Vol.2021-DPS-186 No.33
Vol.2021-CSEC-92 No.33
2021/3/15

解読計算量に基づくLWE暗号の安全性に関する検討

岡　翔子[†1]　國枝 義敏[1]　上原 哲太郎[1]　猪俣 敦夫[2]

概要：社会の情報化が世界的に進む現在、最も普及している公開鍵暗号として RSA 暗号がある。そして RSA 暗号よりはるかに短い鍵長で同等の安全性を保持できる楕円曲線暗号がその後継として注目を集めているが、これら RSA 暗号と楕円曲線暗号はともに量子計算機によって多項式時間内に解読されてしまうことが知られている。そこで量子計算機による解読に耐えうる耐量子計算機暗号 (Post-Quantum Cryptography; PQC) の開発が望まれている。本研究においては、耐量子計算機暗号に関する研究全体を俯瞰するとともに、特に有力視され研究の進んでいる LWE 暗号の解読に必要な時間計算量に着目し、PQC である LWE 暗号および改良型の ring-LWE 暗号が真に現行の暗号方式に置換できうるかを考察した。

A Study on the Security of LWE Cryptosystem Based on the Computational Complexity of Decoding

Abstract: The RSA cryptosystem is the most widespread public key cryptosystem in the world today. And elliptic curve cryptography, which can be the same level of security with a much shorter key length than RSA cryptography, is attracting attention as its successor. However, it is known that both RSA and elliptic curve cryptography can be decoded by quantum computers in polynomial time. Therefore, it is desirable to develop post-quantum cryptography (PQC) that can withstand decoding by quantum computers. In this research, I overview the research on post-quantum cryptography, and focus on the running time required to decode the LWE cryptosystem, which is one of the most promising cryptosystems in the world and consider whether the LWE cryptosystem and the improved ring-LWE cryptosystem can truly replace the current cryptosystem.

1. はじめに

世界的に情報化が進む現在，社会において，暗号技術は金融取引のみならず映像コンテンツの保護や印鑑に替わる本人証明など幅広い用途に活用されている． 通常，データ通信において機密性を保つ手段としては主に AES（Advanced Encryption Standard）やトリプル DES（Data Encryption Standard）といった共通鍵暗号が用いられている．一方でデータの改ざん検知や通信相手の検証，共通鍵暗号の鍵の配送手段としては主に公開鍵暗号が利用されており，RSA 暗号が標準規格として広く普及している．また，現在では楕円曲線暗号が次世代を担う公開鍵暗号として注目されている．

公開鍵暗号は，落とし戸つき一方向性関数という，引数から出力結果を求めることは容易であるが出力結果から逆に引数を求めることは極めて難しいという特徴をもつ数学的問題を利用した暗号である．RSA 暗号は巨大な合成数の素因数分解 [1]，楕円曲線暗号は ECDLP（楕円曲線上の離散対数問題）の求解困難性を用いている [2][3].

だが，1994 年に Shor によって発表されたアルゴリズム [4] と，開発・改良が進む量子計算機によって，量子計算機を用いると素因数分解や ECDLP を解くことが現実的な時間内に行えるために，現在普及している公開鍵暗号の多くが将来危殆化するという認識が広まった．ただし，現時点における量子計算機の性能は現在使われている公開鍵暗号を解読できるほどではなく，現行の公開鍵暗号すべてがただちに危殆化するわけではない.

しかしながら，RSA 暗号が世界基準として普及するまでに 20 年近く要していることを考えると，将来量子計算機が実用化，普及することを踏まえた上で，量子計算機による解読攻撃に耐える暗号方式，耐量子計算機暗号（Post-Quantum

[1] 立命館大学大学院
Ritsumeikan University , Kusatsu, Shiga 525–8577, Japan
[2] 立命館大学総合科学技術研究機構
Ritsumeikan Univercity Research Organization of Science and Technology
[†1] 現在，立命館大学大学院
Presently with Ritsumeikan University

Cryptography, PQC）の実用化に今から取り組む必要がある．

暗号の実用化にはプロトコルの策定などとともに，解読を行い暗号の強度を確かめる必要がある．しかし現在までに複数の解読手法が提示されてきたものの，その時間計算量は明示されず，暗号の強度は実時間でしか測られてこなかった．

そこで，本研究では耐量子計算機暗号の中でも有力視されている格子暗号，特に LWE 方式の解読に必要な計算量を明らかにした．その上で LWE 暗号との比較を容易にするため現代暗号の計算量も併せて示し，LWE 暗号が現代暗号に置換しうるかを考察した．

本論文では，第 2 章において量子計算機が現代暗号の潜在的な脅威となっている現状について概説したのち，耐量子計算機暗号の研究全体を俯瞰する．続く第 3 章では LWE 暗号の構成方法と解読手法および必要な計算量について述べ，第 4 章において LWE 暗号の安全性について考察したのち，結論を述べる．

