IMES DISCUSSION PAPER SERIES

量子コンピュータに耐性のある暗号技術の標準化動向：米国政府標準暗号について

四方順司（しかた じゅんじ）

Discussion Paper No. 2019-J-4

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
https://www.imes.boj.or.jp

IMES Discussion Paper Series 2019-J-4
2019 年 3 月

量子コンピュータに耐性のある暗号技術の標準化動向：米国政府標準暗号について

しかたじゅんじ
四方順司*

要　旨

近年、これまでとは異なる新たな計算技術として、量子コンピュータの研究開発が進展している。量子コンピュータは、現代のコンピュータと比較して高速な演算処理が可能とされているため、その将来的な実用化の可能性を見据えて、量子コンピュータに耐性を有する暗号技術の研究開発が活発化している。現在、米国政府は量子コンピュータでも解読できない暗号技術（公開鍵暗号やデジタル署名）の標準化を進めており、全世界から標準化候補の方式を募集し、今後、数年をかけて米国政府標準暗号を選定する計画である。本稿では、その候補になっている暗号技術を概観し、それらの特徴について解説する。

キーワード：鍵カプセル化メカニズム、鍵配送、公開鍵暗号、耐量子計算機暗号、デジタル署名、標準化
JEL classification: L86、L96、Z00

* 横浜国立大学大学院環境情報研究院（E-mail: shikata@ynu.ac.jp）

本稿は、筆者が日本銀行金融研究所客員研究員の期間に行った研究をまとめたものである。本稿の作成に当たっては、三菱電機株式会社の高島克幸氏、および金融研究所スタッフから有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

１．はじめに

近年、これまでとは異なる新たな計算技術として、量子コンピュータの研究開発が進展している[1]。量子コンピュータとは、量子力学の性質を演算処理に利用したコンピュータの総称であり、現代のコンピュータと比較して高速な演算処理が可能となることが期待されている。特に、量子コンピュータが注目されているのは、現代のコンピュータでは素因数分解問題を高速に解く手法が知られていないのに対し、量子コンピュータではこれが可能となるとされているからである（Shor [1994, 1997]）。このことは、現在、金融分野等で主流で用いられている RSA 暗号（Rivest, Shamir, and Adleman [1978]）が量子コンピュータに対して安全でないことを意味する。そのため、量子コンピュータの将来的な実用化の可能性を見据えて、量子コンピュータに耐性を有する暗号技術の研究開発が活発化してきている。

このような状況に対して、米国立標準技術研究所（National Institute of Standards and Technology：NIST）は、「現在主流の RSA 暗号を数時間で解読可能な量子コンピュータが 2030 年までに登場する可能性がある」との見解を示しており、現在、NIST は量子コンピュータでも解読できない公開鍵暗号、デジタル署名等の標準化を進めている。具体的には、NIST は 2017 年 11 月末を期限に全世界から標準化候補の方式を募集し、その後、数年をかけて米国政府標準暗号を選定する計画としている（National Institute of Standards and Technology [2017]）。

本稿では、その候補になっている暗号技術を概観し、それらの特徴について解説する。

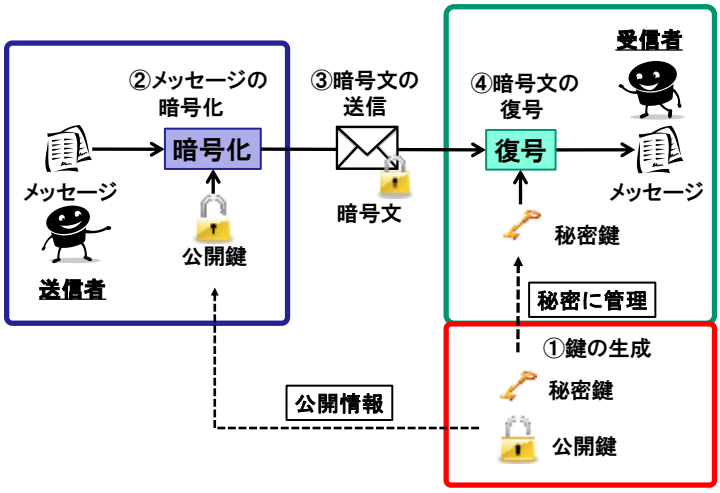
２．暗号技術のモデルと安全性

（１）公開鍵暗号

公開鍵暗号（Public Key Encryption: PKE）は、暗号化に利用する鍵（公開鍵）と復号に利用する鍵（秘密鍵）が異なり、秘密鍵は各利用者が秘密に管理する一方、公開鍵を公開できるという特長を有する。ここで、受信者は、予め公開鍵と秘密鍵を生成し、公開鍵を公開するとともに、秘密鍵を自身で秘密に管理する。また、送信者はこの公開鍵を入手しているものとする。送信者は、公開鍵を用いてメッセージ（平文）を暗号文に変換したうえで送信し、それを受信した受信者は秘密鍵を用いてもとのメッセージに復号する（図表 1 を参照）。

