. この $\vec{a}_i$ を covering code の受信語とみなすことで探索空間の圧縮を行い, 高速化に成功している.

■サンプル数が少ない場合: これまでに挙げてきた BKW アルゴリズムおよびその改良では, サンプルが $O(2^{n/\log n})$ 個必要であった. Lyubashevsky [Lyu05] はサンプル数が $n^{1+\epsilon}$ 個と少ない場合であっても, BKW アルゴリズムを適用できるような指数個のサンプルの構成法を示している. また, 上中谷と國廣 [KK15] は BKW アルゴリズムと Lyubashevsky の方法とを補間するようなアルゴリズムを提案している.

4.3.2 Arora-Ge アルゴリズム

Arora と Ge [AG11] は多変数多項式問題で古くから用いられている再線形化と呼ばれる手法を用いて, LPN 問題を解くことを考えた. このアルゴリズムを $\mathsf{LPN}_{n,m,\tau}$ に用いた場合, $w = \tau m$ として, $\mathrm{poly}(n^w)$ 時間で解くことができる. $\mathrm{poly}(n^w) = 2^{O(\tau m \log n)}$ であるから, $\tau = o(n/m \log n^2)$ であれば, BKW アルゴリズムよりも効率が良い.

4.3.3 SD 問題を経由するアルゴリズム

$\mathsf{LPN}_{n,m,\tau}$ に対応するシンドローム復号問題を考える. 対応するシンドローム復号問題での重みを w とする.

この問題を総当りで解く場合には, 重みが w の m 次元ベクトル $\vec{e}$ を列挙すればよい. そのため, 時間計算量は $O(\binom{m}{w})$ となる.

より効率的な手法として, "Information set decoding" と呼ばれる手法が McEliece [McE78] によって提案されている. 近年その高速化が進んでおり, 時間計算量は $2^{m/20}$ にまで引き下げられている. Becker, Joux, May, Meurer [BJMM12] らによる評価例を表 4.2 に示す. この表は, 時間計算量を最小化した場合の $R = n/m$ の最悪時についてまとめられている. 問題のパラメータによっては, 表の数値よりも速く解くことが可能となる.

表 4.2 Becker らによる確率 1/2 以上で SD 問題を解く場合のパラメータ例 [BJMM12]

	log(時間計算量)/m	log(空間計算量)/m	備考
Lee-Brickel	0.05752	–	[LB88]
Stern	0.05564	0.0135	[Ste88]
BLP	0.05549	0.0148	[BLP11b]
MMT	0.05364	0.0216	[MMT11]
BJMM	0.04934	0.0286	[BJMM12]

パラメータ設定によっては, $\mathsf{LPN}_{n,m,\tau}$ 問題を $\mathsf{SD}_{m-n,m,w}$ 問題に置き換えることで, これらの SD 問題用アルゴリズムも検討する必要がある.

4.3.4 量子アルゴリズムへの耐性

現在のところ多項式時間で LPN 問題を解く量子アルゴリズムは提案されていない. [BJLM13] などで一定の高速化は行われているため, 今後も継続して注視する必要がある.

4.4 まとめ

LPN 問題は学習理論や符号理論から派生した問題である. 誤り確率 τ が十分大きい場合の LPN 問題を多項式時間で効率的に解くことは困難であると予想されている.

共通鍵や公開鍵の分野で多くの方式が LPN 問題に基づいて提案されている. LWE 問題と比較した場合, 利点としては,

- $\mathbb{F}_2$ およびその拡大体を基に構成するため, ハードウェア構成との相性が良い点
- 誤差分布としてベルヌーイ分布やその一般化した分布を用いるため, 誤差のサンプリングが容易である点

が挙げられる. 一方, 欠点として,

- 鍵や暗号文のサイズが大きくなりやすい点
- ID ベース暗号や完全準同型暗号といった発展的な応用が少ない点

が挙げられる.

暗号方式のパラメータ設定の際には, 4.2 節で挙げたさまざまなアルゴリズムを考慮する必要がある. アルゴリズムの高速化について盛んに研究されており, 動向を注視する必要がある. また, 攻撃に用いられるアルゴリズムの研究は理論的なものが多く, 攻撃実験報告は小さいパラメータに対して行ったものが多い. そのため, 攻撃実験に関する研究もこれから非常に重要である.

第 4 章の参照文献

[Ale11] M. Alekhnovich, "More on average case vs approximation complexity," Computational Complexity 20(4): 755–786 (2011).

[App13] B. Applebaum, "Garbling XOR gates "For Free" in the standard model," In *Theory of Cryptography Conference–TCC 2013*, Springer, LNCS 7785, pp. 162–181, 2013.

[ACPS09] B. Applebaum, D. Cash, C. Peikert and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems," In *Advances in Cryptology–CRYPTO 2009*, Springer LNCS 5677, pp. 595–618, 2009.

[AHI11] B. Applebaum, D. Harnik and Y. Ishai, "Semantic security under related-key attacks and applications," In *Innovations in Computer Science–ICS 2011*, Tsinghua University, pp.45-60, 2011.

[AG11] S. Arora and R. Ge, "New algorithms for learning in presence of errors," In *International Colloquium on Automata, Languages and Programming–ICALP 2011*, Part I, Springer LNCS 6755, pp. 403–415, 2011.

[BJMM12] A. Becker, A. Joux, A. May and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How $1+1=0$ improves information set decoding," In *Advances in Cryptology–EUROCRYPT 2012*, Springer LNCS 7237, pp. 520–536, 2012.

[BMvT78] E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Transactions on Information Theory 24(3): 384–386 (1978).