2. 研究背景

2.1 現代暗号

1976 年，Diffie と Hellman により公開鍵暗号の概念が発表され，翌 1977 年に Rivest，Shamir，Adleman らによって公開鍵暗号の概念を実現する具体的な方式が開発された．この方式は，開発者らの頭文字をとって RSA 暗号と呼ばれている．

RSA 暗号の安全性は素因数分解問題に依拠しており，素因数分解問題は現在，古典計算機（現在普及している汎用コンピュータ）を用いて多項式時間内で解ける解読法が知られていないことから，安全だと期待されている．コンピュータの性能上昇に伴う安全性の経年劣化については鍵長を伸展させることで対応しており，アメリカ国立標準技術研究所（National Institute of Standards and Technology, NIST）は RSA 暗号に対し，128 ビット安全を保持するためには 3072 ビット，256 ビット安全を保持するためには 15360 ビットの鍵長が必要であると発表している [5].

このように，鍵長が増加することで，いずれはメモリ容量等が制限されたハードウェア環境での実装が難しくなるという懸念が，RSA 暗号の課題である．

この課題を払拭する次世代の暗号として，楕円曲線暗号がポスト RSA 暗号として注目されている．

楕円曲線暗号とは，1980 年代に Miller と Koblitz によってそれぞれ独立に提案された公開鍵暗号の実現方式であり，楕円曲線上の離散対数問題（ECDLP）の求解困難性を安全性の根拠としている．現行のコンピュータで ECDLP を効率的に解くアルゴリズムは発見されておらず，また RSA 暗号の約 10 分の 1 程度の短い鍵長で同等の安全性を保持できるとして，2000 年代後半から広く使用されている．

後述する耐量子計算機暗号（Post-quantum cryptography, PQC）に対し，これら現行の暗号は現代暗号と呼ばれている．

2.2 量子計算機

量子計算機そのものは 1980 年代から研究が行われており，現在は量子ゲート型（デジタル型），量子アニーリング型（アナログ型）の二種類に大別されている．これらはともに計算に量子状態を利用するが，その実現方式は全く異なる．量子ゲート型は相互作用をもつ量子ビットを組み合わせた演算回路「量子ゲート」を用いて演算するのに対し，量子アニーリング型は極低温における量子ビット列の変化「量子ゆらぎ」を利用して演算する．それぞれの実現方式の特徴として，量子ゲート型は現行のコンピュータの上位互換を目標としており，現在数十ビットの性能のものしか実現していないが実用化が進めば大きなブレイクスルーになると期待されている．対し，量子アニーリング型は組合せ最適化に特化しており，解ける問題は限られているが数千ビットの性能のものが開発されている．

また 1994 年，Shor によって量子計算機上で因数分解を多項式時間内で行うことができる Shor のアルゴリズムが発表された [4]．Shor のアルゴリズムはゲート方式の量子計算機が離散フーリエ変換を高速に実行できることを利用しており，さらにアルゴリズムを改造することで離散対数問題も多項式時間内で解くことができるとされている．

つまり，巨大な合成数の素因数分解が困難であることを数学的根拠にしている RSA 暗号，ECDLP の求解困難性を利用している楕円曲線暗号にとって，Shor のアルゴリズムの登場と数十年前まで実現が難しいとされていたゲート方式の量子計算機の開発・改良が進んでいる現状は楽観視できないものとなっている．

2.3 解読手法

本節では，現代暗号に対する従来の解読手法と量子計算機を用いた解読手法を比較し，量子計算機を用いた場合に現代暗号が容易に危殆化しうることを示す．

まず，現代暗号に対し，暗号ごとに用いられる解読手法と計算量を表 1 にまとめた [8][9][10].

表 1 現代暗号を古典計算機上で解読する手法

	古典計算機上での解読手法と計算量
RSA 暗号	楕円曲線法　$L_p[\frac{1}{2}, 1.414]$
	一般数体ふるい法　$L_n[\frac{1}{3}, 1.901]$
楕円曲線暗号	Baby-step Giant-step 法　$O(\sqrt{\#P})$
	Pollard Rho 法　$O(\sqrt{\#P})$

ここで，関数 $L_x[u,v]$ は $L_x[u,v] = exp((v + o(1))(logx)^u(loglogx)^{1-u})$ と定義する．この関数は

$L_x[0,v] = exp(vloglogx) = (logx)^v$

$L_x[1,v] = exp(vlogx) = x^v$

となることより，多項式関数と指数関数の間，つまり準指数関数であることを示す．

また，$\#P$ は巡回群上の点 P に関する位数である．

次に，量子計算機上で Shor のアルゴリズムを用いて現代暗号を解読する場合について述べる．ここでは Shor のアルゴリズムを，素因数分解問題を解く場合を例として概説する．また，入力は L ビット長の合成数 N とする．