[1] 量子コンピュータには、量子ゲート型コンピュータと量子アニーリング型（量子イジングマシン型とも呼ばれる）コンピュータの 2 種類の実装方法が知られている（清藤・青野・四方［2015］等を参照）。

図表 1. 公開鍵暗号のモデル



公開鍵暗号の安全性を検討する際には、公開鍵を有する攻撃者を想定する。攻撃者が公開鍵から秘密鍵を効率よく計算できないように構成することは最低限必要であるが、それ以上の安全性レベル――すなわち、攻撃者に、攻撃対象となる暗号文からメッセージの内容が漏えいしないこと――を設定することが一般的である。特に、選択平文攻撃に対する識別困難性（IND-CPA 安全性）と、選択暗号文攻撃に対する識別困難性（IND-CCA 安全性）を備えていることが標準的な安全性レベルとされており、これらは、米国政府標準暗号の選定過程でも採用されている[2,3]。IND-CPA 安全性とは、公開情報にアクセス可能な攻撃者が、攻撃対象となる暗号文からそのメッセージの部分情報さえも（1 ビットの情報さえも）得られないという安全性レベルである。また、IND-CCA 安全性とは、公開情報だけでなく任意の暗号文とその復号結果をも知りうる攻撃者が、攻撃対象となる暗号文からそのメッセージの部分情報さえも（1 ビットの情報さえも）得られないという安全性レベルである[4,5]。

IND-CCA 安全性は、公開鍵暗号における最も高い安全性レベルであるため、多くのアプリケーションにおいてこの安全性レベルが必要とされる。一方で、アプリケーションによっては、IND-CPA 安全性で十分と考えられる場合もありうる。また、暗号構成の観点からみると、IND-CPA 安全性を構成する方式の方がメカニズムが簡潔であり、鍵生成・暗号化・復号処理に必要な各種アルゴリ

[2] IND-CPA は Indistinguishability against Chosen Plaintext Attack の略である。
[3] IND-CCA は Indistinguishability against Chosen Ciphertext Attack の略である。
[4] ただし、当然のことながら、攻撃対象となる暗号文の復号結果は知りえないとする。
[5] これらに加えて、OW-CPA 安全性という安全性レベルもある。OW-CPA は One-Wayness against Chosen Plaintext Attack の略である。脚注 7 参照。

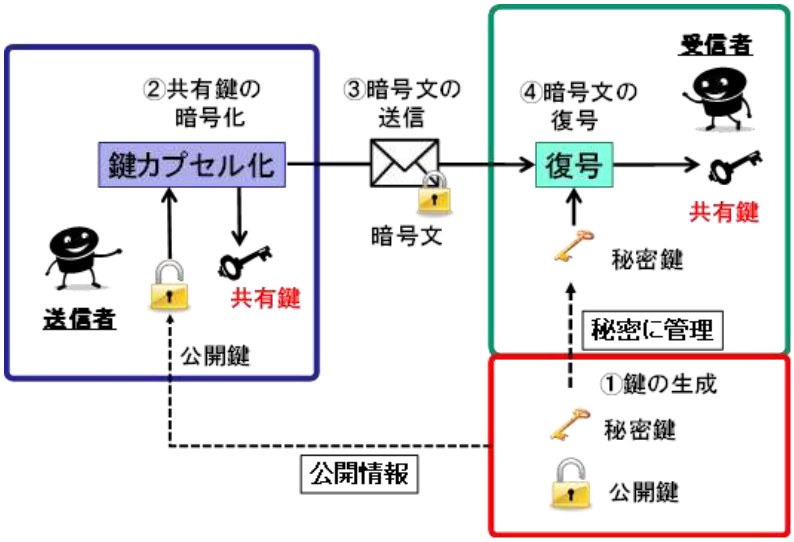
ズムの計算時間の短縮や、公開鍵・秘密鍵・暗号文のサイズの削減等により、効率的に構成できる場合も多い。こうした安全性レベルと効率性のトレードオフを踏まえ、公開鍵暗号の安全性レベルとして、IND-CPA 安全性と IND-CCA 安全性のいずれかを備えていることが重要とされている。