[BJLM13] D. J. Bernstein, S. Jeffery, T. Lange, and A. Meurer, "Quantum algorithms for the subset-sum problem," In *Post-Quantum Cryptography–PQCrypto 2013*, Springer LNCS 7932, pp. 16–33, 2013.

[BLP10] D. J. Bernstein, T. Lange and C. Peters, "Wild McEliece," In *Selected Areas in Cryptography–SAC 2010*, Springer LNCS 6544, pp. 143–158, 2011.

[BLP11a] D. J. Bernstein, T. Lange and C. Peters, "Wild McEliece incognito," In *Post-Quantum Cryptography–PQCrypto 2011*, Springer LNCS 7071, pp. 244–254, 2011.

[BLP11b] D. J. Bernstein, T. Lange and C. Peters, "Smaller decoding exponents: Ball-collision decoding," In *Advances in Cryptology–CRYPTO 2011*, Springer LNCS 6841, pp. 743–760, 2011.

[BL12] D. J. Bernstein and T. Lange, "Never trust a bunny," In *Radio Frequency Identification. Security and Privacy Issues–RFIDSec 2012*, Springer LNCS 7739, pp. 137–148, 2013.

[BFKL93] A. Blum, M. L. Furst, M. J. Kearns and R. J. Lipton, "Cryptographic primitives based on hard learning problems," In *Advances in Cryptology–CRYPTO '93*, Springer LNCS 773, pp. 278–291, 1994.

[BKW03] A. Blum, A. Kalai and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," J. ACM 50(4): 506–519 (2003).

[DP12] I. Damgård and S. Park, “Is public-key encryption based on LPN practical?” IACR Cryptology ePrint Archive 2012: 699 (2012). 20140126:205953 版.

[DvdGMQN12] R. Dowsley, J. van de Graaf, J. Muller-Quade and A. C. A. Nascimento, “Oblivious Transfer Based on the McEliece Assumptions,” IEICE Transactions 95-A(2): 567–575 (2012).

[DNdS12] B. M. David, A. C. A. Nascimento and R. T. de Sousa Jr., “Efficient Fully Simulatable Oblivious Transfer from the McEliece Assumptions,” IEICE Transactions 95-A(11): 2059–2066 (2012).

[DNMQ12] B. M. David, A. C. A. Nascimento and J. Müller-Quade, “Universally Composable Oblivious Transfer from Lossy Encryption and the McEliece Assumptions,” In *International Conference on Information Theoretic Security–ICITS 2012*, Springer LNCS 7412, pp. 80–99, 2012.

[DMQN12] N. Döttling, J. Müller-Quade and A. C. A. Nasciment, “IND-CCA secure cryptography based on a variant of the LPN problem,” In *Advances in Cryptology–ASIACRYPT 2012*, Springer LNCS 7658, pp. 485–503, 2012.

[DDMQN12] N. Döttling, R. Dowsley, J. Müller-Quade and A. C. A. Nasciment, “A CCA2 secure variant of the McEliece cryptosystem,” IEEE Transactions on Information Theory 58(10): 6672–6680 (2012).

[FGOPT13] J.-C. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret and J. P. Tillich, “A distinguisher for high-rate McEliece cryptosystems,” IEEE Transactions on Information Theory 59(10): 6830–6844 (2013).

[FS96] J. B. Fischer and J. Stern, “An Efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding,” In *Advances in Cryptology–EUROCRYPT ’96*, Springer LNCS 1070, pp. 245–255, 1996.

[FGK+13] D. M. Freeman, O. Goldreich, E. Kiltz, A. Rosen and G. Segev, “More constructions of lossy and correlation-secure trapdoor functions,” J. Cryptology 26(1): 39–74 (2013).

[GRS08] H. Gilbert, M. J. B. Robshaw and Y. Seurin, “HB$^{\#}$: Increasing the security and efficiency of HB+,” In *Advances in Cryptology–EUROCRYPT 2008*, Springer LNCS 4965, pp. 361–378, 2008.

[GRS08] H. Gilbert, M. J. B. Robshaw and Y. Seurin, “How to encrypt with the LPN problem,” In *International Colloquium on Automata, Languages and Programming–ICALP 2008*, Part II–Track B, Springer LNCS 5126, pp. 679–690, 2008.

[GJL14] Q. Guo, T. Johansson and C. Löndahl, “Solving LPN Using Covering Codes,” In *Advances in Cryptology–ASIACRYPT 2014*, Part I, Springer LNCS 8873, pp. 1–20, 2014.

[Hås01] J. Håstad, “Some optimal inapproximability results,” J. ACM 48(4): 798–859 (2001).

[HKL+12] S. Heyse, E. Kiltz, V. Lyubashevsky, C. Paar and K. Pietrzak, “Lapin: An efficient authentication protocol based on ring-LPN,” In *Fast Software Encryption–FSE 2012*, Springer LNCS 7549, pp. 346–365, 2012.

[HB01] N. J. Hopper and M. Blum, “Secure human identification protocols,” In *Advances in Cryptology–ASIACRYPT 2001*, Springer LNCS 2248, pp. 52–66, 2001.

[JKPT12] A. Jain, S. Krenn, K. Pietrzak and A. Tentes, “Commitments and efficient zero-knowledge proofs from learning parity with noise,” In *Advances in Cryptology - ASIACRYPT 2012*, Springer LNCS 7658, pp. 663–680, 2012.

[KK15] 上中谷 健, 國廣 昇, “LPN 問題に対する BKW アルゴリズムの拡張,” SCIS2015, 3E1-3, 2015.

[KSS10] J. Katz, J. S. Shin, and A. Smith, “Parallel and concurrent security of the HB and HB+ protocols,” J. Cryptology 23(3): 402–421 (2010).