Step.1
因数が自明である場合，計算を行ってアルゴリズムを終了する．具体的には N が偶数である場合と N がべき乗数である場合に分かれるが，前者では因数は 2，後者では $N = x^y$ の形に変形して因数 x を出力する．

Step.2
$2 < a < N$ となる整数 a をランダムに選択する．

Step.3
gcd(a,N) を計算する．このステップでは，a とNに共通した（1 以外の）約数があるかをユークリッド互除法を用いて調べる．a と N が互いに素である場合は Step.4 に進み，そうでない場合（最大公約数が 1 以外にある場合），その数を因数として出力する．

Step.4
$X^r = 1 \ mod \ N$ となる r を量子位数発見アルゴリズムによって発見する（つまり，a と N の位数を求める）．

Step.5
$(X^{\frac{r}{2}} + 1)$ と N，または $(X^{\frac{r}{2}} - 1)$ と N の最大公約数のうち，1 でない方を返す（つまり，N の素因数のうちひとつを出力）．

ここで，Step.4 以外のステップはいずれも重い計算を含んでいないため，古典計算機で十分行うことができる．

以下に，Step.4 において量子位数発見アルゴリズム（量子フーリエ逆変換）を量子計算機上で行う場合の手順について詳述する．また，量子計算機では計算量は使用するトフォリゲートの数で評価されることに注意する．

Step.1
第 1 レジスタにおいて，$\frac{s}{r}$ の値を得るための量子ビットを用意する．（r は位数，s は $0 \leq s \leq r-1 | s \in \mathbb{Z}$）

Step.2
第 2 レジスタに，ビット数 L の量子ビットを用意する．このとき，0 ビット目にだけ X ゲートを適用して |1 > としておき，他ビットは |0 > としておく．

Step.3
ユニタリ変換 $U_{x,N} : |j> |k> \longrightarrow |j> |x^j k \ mod \ N>$ を行う．この変換を初期状態 $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{r-1} |j> |1>$ に適用すると，$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{r-1} |j> |x^j \ mod \ N>$ が得られる．

Step.4
第 1 レジスタに量子フーリエ逆変換を行うと，$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\frac{s}{r}> |u_s>$ が得られる．

Step.5
第 1 レジスタを観測するとランダムに s と $\frac{s}{r}$ が選ばれるため，これらから r を求めることで位数を得る．

Step.2 までの計算量は N のビット数の 2 倍より少し多い程度なので $O(L)$ とできる．

Step.3 の計算量は [6] より入力ビットの 3 乗，つまり $O(L^3)$ とある．

Step.4 の計算量は [7] より $O(L^2)$ とわかる．

Step.5 の計算量は，Step.5（連分数近似）自体を真の位数が求まるまで繰り返すが，高々入力ビットの桁数回行えばよいので $O(L)$ とできる．

よって，量子位数発見アルゴリズムで使用するゲートの数は $O(L^3)$ であることがわかる．これは，古典計算機上で因数分解や離散対数問題を多項式時間内に解く方法が知られていないことに対し，量子計算機では多項式時間の $O(L^3)$ で解くことができることを示している．

つまり，Shor のアルゴリズムを量子計算機で実装した際，非常に高速に因数分解や離散対数問題が解ける理由は，Shor のアルゴリズムの Step.4 において量子計算機の特性を利用した量子逆フーリエ変換によって位数を従来よりはるかに短い時間で求められるためである．逆を言えば，量子逆フーリエ変換を使用できない問題に関しては Shor のアルゴリズムが適用できず，現時点では量子計算機による解読の高速化が難しいということになる．

表 2 に，表 1 で示した計算量に加え，上記で述べた量子計算機で解読する際に主に用いられる解読手法と必要な計算量をそれぞれ示した [4][8][9][10].

従来の手法では RSA 暗号の解読に準指数関数時間，楕円曲線暗号の解読に指数関数時間がかかるために安全性が保持できるとされているが，量子計算機が実用化した場合，表 2 からこれら現代暗号は容易に危殆化しうることがわかる．

表 2 現代暗号を古典計算機と量子計算機それぞれで解読した場合の計算量

	古典計算機	量子計算機
RSA 暗号	楕円曲線法 $L_p[\frac{1}{2}, 1.414]$	Shor のアルゴリズム $O(L^3)$
	一般数体ふるい法 $L_n[\frac{1}{3}, 1.901]$	
楕円曲線暗号	Baby-step Giant-step 法 $O(\sqrt{\#P})$	Shor のアルゴリズム（多項式時間）
	Pollard Rho 法 $O(\sqrt{\#P})$	

2.4 耐量子計算機暗号

これらの経緯から，量子計算機でも解くことが難しい耐量子計算機暗号の開発が望まれている．耐量子計算機暗号はこれまでに様々な方式が提案されているが，これらは暗号アルゴリズムの種類により計算量的暗号型と情報理論的暗号型に大きく分けられる．