（２）鍵カプセル化メカニズム（KEM）

鍵カプセル化メカニズム（Key Encapsulation Mechanism：KEM）は、公開鍵暗号の仕組みを利用して、送信者から受信者への 1 回の通信により、送信者と受信者の間で共有する鍵（共有鍵）を受信者に配送する技術（key transport）である[6]。KEM によって送信者から受信者への共有鍵の配送を実現することができれば、共通鍵暗号（AES 等）を利用することで高速な暗号通信が可能となる。

KEM のモデルは、以下のとおりである。まず、受信者は、予め公開鍵と秘密鍵を生成し、公開鍵を公開し、秘密鍵を自身で秘密に管理する。また、送信者はこの公開鍵を入手しているものとする。送信者は、鍵カプセル化処理を行うことで、ランダムな共有鍵とその暗号文を生成し送信する。暗号文の受信者は、自身の秘密鍵を用いて暗号文から共有鍵を復号する（図表 2 を参照）。

図表 2.　KEM のモデル



[6] 鍵を共有するためのプロトコルである鍵配送方式としては、ディフィ＝ヘルマン（Diffie-Helmann）方式が有名である。なお、鍵配送方式において用いる通信回数に特に制限はないが、通信回数が増えると、その安全性定義が複雑になることが多い。この点、KEM は、公開鍵暗号のモデルに類似した 1 回の通信による鍵配送方式であるため、その安全性は公開鍵暗号の安全性と同様に簡潔に定義することが可能である。また、一般に、公開鍵暗号では送信者が任意に選んだメッセージを送信するのに対して、KEM は（必ずしも送信者が選ぶ必要のない）一様ランダムな鍵を送信するだけであるため、公開鍵暗号よりも効率的に構成できる余地がある。

KEM においても、公開鍵暗号と同様に IND-CPA 安全性または IND-CCA 安全性を設定するのが標準的であり、米国政府標準暗号の選定でも採用されている。

一般に、共通鍵暗号は公開鍵暗号よりも暗号化や復号を高速に処理できるメリットがあるが、送受信者間での鍵の共有が必要となる。一方、公開鍵暗号は、暗号化を公開鍵で行うため、送受信者間での鍵の共有を必要としない。そこで、公開鍵暗号と共通鍵暗号の両方の特長を活かす暗号通信の仕組みとして、ハイブリッド暗号（Cramer and Shoup [2004]、Shoup [2000]）が考案されている。ハイブリッド暗号では、KEM によって送信者から受信者へ共有鍵の配送を行い、個々のメッセージはその共有鍵を用いて共通鍵暗号により暗号化を行う。ハイブリッド暗号の枠組みで利用される共通鍵暗号は DEM（Data Encapsulation Mechanisum）と呼ばれる。KEM と DEM を組み合わせたハイブリッド暗号は、公開鍵暗号の安全性を実現するだけでなく、任意のメッセージの暗号化には共通鍵暗号を利用するため、高速処理も実現することが可能である。

（３）IND-CCA 安全性を満たす公開鍵暗号や KEM の構成法

IND-CCA 安全性を満たす公開鍵暗号や KEM を構成する手法として、まずは、OW-CPA 安全性を満たす公開鍵暗号を構成し、それを（量子）ランダムオラクルモデルを用いて、IND-CCA 安全性を満たす公開鍵暗号や KEM に変換する手法が知られている[7,8]。その代表的な変換手法としては、FO 変換（Fujisaki and Okamoto [1999]）、TU 変換（Targhi and Unruh [2016]）、デント変換（Dent [2003]）、HHK 変換（Hofheinz, Hövelmanns, and Kiltz [2017]）が挙げられる。

いずれの変換も相対的に弱い安全性である OW-CPA 安全性を満たす公開鍵暗号に適用するものであるが、FO 変換と TU 変換を適用した場合には IND-CCA 安全性を満たす公開鍵暗号が構成されるのに対し、デント変換と HHK 変換を適用した場合には IND-CCA 安全性を満たす KEM が構成される。

これらの変換手法の特徴をまとめたのが図表 3 である。現在、NIST に提出さ

---

[7] OW-CPA 安全性は、公開情報にアクセス可能な攻撃者が、攻撃対象となる暗号文からもとのメッセージを完全には計算できないという安全性レベルであり、IND-CPA 安全性よりも弱い安全性である。