[KPC+11] E. Kiltz, K. Pietrzak, D. Cash, A. Jain and D. Venturi. "Efficient Authentication from Hard Learning Problems," In *Advances in Cryptology–EUROCRYPT 2011*, Springer LNCS 6632, pp. 7–26, 2011.

[Kir11] P. Kirchner, "Improved generalized birthday attack," IACR Cryptology ePrint Archive 2011: 377 (2011).

[KI01] K. Kobara and H. Imai, "Semantically secure McEliece public-key cryptosystems – conversions for McEliece PKC," In *Public Key Cryptography–PKC 2001*, Springer LNCS 1992, pp. 19–35, 2001.

[LB88] P. J. Lee and E. F. Brickell, "An observation on the security of McEliece's public-key cryptosystem," In *Advances in Cryptology–EUROCRYPT '88*, Springer LNCS 330, pp. 275–280, 1988.

[LF06] É. Levieil and P.-A. Fouque, "An improved LPN algorithm," In *Security and Cryptography for Networks–SCN 2006*, Springer LNCS 4116, pp. 348–359, 2006.

[LDW94] Y. X. Li, R. H. Deng and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," IEEE Transactions on Information Theory 40(1): 271–273 (1994).

[Lyu05] V. Lyubashevsky, "The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem," In *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques–APPROX–RANDOM 2005*, Springer LNCS 3624, pp. 378–389, 2005.

[MVVR12] K. P. Mathew, S. Vasant, S. Venkatesan and C. P. Rangan, "An efficient IND-CCA2 secure variant of the Niederreiter encryption scheme in the standard model," In *Australasian Conference on Information Security and Privacy–ACISP 2012*, Springer LNCS 7372, pp. 166–179, 2012.

[MMT11] A. May, A. Meurer and E. Thomae, "Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$," In *Advances in Cryptology–ASIACRYPT 2011*, Springer LNCS 7073, pp. 107–124, 2011.

[McE78] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Jet Propulsion Laboratory DSN Progress Report 42-44: 114–116 (1978).

[Nie86] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," Problems of Control and Information Theory 15: 19–34. Problemy Upravleniia i Teorii Informatsii 15: pp. 159-166 (1986).

[NIKM08] R. Nojima, H. Imai, K. Kobara and K. Morozov, "Semantic security for the McEliece cryptosystem without random oracles," Designs, Codes and Cryptography 49: pp. 289–305 (2008).

[Per13] E. Persichetti, "Improving the Efficiency of Code-Based Cryptography," University of Auckland, 2013.

[Pie12a] K. Pietrzak, "Subspace LWE," In *Theory of Cryptography Conference–TCC 2012*, Springer LNCS 7194, pp. 548–563, 2012.

[Pie12b] K. Pietrzak, "Cryptography from learning parity with noise," In *Conference on Current Trends in Theory and Practice of Computer Science–SOFSEM 2012*, Springer LNCS 7147, pp. 99–114, 2012.

[Reg09] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, 56(6): 1–40 (2009).

[Ste88] J. Stern, "A method for finding codewords of small weight," Coding Theory and Applications 1988: pp. 106–113.

第 5 章

Approximate Common Divisor 問題

本章では, Approximate Common Divisor (ACD) 問題及び関連する問題の困難性や暗号技術へのアプリケーションについての調査結果について述べる.

5.1 Approximate Common Divisor 問題の概説

5.1.1 Approximate Common Divisor 問題とは

Approximate Common Divisor 問題 (ACDP) は, CaLC2001 において, Howgrave-Graham により, 導入された問題である [HG01]. いくつかの暗号方式の安全性評価が, この問題を経由することにより行われている. Approximate Common Divisor (ACD) 問題は, 次のように定式化される.

定義 5.1 (ACD 問題 (その 1)) p を未知の素数とし, p の倍数 N は, 既知であるとする. r を, その絶対値が N^{α} 以下の整数とする. q を N/p 程度の乱数として,

$$x = pq + r$$

とする. x が与えられた時に, r を求める問題である.

この問題に対して, 法を p として簡約したものを考えることが多い. すなわち, 次の問題を ACD 問題とみなすことも多い.

定義 5.2 (ACD 問題 (その 2)) N を合成数として, p は, N の未知の素因数とする. ただし, $p \approx N^{\beta}$ とする. a を与えられた整数として,

$$a + x \equiv 0 \pmod{p}$$

をみたす x を求める問題である. ただし, $\alpha \leq \beta$ に対して, 解 x は, $|x| < N^{\alpha}$ を満たしているとする.

5.1.2 Approximate Common Divisor 問題の拡張

ACD 問題は, いくつかの拡張問題を持つ. ここでは, 以下の問題を考える.

定義 5.3 (複数 ACD 問題 (その 1)[CMNT11]) p を未知の素数とする. q を十分大きい自然数として, $N = pq$ とす

る. この N は既知であるとする. r_i を絶対値が N^α 以下の整数とする. q_i を q 程度の乱数として,

$$\begin{cases} x_1 &= pq_1 + r_1 \\ x_2 &= pq_2 + r_2 \\ &\vdots \\ x_n &= pq_n + r_n \end{cases}$$

とする. $x_1, x_2, \ldots, x_n$ が与えられた時に, $r_1, r_2, \ldots, r_n$ を求める問題である.

同様に, 以下のようにも定式化される.