計算量的暗号型に類する耐量子計算機暗号は，「理論的には解読が可能であるが，古典計算機でも量子計算機でも効率的に（多項式時間内に）解くアルゴリズムが見つかっておらず，解読することが事実上困難である」という特長をもつ．

情報理論的暗号型に類する耐量子計算機暗号は，「攻撃者に解読に必要な情報を与えない仕組みによって，攻撃者が利用可能な計算能力が無限であっても原理的に平文を推測することが不可能である」という特長をもつ．この暗号の例として Vernam 暗号（ワンタイムパッド暗号）があるが，送信者と受信者の間で予め鍵を共有しなければならないことや鍵長が平文の長さに比例することなどから多くの課題がある．

計算量的暗号型に属する主な公開鍵暗号として，格子点探索問題を利用した格子暗号 [11]，線形符号の復号問題を利用した符号ベース暗号 [12]，多変数多項式を利用した多変数暗号 [13] などがある．本研究では，このうち安全性と効率のバランスが優れているとして学界での研究が活発化している格子暗号に注目した．

格子暗号とは，格子点探索問題と呼ばれる数学上の問題を安全性の根拠とする公開鍵暗号の総称である．

格子点探索問題における格子の性質として，同じ格子を構成できる基底が複数個存在することが知られており，その基底は任意の 2 本の基底が垂直に近い状態で交わっている「直交型」およびそれ以外の「非直交型」に分けられる．このとき，直交型基底から非直交型基底を演算することは容易であるが，非直交型基底から直交型基底を演算で求めることは非常に難しい．

格子暗号はこの一方向性を利用し，公開鍵として非直交型基底を使うことにより，「非直交型基底のみが与えられている状況で，ある条件（秘密鍵となるパラメタ）を満たす格子点を探索することは非常に難しい」という状況を作っている．

この格子点探索問題は Shor のアルゴリズムが扱う位数発見問題に帰着させることができないため，量子計算機に対して耐性をもつと言える．

格子暗号の実現方式は現在までに AD 方式，GGH 方式，NTRU 方式，LWE 方式の 4 つが提案されている．

AD 方式は近似版 SVP を安全性の根拠としており，1 ビットの平文の暗号化のみが可能である．

GGH 方式は CVP を，NTRU 方式は SVP を安全性の根拠としているが，両方式の安全性と CVP および SVP の難しさが同程度であるかについて現時点では知られていない．よって今後，各方式固有の脆弱性が発見され，安全性が低下するおそれがある．NTRU 方式に関しては，用いられている格子が特殊な構造を有しているために生じる特有の脆弱性を利用した攻撃手法が既に提案されている [17].

また，AD 方式と GGH 方式については Nguyen らによる厳密な安全性評価の結果，これらの方式は大幅な効率化が難しいことが指摘されたため，大きな進展は上がっていない [15][16].

LWE 暗号は Regev によって考案された格子暗号実現方式のひとつであり，現時点で他の暗号方式と比較した際に安全性と効率のバランスが現時点で最も優れていると考えられている．その根拠として，(1) LWE 暗号の安全性と，次章で詳述する LWE 問題の難しさが同程度であることが数学的に証明されているため，今後実現方式に起因する安全性の低下が起こりにくいこと (2) LWE 暗号は根拠とする数学的問題が相対的に他の暗号方式より難しいため，より短い鍵長で同等の安全性が保持できることの二点が上げられる．これらのことから，現在 LWE 暗号に関する研究が活発化している．

しかしながら，現在までに LWE 暗号の解読全体に必要な時間計算量を明示した論文は少なく，LWE 暗号の強度は明らかとは言い難い状況であった．そこで，次節以降で LWE 暗号の解読に必要な計算量を見積もり，LWE 暗号の強度を明らかにしていく．

3. LWE 暗号と解読手法

3.1 LWE 問題と LWE 暗号

Learning with Errors（LWE）問題の概略は次の通りである．

正の整数 q を用いた剰余類環 $\mathbb{Z}q$ を $\mathbb{Z}q = \mathbb{Z}/q\mathbb{Z} = \{0, 1, ..., q-1\}$ とする．次に，m × n 行列 $\mathbf{A} \in \mathbb{Z}_q^{\mathrm{m} \times \mathrm{n}}$ となる非直交型基底 $\mathbf{A}$ とランダムなベクトル $\mathbf{s} \in \mathbb{Z}_q^{\mathrm{n} \times 1}$ に対し，標準偏差 σ と平均が 0 である離散ガウス分布 χ_σ から生成される整数のエラーベクトル $\mathbf{e} \in \chi_\sigma^n$ を用いて，