定義 5.4 (複数 ACD 問題 (その2)) N を合成数として, p は, N の未知の素因数とする. ただし, $p \approx N^\beta$ とする. $a_1, a_2, \ldots, a_n$ を与えられた整数として,

$$\begin{cases} a_1 + x_1 &\equiv 0 \pmod{p} \\ a_2 + x_2 &\equiv 0 \pmod{p} \\ &\vdots \\ a_n + x_n &\equiv 0 \pmod{p} \end{cases}$$

をみたす $x_1, x_2, \ldots, x_n$ を求める問題である. ただし $\alpha_1, \alpha_2, \ldots, \alpha_n \leq \beta$ となる α_i に対して, 解 $x_1, x_2, \ldots, x_n$ は, $|x_i| < N^{\alpha_i}$ を満たしているとする. 簡単のため, $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$ であるとする.

N が与えられない問題を, General ACD 問題 (GACD 問題) と呼ぶ. この問題と区別するため, N が与えられる問題を Partial ACD 問題 (PACD 問題) と呼ぶこともある. 明らかに, 同一の n に対して, GACD 問題の方が, PACD 問題よりも困難である. 複数 GACD 問題は, 以下のように定義される.

定義 5.5 (複数 GACD 問題) p を未知の素数, N を γ ビットの自然数として, $p \approx N^\beta$ とする. q_i を 0 から N/p の間の乱数とし, r_i を絶対値が N^α 以下の整数とする. $x_1, x_2, \ldots, x_n$ を

$$\begin{cases} x_1 &= pq_1 + r_1 \\ x_2 &= pq_2 + r_2 \\ &\vdots \\ x_n &= pq_n + r_n \end{cases}$$

とする. $x_1, x_2, \ldots, x_n$ が与えられた時に, $r_1, r_2, \ldots, r_n$ を求める問題である.

5.1.3 Approximate Common Divisor 問題のアプリケーション

van Dijk ら [DGHV10] は, 複数 GACD 問題の困難さを安全性の根拠として持つ, 整数上での完全準同型暗号を提案している. さらに, 仮定を複数 PACD 問題の困難さに強めることにより, 効率的になることを述べている. ついで, Coron らは, 公開鍵サイズを削減する方式を提案している [CMNT11]. 彼らの方式も, 複数 PACD 問題の困難さを安全性の根拠としている. さらに, [CCK+13] では, 中国人の剰余定理を用いる事により, バッチ処理が可能な方式を提案している. この論文では, 新たに, 判定 Approximate GCD 問題を導入し, この問題の困難さを安全性の根拠とした方式を提案している. さらに, 提案方式をベースに, 128 ビット AES 回路の実装を行っている. 72 ビットセキュリティを担保した上で, 13 分以内で, 暗号化の処理が終了すると報告している. この論文では, 後に述べる [CN11] による攻撃を考慮した上で, パラメータ設定を行っている.

以下, 順に, van Dijk らの方式 [DGHV10], Cheon らの方式 [CCK+13] を説明する. ただし, 記述を容易にするため, 完全準同型方式ではなく, somewhat 準同型方式を記載する.

5.1.3.1 van Dijk らの方式 [DGHV10]

正の奇数 p に対して, 以下のように, γ ビットの整数上の分布 $\mathcal{D}_{\gamma,\rho}(p)$ を導入する.

$$\mathcal{D}_{\gamma,\rho}(p) = \{ \text{ choose } q \leftarrow \mathbb{Z} \cap [0, 2^\gamma/p), r \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho) : \text{ output } x = pq + r\}$$

KeyGen(λ)

秘密鍵： η ビットの奇数 p

公開鍵： x_i を $D_{\gamma,\rho}(p)$ から $\tau + 1$ 個取り, それらを $x_0, x_1, \ldots, x_\tau$ とする. ただし, x_0 が最大とする. x_0 は奇数で, $x_0 \bmod p$ は偶数であるとし, そうでなければ, あらためて, x_i を取り直す. 公開鍵 pk は, $(x_0, x_1, \ldots, x_\tau)$ である.

Enc($pk, m \in \{0, 1\}$)

Step1 ランダムな部分集合 $S \subseteq \{1, 2, \ldots, \tau\}$ を選ぶ.

Step2 $r \leftarrow \mathbb{Z} \cap (-2^{\rho'}, 2^{\rho'})$ を選ぶ.

Step3 暗号文

$$c \leftarrow (m + 2r + 2\sum_{i \in S} x_i) \bmod x_0$$

とする.

Dec(sk, c)

$m' \leftarrow (c \bmod p) \bmod 2$ を計算し, m' を出力する.

5.1.3.2 CCK+13 方式 [CCK+13]

簡単のため, 論文中メッセージ空間は, 二進系列の場合のみを記述する. 一般の場合の記述は, [CCK+13] を参照されたい.

KeyGen(λ)

秘密鍵： η ビットの異なる奇数 $p_0, p_1, \ldots, p_{l-1}$

公開鍵： $\pi = \prod_{i=0}^{l-1} p_i$ とする. q_0 を, 0 から $2^\gamma/\pi$ の間の整数をランダムに選び, $x_0 = q_0\pi$ とする. ただし, q_0 は, 2^{λ^2}-rough であるとする.

$$x_i \bmod p_j = 2r_{i,j}, r_{i,j} \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho) \text{ for } 1 \le i \le \tau$$
$$x'_i \bmod p_j = 2r'_{i,j} + \delta_{i,j}, r'_{i,j} \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho) \text{ for } 0 \le i \le l-1$$

ここで, $\delta_{i,j}$ は, $i = j$ のときに, 1 であり, $i \neq j$ とき, 0 を取る. 公開鍵 pk は, $(x_0, x_1, \ldots, x_\tau, x'_0, x'_1, \ldots, x'_{l-1})$ である.

Enc($pk, \boldsymbol{m} = (m_0, m_1, \ldots, m_{l-1}) \in \{0, 1\}^l$)

Step1 $\boldsymbol{b} = (b_1, b_2, \ldots, b_\tau) \in \{0, 1\}^\tau$ をランダムに選ぶ.