$\mathbf{b} = \mathbf{A}\cdot\mathbf{s} + \mathbf{e}\, mod\, q$ とする．

つまり LWE 問題とは，素数 q を法とする有限体 $\mathbb{Z}_q$ 上からとった誤差 $\mathbf{e}$ を付加した連立一次方程式について，行列 $\mathbf{A}, \mathbf{s}$ が与えられたとき，ベクトル $\mathbf{s}$ を求める問題であり，次元 n，サンプル数 m，法 q，標準偏差 σ という 4 つのパラメタによって定義される．

2009 年，Regev はこの LWE 問題を安全性の根拠とする LWE 暗号を提案した [11]．以下に，清藤ら [14] の手法をもとにして次元 n=サンプル数 m，法 q，標準偏差 σ，平文 d，平文空間のサイズが D の Regev 方式の LWE 暗号の構成方法を説明する．

3.1.1 秘密鍵，公開鍵の生成

Step.1
受信者はベクトル $s \in \mathbb{Z}_q$，エラーベクトル $\mathbf{e} \in \chi_\sigma$ をそれぞれランダムに選択する．

Step.2
$\mathbf{A} \in \mathbb{Z}_q^{\mathrm{n}\times \mathrm{n}}$ と $\mathbf{s} \in \mathbb{Z}_q^{\mathrm{n}\times 1}$ を用いて乗算 $\mathbf{G} = \mathbf{A}\cdot\mathbf{s}\, mod\, q$ を行い，得られた結果 $\mathbf{G} \in \mathbb{Z}_q^{\mathrm{n}\times 1}$ を格子点とする．

Step.3
格子点 $\mathbf{G} \in \mathbb{Z}_q^{\mathrm{n}\times 1}$ にエラーベクトル $\mathbf{e} \in \chi_\sigma^n$ を加え，点 $\mathbf{T}$ に関して $\mathbf{T} = \mathbf{G} + \mathbf{e}\, mod\, q$ を計算する．

Step.4
$(\mathbf{s}, \mathbf{e})$ を秘密鍵とし，点 $\mathbf{T} \in \mathbb{Z}_q^{\mathrm{n}\times 1}$ を公開鍵とする．

3.1.2 送信者による暗号化

Step.1
乱数 $\mathbf{r} \in \chi_\sigma^{1\times \mathrm{n}}$ を発生させ，基底 $\mathbf{A}$ を用いて $\mathbf{C}_1 = \mathbf{r}\cdot\mathbf{A} mod q$ を計算する．

Step.2
$\mathbf{C}_2$ を，$\mathbf{C}_2 = \mathbf{r}\cdot\mathbf{T} - d\lfloor\frac{q}{D}\rfloor\, mod\, q$ として計算する．

Step.3
得られた $(\mathbf{C}_1, \mathbf{C}_2)$ を暗号文として送信する．

3.1.3 受信者による復号

Step.1
暗号文 $(\mathbf{C}_1, \mathbf{C}_2)$ と秘密鍵 $(\mathbf{s}, \mathbf{e})$ を用いて，$\mathbf{C}_1\cdot\mathbf{s} - \mathbf{C}_2 = -\mathbf{r}\cdot\mathbf{e} + d\lfloor\frac{q}{D}\rfloor\, mod\, q$ を計算する．

Step.2
d 番目の平文が「i」(i$\in 0, ..., D-1$) である条件は，
$(2i-1)\lfloor\frac{q}{2D}\rfloor < P_d < (2i+1)\lfloor\frac{q}{2D}\rfloor$
であり，この条件に合致した i を d 番目の平文として出力する．

復号の正当性について，誤差 $\mathbf{e}$ が $-\frac{q}{2D} < \mathbf{e} < \frac{q}{2D}$ であれば復号に成功する．エラーベクトルの各成分 $\mathbf{e}_i (i = 1, ...n)$ は標準偏差 σ の離散ガウス分布 χ_σ から選ばれているため，エラーベクトル $\mathbf{e}$ の標準偏差は高々 $\sqrt{n\sigma}$ となる．各パラメタの選択方法から $\sqrt{n\sigma} < \frac{q}{log\, n}$ なので，非常に高い確率で復号に成功することがわかる．

3.2 解読手法

LWE 問題に対する汎用的な攻撃として，以下に代表される手法が提案されている．

SIS(Short Integer Solution) 攻撃 LWE 問題を q-ary 格子に埋め込んで SVP 問題に帰着させ，SVP 問題を解く．

BDD(Bounded Distanve Decoding) 攻撃 nearest plane アルゴリズムにより CVP 問題に帰着させ，CVP 問題を解く．

現在までの LWE 暗号で利用される実用的なパラメタに対する解読アルゴリズムには，BDD 攻撃に extreme pruning と呼ばれる列挙法を適用する方法（計算量 $O(2^{n^2})$），BDD 攻撃に Kannan の embedding 法を適用する方法（計算量 $O(2^{\beta log\beta})$〜$O(2^\beta)$) がある（β は embedding 法中の BKZ アルゴリズムで用いられるブロックサイズを指す）．他にボロノイセルを用いる方法やガウス篩法を用いる方法があり，どちらも計算量は $O(2^n)$ を考えられているが，これら二つの方法では実行に $O(2^n)$ サイズのメモリが必要となる．