Step2 暗号文

$$c \leftarrow (\sum_{i=0}^{l-1} m_i x'_i + \sum_{i=1}^{\tau} b_i x_i) \bmod x_0$$

とする.

Dec(sk, c)

$m_j \leftarrow (c \bmod p_j) \bmod 2$ を計算し, $\boldsymbol{m} = (m_0, m_1, \ldots, m_{l-1})$ を出力する.

5.1.4 安全性の根拠となる問題

[DGHV10] では, Approximate GCD 問題を次のように定義している. (ρ, η, γ)-approximate GCD 問題とは, ランダムに選ばれた η ビットの奇数 p に対して, $\mathcal{D}_{\gamma,\rho}(p)$ からの多項式個のサンプルが与えられた時に, p を求める問題である.

[DGHV10] で提案された somewhat 準同型暗号方式の安全性は, 以下のように示されている. ここで, 用いるパラメータを $(\rho, \rho', \eta, \gamma, \tau)$ とする. このとき, advantage ϵ で方式を破る攻撃者 A は, (ρ, η, γ)-approximate GCD 問題を, 確率 $\epsilon/2$ 以上で, 解くアルゴリズム B に変換することができる. アルゴリズム B の動作時間は, A の動作時間, $\lambda, 1/\epsilon$ の多項式である.

[CMNT11] では, Error-free Approximate GCD 問題を次のように定義している. 正の奇数 p, q_0 に対して, 整数上の分布 $\mathcal{D}'_\rho(p, q_0)$ を, 次のように定義する.

$$\mathcal{D}'_\rho(p, q_0) = \{ \text{ choose } q \leftarrow \mathbb{Z} \cap [0, q_0), r \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho) : \text{ output } x = pq + r \}$$

(ρ, η, γ)-error-free approximate GCD 問題とは, ランダムに選ばれた η ビットの奇数 p とランダムに選ばれた square-free かつ 2^λ-rough で, 0 から $2^\gamma/p$ の間の整数 q_0 に対して, $x_0 = q_0 p$ と $\mathcal{D}'_\rho(p, q_0)$ からの多項式的に多くのサンプルが与えられた時に, p を求める問題である.

[CMNT11] で提案された somewhat 準同型暗号方式の安全性は, 以下のように示されている. ここで, 用いるパラメータを $(\rho, \rho', \eta, \gamma, \tau)$ とする. このとき, advantage ϵ で方式を破る攻撃者 A は, (ρ, η, γ)-error-free approximate GCD 問題を, 確率 $\epsilon/2$ 以上で, 解くアルゴリズム B に変換することができる. アルゴリズム B の動作時間は, A の動作時間, $\lambda, 1/\epsilon$ の多項式である.

[CCK+13] で提案された somewhat 準同型暗号方式は, 判定 Approximate GCD 問題の困難さに安全性の根拠をおいている. この問題は, 以下のように定式化される.

1. $\mathcal{D}'_\rho(p, q_0)$ から多項式個のサンプルを受け取った上で,
2. $z = x + rb \bmod x_0$ を受け取った時に, $b \in \{0, 1\}$ を判定する問題である. ここで, $x \leftarrow \mathcal{D}'_\rho(p, q_0)$ と $r \leftarrow \mathbb{Z} \cap [0, x_0)$ である.

以上の記述では, 原論文での記述を採用している. そのため, 用いるパラメータが異なっているが, $\eta = \beta \log N, \rho = \alpha \log N, \gamma = \log N$ という関係にあることに注意されたい.

5.2 ACD 問題に対する評価

PACD 問題は, N の素因数分解を経由することにより, 容易に解くことができる. 具体的には, 以下の手順による. まず, N を素因数分解をすることにより, p を求める. 求めた p を用いることにより, x を求めることができる. 法が既知

の一次方程式 $a + x \equiv 0 \pmod{p}$ を解くことは, 容易であるためである. これ以降, N の素因数分解を, 直接的には, 経由しないアルゴリズムを考察する.

N の素因数分解を直接的には経由しないアルゴリズムを, 以下の二つに大別して説明をする.

1. 組み合わせ論に基づくアルゴリズム
2. 格子理論に基づくアルゴリズム

前者のアルゴリズムは, 指数関数時間アルゴリズムではあるが, 解に制約は存在しない. すなわち, どのような α に対しても, 解を求めることが可能である. しかし, 計算量は, α に依存する. その一方で, 後者のアルゴリズムは, 解くことができる解に制約が存在するものの, 解がその制約をみたせば, 多項式時間で求解が可能である. すなわち, 任意の α に対して, 解を求めることができる訳ではなく, 制限が存在するが, 十分高速に解を求めることができる. そのため, 求める問題に応じて, 適切なアルゴリズムの選択が重要である.

5.2.1 組み合わせ論に基づくアルゴリズム

PACD 問題を解く最も素朴なアルゴリズムは, 全数探索アルゴリズムである. 解 x の可能な値は, $2N^{\alpha}$ 個であるので, 全数探索により, $\tilde{O}(N^{\alpha})$ の計算量で解の探索が可能である. これは, ビット長 $\log N$ に対して, 指数関数時間必要である.

Chen と Nguyen は, 全数探索よりも効率的に, 解を求めるアルゴリズムを提案している [CN11]. 彼らは, multipoint evaluation of univariate polynomials というテクニックを導入することにより, 効率化に成功している. まず, このテクニックについて説明する. 整数係数でモニックな 1 変数 n 次多項式 $f(x)$ を考える. $a_1, a_2, \ldots, a_n$ を整数として, $f(a_1), f(a_2), \ldots, f(a_n)$ の値全てを計算したい状況を考える. 素朴なアルゴリズムでは, この計算には, $O(n^2)$ の計算量が必要である. これに対して, 彼らは, $\tilde{O}(n)$ の計算量で, $f(a_1), f(a_2), \ldots, f(a_n)$ の全てを計算するアルゴリズムを提案している. すなわち, 平方根の高速化が実現している. 彼らは, PACD 問題を, multipoint evaluation of univariate polynomials に帰着した上で, このアルゴリズムを適用することにより, PACD 問題を解くアルゴリズムを構成している. 実際の計算量は,

$$\tilde{O}(N^{\alpha/2})$$

で与えられる.

Chen と Nguyen[CN11] は, 提案アルゴリズムを実装することにより, Coron らの論文 [CMNT11] 中で提示された推奨パラメータに対して, 安全性の再評価を行っている. 再評価結果を表 5.1 に記す. 表中, 「Securtiy Level」の欄は, 総当たりの攻撃により, 見積もられた Security Level である. その一方で, 「新しい Security Level」の欄は, Chen-Nguyen の攻撃により見積もられた Security Level である. 従来の見積もりよりも, 安全性が低下していることが確認できる.

表 5.1 Chen–Nguyen アルゴリズムによる評価 ([CN11] より)

Name	Toy	Small	Medium		Large	
Security Level	52	61	72		100	
計算時間の見積もり	1.6 分	7.1 時間	190 日	76 日	2153 年	9 年
使用メモリ量	$\leq$ 130 Mb	$\leq$ 15 Gb	$\leq$ 72 Gb	$\approx$ 240 Gb	$\leq$ 72 Gb	$\approx$ 25 Tb
新しい Security Level	$\leq$ 37.7	$\leq$ 45.7	$\leq$ 55	$\leq$ 54	$\leq$ 67	$\leq$ 59

5.2.2 格子理論に基づくアルゴリズム

一般に, 暗号の安全性解析において, 格子理論にもとづくアルゴリズム [Cop95, Cop96, Cop97, HG97] は, 重要なツールである. ここでは, 格子理論を用いた ACD 問題を解くアルゴリズムについて説明する. Partial ACD 問題を解く格子理論に基づくアルゴリズムの中で, 現状で最も優れたアルゴリズムは, Howgrave-Graham によるアルゴリズムである [HG01]. このアルゴリズムでは, α と β が,

$$\alpha < \beta^2 \tag{5.1}$$

を満たすときに, 多項式時間で解を求めることが可能である.

この結果を用いると, よく知られた以下の結果を, 容易に導くことができる [Cop96:A].

RSA タイプの合成数 $N = pq$ に対して, p の上位半分のビットがわかった時に, 素因数分解が可能である.

RSA 型の合成数 $N = pq$ に対して, p の近似値 $\tilde{p}$ がわかった場合を考える. $x = p - \tilde{p}$ とおくと, $\tilde{p} + x \equiv 0 \pmod{p}$ が成り立つ. このため, PACD 問題が解ければ, 素因数分解が可能となる. $p \approx N^{1/2}$ の時, すなわち, $|p - \tilde{p}| < N^{1/4}$ の時には, 素因数分解が可能となる. 具体的には, p の上位半分がわかれば, 素因数分解が可能である.

5.2.3 量子アルゴリズムへの耐性

前述のように, Partial ACD 問題は, N の素因数分解ができれば, 簡単に解くことができる. 量子計算機を用いることができれば, Shor のアルゴリズム [Shor94] により, 多項式時間で素因数分解を行うことができるため, PACD 問題を解くことは容易である.

5.2.4 ACD 問題に対する評価のまとめ

以上の議論をまとめる. Partial ACD 問題は,

1. 解の大きさに $\alpha < \beta^2$ という制限がある場合には, 多項式時間で解くことができる.
2. その一方で, 解の大きさに制限がない場合には, $\tilde{O}(N^{\alpha/2})$ の計算量で解を求めることが可能である.

問題の設定により, 最適なアルゴリズムが異なるため, 適切な選択が必要である.

5.3 複数 ACD 問題に対する評価

5.3.1 組み合わせ論に基づくアルゴリズム

複数 ACD 問題に対しても, 最も素朴なアルゴリズムは, 全数探索アルゴリズムである. 解 $x_1, x_2, \ldots, x_n$ のうち, 一つでも値を求めることができれば, p を求めることができるため, $x_1, x_2, \ldots, x_n$ の全てを求めることが可能である. このため, x_1 をまず求めることにする. このとき, x_1 の取りうる値の可能な個数は, $2N^{\alpha_1}$ である. そのため, 複数 ACD 問題を全数探索アルゴリズムにより解く計算量は, $\tilde{O}(N^{\alpha_1})$ で与えられる.

同様に, Chen-Nguyen のアルゴリズム [CN11] により, $\tilde{O}(N^{\alpha_1/2})$ の計算量で, この問題を解くことができる. このアルゴリズムでは, 複数の方程式が与えられていることを有効に活用できていない.

5.3.2 格子理論に基づくアルゴリズム

5.3.2.1 Coppersmith 流のアルゴリズム

格子理論に基づくアルゴリズムにより, 複数 ACD 問題を多項式時間で解くことができる条件を示す. 前述の Howgrave-Graham アルゴリズム [HG01] を用いることにより, $\alpha_1 < \beta^2$ であれば, 解を求めることができる. このアルゴリズムでも, 方程式が複数個得られていることを活用していない.

ANTS2012 において, Cohn と Heninger は, $\beta \gg \frac{1}{\sqrt{\log N}}$ という条件下で,

$$\frac{\alpha_1 + \alpha_2 + \cdots + \alpha_n}{n} < \beta^{(n+1)/n}$$

の時に, 多項式時間で解を求めるこができることを示している [CH11]. 各 α_i が, 全て等しく α であるとする. このとき, $\alpha < \beta^{(n+1)/n}$ の時に, 解を求めることができる.