以下に，高木 [18] より一部改変した embedding 法を用いた LWE 暗号の解読法を記載する．

Step.0
LWE 暗号の入力 $\mathbf{T}$ に対し，次の $q\mathbf{Z}^n$ を部分格子としてもつ $q-ary$ 格子
$L = (\mathbf{A}, q) = \{\mathbf{v} \in \mathbf{Z}^{\mathrm{m}\times 1} | \mathbf{v} \equiv \mathbf{A}\cdot\mathbf{x} mod q, \mathbf{x} \in \mathbf{Z}^{\mathrm{n}\times 1}\}$
を考える．（ここで LWE 問題 $(\mathbf{T} \equiv \mathbf{A}\cdot\mathbf{s} + \mathbf{e}\, mod\, q)$ は，点 $\mathbf{T}$ に十分近い格子 $L(\mathbf{A}, q)$ 上の点を求める BDD となる．）

以下，この BDD を格子 $L(\mathbf{A}, q)$ をより大きな次元の unique-SVP に埋め込んで格子基底簡約により解くことを目標とする．

Step.1
格子 $L(\mathbf{A}, q)$ で張られる基底 $\mathbf{B}$ を，$\mathbf{B} = \begin{pmatrix}\mathbf{A}^T \\ q\mathbf{I}_m\end{pmatrix} \in \mathbf{Z}^{2\mathrm{n}\times \mathrm{n}}$ として構成する．

次に，基底 $\mathbf{B}$ のエルミート標準形（HNF）となる行列

$$\mathbf{B}_{HNF} = \begin{pmatrix} q\mathbf{I}_n & \mathbf{0} \\ \mathbf{A}' & \mathbf{I}_n \end{pmatrix} \in \mathbf{Z}^{\mathrm{n}} \times \mathrm{n}$$

を計算する．ここで，$\mathbf{A}'$ は $\mathbf{B}$ から求まる n × n 行列となる．

Step.2

基底 $\mathbf{B}_{HNF}$ に対し，ベクトル $\mathbf{T}$ を次のように埋め込み，一次元大きい格子の基底

$$\mathbf{B}' = \begin{pmatrix} \mathbf{B}_{HNF} & \mathbf{0} \\ \mathbf{T}^T & M \end{pmatrix} \in \mathbf{Z}^{(\mathrm{n}+1)} \times (\mathrm{n}+1)$$

に拡張する．このうち，定数 M は embedding factor と呼ばれ，区間 [1, \mathbf{e}\] の整数として選択する．

Step.3

格子 $L = (\mathbf{A}, q)$ の最短ベクトルの長さを λ_1，最短ベクトルに対し一次独立で最も短いベクトルの長さを λ_2 とする．$\lambda_2 > \gamma\lambda_1$ を満たす場合，γ–unique な最短ベクトルをもつと言う．

$M < \frac{\lambda_1}{2\gamma}$ を満たす場合，格子 $L(\mathbf{B}')$ はベクトル $(\mathbf{e}^T, M) \in \mathbf{Z}^{1} \times (\mathrm{n}+1)$ を γ–unique な最短ベクトルとしてもつ．

そのため，γ が十分に大きい場合，格子基底簡約アルゴリズムにより格子 $L(\mathbf{B}')$ の比較的短いベクトルを求めれば，エラーベクトル $\mathbf{e}$ が求まる．

ここでは，格子基底簡約アルゴリズムとして BKZ アルゴリズムを用いることとする．

Step.4

連立一次方程式 $\mathbf{T} - \mathbf{e} = \mathbf{A} \cdot \mathbf{s} \; mod \; q$ を解き，ベクトル $\mathbf{s}$ を求める．

この手法では，入力ベクトル $\mathbf{T} \in \mathbf{Z}^{\mathrm{n}} \times 1$ に最も近い格子点 $\mathbf{v} \in L(\mathbf{A}, q)$ で，それらの差がエラーベクトル $\mathbf{e}$ となる場合に攻撃が成功する．一般的には，次元 n か標準偏差 σ，素数 q が増加すると基底 $\mathbf{B}'$ で張られる格子の SVP の求解がより困難になるため，結果として LWE 暗号は難化すると考えられている．

4. 考察

LWE 暗号が耐量子計算機のスタンダードとして現代暗号に置換されうるかを判断する基準として，（1）少なくとも現時点において量子計算機による解読攻撃に耐えられるか（2）古典計算機でも無限大に近い計算リソースがあった場合に解読は可能なのか（3）鍵長や平文，暗号文のビット数などが実用的であるかの 3 点から論じるとともに，従来の安全性評価指標に照らすとどれだけのパラメタが必要であるかについても紹介し，考察を行う．