その一方で, Cohn と Heninger の結果は, α_i が等しく無い場合には, 必ずしも最適ではない. これに対して, Takayasu と Kunihiro は, 解くことができる条件の改良を行っている [TK13]. 彼らは,

$$\sqrt[n]{\alpha_1 \alpha_2 \cdots \alpha_n} < \beta^{(n+1)/n}$$

の時に多項式時間で解を全て求めることができることを示している. 常に,

$$\frac{\alpha_1 + \alpha_2 + \cdots + \alpha_n}{n} \geq \sqrt[n]{\alpha_1 \alpha_2 \cdots \alpha_n}$$

が成り立つため, 彼らの条件は, Cohn–Heninger の条件の改良となっている. ただし, 各 α_i が, 全て等しく α であるときには, この条件は, $\alpha < \beta^{(n+1)/n}$ となり, Cohn–Heninger の結果と一致する.

この結果の妥当性を検証する. $\alpha_1 = \beta^2$ であれば, $2 \leq i \leq n$ となる i に対して, $\alpha_i = \beta$ と取ることができるため, Takayasu–Kunihiro の結果は, Howgrave-Graham の結果の自然な拡張となっている.

5.4 GACD 問題の格子理論を用いたアルゴリズム

GACD 問題を解くアルゴリズムに関して, 議論する.

5.4.1 組み合わせ論に基づくアルゴリズム

Chen と Nguyen は, PACD 問題を解くアルゴリズムを拡張により, General ACD 問題を, $\tilde{O}(N^{3\alpha/2})$ で解くことができることを示している [CN11]. 総当たりのアルゴリズムでは, $\tilde{O}(N^{2\alpha})$ の計算量が必要であるため, 指数関数の高速化を実現している. このとき, 必要となるメモリ量は, $\tilde{O}(N^{\alpha/2})$ である.

Chen と Nguyen のアルゴリズムは, GACD の 2 個のサンプルしか用いていないが, 積極的に複数個のサンプルを用いることにより計算量の削減が可能である. Coron らは, [CNT12] において, 計算量 $\tilde{O}(N^{\alpha})$, メモリ量 $\tilde{O}(N^{\alpha})$ のアルゴリズムを提案している.

5.4.2 格子理論に基づくアルゴリズム

次に, 格子理論に基づくアルゴリズムを述べる, Coppersmith の手法に基づくように, 十分大きい法に対して成り立つ関係式を用いて, 法を外し, 整数上の方程式に変換してから解く方法と, 解を最短ベクトルに埋め込むことにより解く方法を紹介する. この二つの方法の一般論に関しては, [K11] に詳しい.

5.4.2.1 Coppersmith の手法に基づく解析

Howgrave-Graham は, $n = 2$ の時の解析を行っている [HG01]. $n = 2, \alpha_1 = \alpha_2 := \alpha$ の時は,

$$\alpha < 1 - \frac{1}{2}\beta - \sqrt{1 - \beta - \frac{1}{2}\beta^2}$$

であれば, 解を求めることができることを示している. 一般の n の状況に関しては, Cohn と Heninger は,

$$\alpha < \frac{1 - 1/n^2}{n^{1/(n-1)}}\beta^{n/(n-1)}$$

のときに, 多項式時間で解を求めることができることを示している [CH11].

5.4.2.2 最短ベクトルに埋め込む解法

次に, 解きたい解を短いベクトルに埋め込む手法を用いた場合の解析について説明する. [DGHV10] では, Lagarias の同時 Diophantine 近似 (SDA) 問題を解くアルゴリズムを利用することにより, 複数 ACD 問題が難しくなるかを評価している. 今, サンプルは, $t + 1$ 個用いるとする. $t + 1 < \gamma/\eta$ の時には, 解を埋め込んだベクトルが最短ベクトルにならないことを指摘している. そのため, LLL アルゴリズムなど格子簡約アルゴリズムなどを用いても, 解を見つけることができない. その一方で, t が大きいときには, 埋め込んだベクトルが最短になりやすくなる. しかし, この場合, 用いる格子の次元が大きくなりすぎるため, 効率的に解を求めることができない. 経験的に, 最短ベクトルの 2^k の近似精度でベクトルを求めるためには, $2^{t/k}$ の計算時間が必要である. そのため, $t \geq \gamma/\eta$ の時には, 2^η の近似精度を実現するためには, およそ $2^{\gamma/\eta^2}$ の計算時間が必要である. そのため, γ/η^2 を $\log \lambda$ 程度に設定をすれば, 全体の計算時間は指数関数時間になる.

さらに, [DGHV10] では, Nguyen と Stern による orthogonal 格子を用いた場合の解析も行っている. SDA 問題を経由するときと同様に, 解を求めるためには, $2^{\gamma/\eta^2}$ 程度の計算量が必要であることを述べている.

5.4.3 完全準同型暗号の安全性への影響

いずれの攻撃においても, 適切にパラメータが設定された状況では, 攻撃に成功するのに, 指数関数時間が必要であり, 脆弱性は発見されていない. しかし, いずれも, 理論上の解析であるため, 数値実験により安全性の検証をする必要がある.

5.5 関連問題 co-ACD 問題の安全性評価

Cheon らは, ACM CCS2014 において, ACD 問題の関連問題として, co-ACD 問題を導入し, この問題の困難さに安全性の根拠をおく加法準同型暗号を提案している [CLS14]. この加法準同型暗号方式は, 同様の機能を持つ Paillier 暗号と比べて, 高速に演算が可能であるという性質を持つ. さらに, co-ACD 問題の安全性を議論し, ACD 問題に対するアルゴリズムを適用した場合には, 十分, 安全であることを示している.