（1）について，2.4 節において概説した Shor のアルゴリズムは，量子重ね合わせを利用してフーリエ逆変換を高速に行うことで因数分解の計算量を大幅に短縮することを目的としていた．一方で，LWE 暗号についてはもとより，すべての格子暗号は数学的根拠に『非直交型基底を用いて所定の条件を満たす格子点を探索する問題』を用いており，これは因数分解を適用できる数学的問題ではない．さらに，3.2 節で示した通り LWE 暗号の解読には最速のアルゴリズムをもってしても $O(2^{\beta})$ の計算量が必要であり，時間と効率の兼ね合いが最もよいパラメタ β をとったとしても，解読には指数時間が必要となる．

次に（2）についてであるが，これはスーパーコンピュータを使用する場合など，解読側の計算リソースが非常に大きい場合を想定する．この想定に最も近いケースとして，ドイツのダルムシュタット工科大学が主催している LWE Challenge がある [23]．このチャレンジでは計算リソースに制限はかけられておらず，参加者が LWE 暗号のパラメタを指定してダウンロードし，解読できるかを競う．2021 年 1 月現在，解読済の問題のパラメタは最大で $(n, \alpha) = (40, 0.030)$ から $(75, 0.005)$ である ($\alpha = \frac{\sigma}{q}$)．LWE 暗号の類する計算量的暗号型では解読に 1 年以上を要するかが安全性の評価基準となっているため，3 桁以上の次元を取るなど望ましいパラメタ [14] を選択することでスーパーコンピュータによる解読に耐えることができると考えられる．

最後の（3）については，今回取り上げた Regev 方式の LWE 暗号では，公開鍵と暗号文のサイズが格子の次元 n に依存し，公開鍵は $O(n^2)$ の長さに，暗号文は平文の n 倍に増加するため実用化の観点からは効率的ではない．

以上より，Regev 方式による LWE 暗号は，現時点では量子計算機を用いても現実的な時間内に解読することはできないが，鍵長や暗号文，平文のサイズが現代暗号よりも非常に大きくなってしまうことから，実用化には不向きと言わざるを得ない．

しかしながら，サイズの欠点を改良したものとして，有限体のかわりに円分体の整数環上での演算に限定した ring-LWE(RLWE) 暗号が Lindner, Peikerd, Regev の三人によって提案されている [24]．ring-LWE 暗号では公開鍵の鍵長を数千ビット程度に抑えることができ，複数ビットの平文を多項式の係数で表すことで暗号文のサイズを格段に小さくできる．また，暗号文同士の演算が多項式演算で閉じているため，DFT(Discrete Fourier Transform; 離散フーリエ変換) や FFT(Fast Fourier Transform; 高速フーリエ変換) を用いた計算の高速化を行うことができる．また，高木らのグループの JavaScript による実装で，公開鍵，秘密鍵，暗号文のサイズがそれぞれ 1.42kByte,0.19kByte,0.99kByte（暗号パラメタ:n=320,q=590921, σ=35.77）と非常に短いものが得られ，暗号化および復号について汎用 PC で数 ms という結果を残している [18].

また，格子暗号は現代暗号の多くと同じように準同型性をもつ．他の耐量子計算機暗号の候補とは異なり，データを暗号化したまま任意の計算を行える秘匿計算，データと検索クエリを暗号化したまま検索できる秘匿検索を実現できる完全準同型暗号という特長を有しており，利便性が高いため研究が盛んに行われている．準同型性には加法準同型性と乗法準同型性があり，どちらの性質も持ち合わせ，さらに乗法について回数の制限がない準同型暗号のことを完全準同型暗号（Fully Homomorphic Encryption, FHE）と呼ぶ．この完全準同型暗号を，LWE 暗号を用いて実現したスキームが存在する [25].

これらのことから，ring-LWE 暗号は耐量子計算機暗号のスタンダードとして現代暗号に置換しうる可能性が十分にあると言える．

5. おわりに

本研究では，量子計算機の台頭によって現代暗号が危殆化する可能性について言及した上で，計算量の観点から現代暗号と LWE 暗号の堅牢性を確かめ，（ring-）LWE 暗号が耐量子計算機暗号のスタンダードとして現代暗号に置換しうるかを考察した．

耐量子計算機暗号の今後の課題として，鍵長の短縮と並行し，安全なプロトコルの整備（規格化，標準化）や完全準同型暗号の実現などが挙げられる．

今回取り上げた LWE 暗号や ring-LWE 暗号をはじめとした格子暗号は現段階では鍵長が大きいことがデメリットであるが，研究は未だ途上であることに加え，秘密計算などこれからのインターネット社会に必要な機能も備えているため，今後さらなる研究の進展が見込まれる．