以下に, co-ACD 問題の定義を記す. まず, 分布 $\hat{\mathcal{D}}_{\rho,Q}$ を, 以下のように定義する. 素数 $(p_1, p_2, \ldots, p_k)$ として, $e \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho)$ とし,

$$(eQ \bmod p_1, eQ \bmod p_2, \ldots, eQ \bmod p_k)$$

を出力する. 計算 co-ACD 問題は, $\hat{\mathcal{D}}_{\rho,Q}$ からの多項式個のサンプルが与えられたときに, $\prod_{i=1}^{k} p_i$ の非自明な因数を求める問題である.

しかし, 最近になり, co-ACD 問題に特化した攻撃手法が提案されている [FLT15]. [FLT15] は, 短い平文に対する暗号文を複数得られた状況で, Nguyen-Stern の直交格子解読手法, グレブナー基底手法, Coppersmith アルゴリズムを用いることにより, 効率的に平文の復元が可能であると主張している.

5.6 まとめ

この節の議論をまとめる. 現状において, ACD 問題は, パラメータを適切に選ぶ事により, 現実的な時間で解を求めることは不可能である. つまり, 法に対して, 解が, ある制限よりも小さいときには, 多項式時間で解くことができるものの, その一方で, 解が十分大きいときには, 解を求めることができない. 組み合わせ論に基づくアルゴリズムを用いた場合では, 依然, 指数関数時間の計算量が必要であるが, 全数探索アルゴリズムの平方根の計算量で解を求めることができる. Chen–Nguyen のアルゴリズムは, 暗号の提案時には, 考慮されていなかった攻撃であり, 実際に, 提案論文で書かれた推奨パラメータのいくつかは, 解読されることが示されている. また, ACD 問題に関連した問題 co-ACD 問題は, 当初の想定よりも弱いことが明らかになっている. これらの結果は, ごく最近に示されたものであり, 今後の研究の動向に注視する必要がある.

第 5 章の参照文献

[CN11] Y. Chen and P. Q. Nguyen, “Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers,” In *Advances in Cryptology–EUROCRYPT 2012*, Springer LNCS 7237, pp. 502–519, 2012.

[CCK+13] J. H. Cheon, J.-S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi and A. Yun, “Batch Fully Homomorphic Encryption over Integers,” In *Advances in Cryptology–EUROCRYPT 2013*, Springer LNCS 7237, LNCS 7881, pp. 315–335, 2013.

[CLS14] J. H. Cheon, H. T. Lee and J. H. Seo, “A New Additive Homomorphic Encryption based on the co-ACD Problem,” In *the 2014 ACM SIGSAC Conference on Computer and Communications Security–CCS2014*, ACM, pp. 287–298, 2014.

[CH11] H. Cohn and N. Heninger, “Approximate common divisors via lattices,” In *the 10th Algorithmic Number Theory Symposium–ANTS–X*, pp. 271–293, 2012.

[Cop95] D. Coppersmith, “Factoring with a hint,” IBM Research Report RC 19905, 1995.

[Cop96] D. Coppersmith, “Finding a Small Root of a Univariate Modular Equation,” In *Advances in Cryptology–Eurocrypt ’96*, Springer LNCS 1070, pp. 155–165, 1996.

[Cop96:A] D. Coppersmith, “Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known,” In *Advances in Cryptology–Eurocrypt ’96*, Springer LNCS 1070, pp. 178–189, 1996.

[Cop97] D. Coppersmith, “Small solutions to polynomial equations, and low exponent RSA vulnerabilities,” Journal of Cryptology, Volume 10, Issue 4, pp. 233–260, 1997.

[CMNT11] J.-S. Coron, A. Mandal, D. Naccache and M. Tibouchi, “Fully homomorphic encryption over the integers with shorter public keys,” In *Advances in Cryptology–CRYPTO 2011*, Springer LNCS 6841, pp. 487–504, 2011.

[CNT12] J. -S. Coron, D. Naccache and M. Tibouchi, “Public key compression and modulus switching for fully homomorphic encryption over the integers,” In *Advances in Cryptology–EUROCRYPT 2012*, Springer LNCS 7237, pp. 446–464, 2012.

[DGHV10] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” In *Advances in Cryptology–EUROCRYPT 2004*, Springer LNCS 6110, pp. 14–27, 2010. Longer version available as Report 2009/616 in the Cryptology ePrint Archive (`http://eprint.iacr.org/2009/616/`).

[FLT15] ピエール=アラン・フーク, タンクレード・ルポワン , メディ・ティブシ, “Co-ACD 仮定とそれを基にした準同型暗号方式の安全性評価,” SCIS2015, 3E4-4, 2015.

[HG97] N. Howgrave-Graham, “Finding small roots of univariate modular equations revisited,” In *Cryptog-*

raphy and Coding–IMA 1997, Springer LNCS 1355, pp. 1331–142, 1997.

[HG01] N. Howgrave-Graham, “Approximate integer common divisors,” In *Cryptography and Lattices–CaLC 2001*, Springer LNCS 2146, pp. 51–66, 2001.

[K11] 國廣 昇, “格子理論を用いた暗号解読の最近の研究動向,” 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, Vol. 5, no. 1, pp. 42–55, 2011.

[Shor94] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” In *Annual Symposium on Foundations of Computer Science–FOCS'94*, IEEE Computer Society, pp. 124–134, 1994.

[TK13] A. Takayasu and N. Kunihiro, “Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors,” In *Australasian Conference on Information Security and Privacy–ACISP2013*, Springer LNCS 7959, pp. 118–135, 2013.