参考文献

[1] Rivest, Ronald L.; Shamir, Adi; Adelman, Len M; *A Method for Obtaining Digital Signature and Public-key Cryptsystems*, MIT-LCS-TM-082（MIT Laboratory for Computer Science）(1977).
[2] Miller, V; *Use of elliptic curves in cryptography*, CRYPTO. Lecture Notes in Computer Science 85: pp.417-426.(1985)
[3] Koblitz, N; *Elliptic curve cryptosystems*, Mathematics of Computation 48 （177）: pp.203-209.(1987)
[4] Shor, P.W; *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: pp.124-134.(1994)
[5] National Institute of Standards and Technology （NIST）; *Recommendation on KeyManagement Part I: General*, Special Publication （SP） 800-57, 2005a.(2007)
[6] Vedral, V V et al.; *Quantum Networks for Elementary Arithmetic Operation*, Physical review. A, Atomic, molecular, and optical physics vol. 54,1 pp.147-153. (1996)
[7] M. Nielsen, I. Chuang, 木村達也（訳）：量子コンピュータと量子通信 < 2 >『量子コンピュータとアルゴリズム』オーム社 (2005)
[8] 伊豆哲也：楕円曲線法の高速化について, 情報処理学会研究報告． AL， アルゴリズム研究会報告 69, pp.53-60.(1999)
[9] Pollard, J. M.; *Monte Carlo methods for index computation*（*mod p*）, Mathematics of Computation 32（143）: pp.918-924.(1978)
[10] Daniel Shanks; *Class number, a theory of factorization and genera*, In Proc. Symp. Pure Math., Providence, R.I.: American Mathematical Society, 20, pp. 415-440.(1971)
[11] Regev, Oded; *On lattices, learning with errors, random linear codes, and cryptography*, Journal of the ACM. 56（6）: pp.1-40.(2009)
[12] McEliece, Robert J.; *A Public-Key Cryptosystem based on Algebraic Coding Theory*, JetPropulsion Laboratory DSN Progress Report, 42-44, pp.114-116.(1978)
[13] Matsumoto, Tsutomu, and Hideki Imai; “*Public Quadratic Polynomial-Tuples for EfficientSignature-Verification and Message-Encryption*, Proceedings of EUROCRYPT, LNCS330, Springer-Verlag, pp. 419-453.(1988)
[14] 清藤武暢，青野良範，四方順司：「量子コンピュータの解読に耐えうる「格子暗号」の最新動向」『金融研究』第 34 巻第 4 号，日本銀行金融研究所，pp.135-170.(2015)
[15] Nguyen, Phong, Jacques Stern; *Cryptanalysis of the Ajtai-Dwork Cryptosystem* Proceed-ings of CRYPTO, LNCS 1462, Springer-Verlag, pp. 223-242.(1998)
[16] Nguyen, Phong; *Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem fromCrypto ’97*, Proceedings of CRYPTO, LNCS 1666, Springer-Verlag, pp. 288-304.(1999)
[17] Coppersmith, Don, and Adi Shamir; *Lattice Attacks on NTRU* Proceedings of EURO-CRYPT, LNCS 1233, Springer-Verlag, pp. 52-61.(1997)
[18] 高木剛：「ポスト量子暗号の構成法とその安全性評価」Fundamentals Review，11（1），電子情報通信学会 基礎・協会ソサイエティ，pp17-27.(2017)
[19] Micciancio, Daniele, and Oded Regev; *Worst-case to Average-case Reductions based onGaussian Measures* Journal of Computing, 37（1）, pp. 267-302.(2007)
[20] 青野良範・林卓也・レチュウフォン・王立華：セキュリティアップデータブル準同型暗号を用いた秘匿データの線形回帰計算，暗号と情報セキュリティシンポジウム (2015)
[21] Laine, Kim, and Kristin Lauter; *Key Recovery for LWE in Polynomial Time*, IACR Cryp-tology ePrint Archive, no. 176(2015)
[22] Albrecht, Martin R., Carlos Cid, Jean-Charles Faugere, Robert Fitzpatrick, and LudovicPerret; *Algebraic Algorithms for LWE Problems* IACR Cryptology ePrint Archive,no. 1018,(2014)
[23] *TU Darmstadt LWE Challenge*; TU Darmstadt(URL: https://www.latticechallenge.org/lwe_challenge/challenge.php) (2021.02.15)
[24] Vadim Lyubashevsky, Chris Peikert, and Oded Regev; *On ideal lattices andlearning with errors over rings*, InAnnual International Conference on theTheory and Applications of Cryptographic Techniques, pp.1-23. Springer(2010)
[25] Brakerski, Z, Vaikuntanathan, V; *Efficient fully homomorphic encryption from （standard） LWE* SIAM Journal on Computing, 43（2）, pp.831-871.(2014)