[8] ランダムオラクルモデルとは、ランダム関数（任意の入力分布に対して、その出力の分布が一様ランダムな関数）を利用するモデルである。また、量子ランダムオラクルモデルとは、量子ランダム関数（入力として重ね合わせ状態の入力を与えたとき、その出力が乱数の重ね合わせ状態である関数）を利用するモデルである。ランダム関数を利用せずに IND-CCA 安全性を満たす公開鍵暗号や KEM の構成法も考えられるが、一般にランダムオラクルモデルによる構成の方が鍵サイズ（公開鍵、秘密鍵）や暗号文サイズを小さくできるという利点がある。NIST の公募では、量子コンピュータでも計算が困難な問題（3 節参照）を利用し、要求する安全性（IND-CCA 安全性や UF-CMA 安全性等）を満たす方式を求めており、ランダム関数あるいは量子ランダム関数の使用は必須という訳ではない。

図表 3. IND-CCA 安全な方式への変換手法

変換手法	変換前の方式	変換後の方式	モデル
FO 変換	公開鍵暗号 （OW-CPA 安全性）	公開鍵暗号 （IND-CCA 安全性）	RO
TU 変換	公開鍵暗号 （OW-CPA 安全性）	公開鍵暗号 （IND-CCA 安全性）	QRO
デント変換	公開鍵暗号 （OW-CPA 安全性）	KEM （IND-CCA 安全性）	RO
HHK 変換	公開鍵暗号 （OW-CPA 安全性）	KEM （IND-CCA 安全性）	RO/QRO

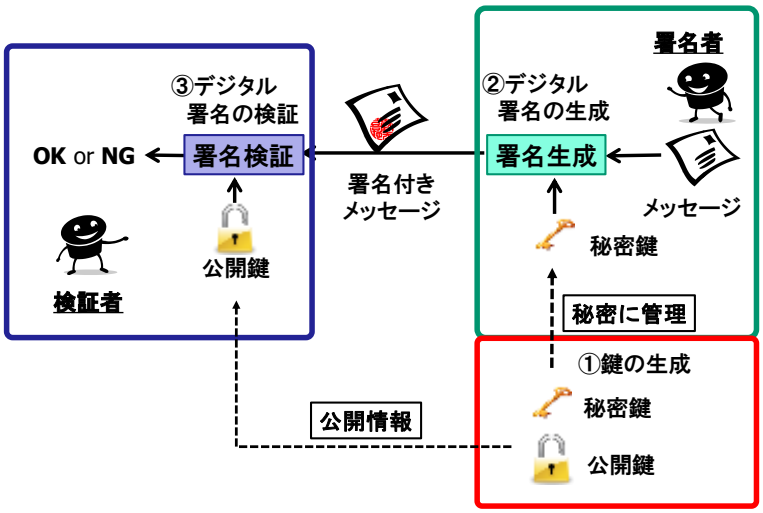
備考：RO はランダムオラクルモデル、QRO は量子ランダムオラクルモデルであることを示す。

れている公開鍵暗号や KEM のうち IND-CCA 安全性を満たすと主張されているほとんどすべての方式は、これらのいずれかの変換手法を利用して構成されている。

（４）デジタル署名

デジタル署名は、メッセージに署名（signature）と呼ばれるデータを付加することにより、署名が付加された時点からそのメッセージが改ざんされていないことを検証できる技術である。デジタル署名は、署名生成時に利用する鍵（秘密鍵）と署名検証時に利用する鍵（公開鍵）が異なるため、検証者は公開情報だけでメッセージの真正性を検証できる。すなわち、署名者は、メッセージと秘密鍵を用いて署名を生成し、その署名をメッセージに付加したデータ（以下、署名付きメッセージと呼ぶ）を検証者に送信する。それを受信した検証者は、公開鍵を用いてそのメッセージの真正性を検証する（図表 4 を参照）。

図表 4.　デジタル署名のモデル



デジタル署名の安全性として、公開鍵暗号の場合と同様に、攻撃者が公開鍵から秘密鍵を効率よく計算できないように構成することは最低限必要であるが、それ以上の安全性レベルを設定することが一般的である。デジタル署名については、選択メッセージ攻撃に対する偽造困難性（UF-CMA 安全性）と、選択メッセージ攻撃に対する強偽造困難性（SUF-CMA 安全性）を備えていることが標準的な安全性レベルとされており、この安全性レベルは米国政府標準暗号の選定過程でも採用されている[9,10]。

ここで、UF-CMA 安全性とは、任意のメッセージとその署名のペアを複数個手に入れることができる攻撃者（以下、選択メッセージ攻撃を行う攻撃者と呼ぶ）が、新たなメッセージに対応する署名を生成できないという安全性レベルである。また、SUF-CMA 安全性とは、選択メッセージ攻撃を行う攻撃者が、手に入れたメッセージとその署名のペア以外に、メッセージと署名の新たなペアを生成できないという安全性レベルである。SUF-CMA 安全性における攻撃者の生成目標であるメッセージと署名の新たなペアは、新たなメッセージとその署名（UF-CMA 安全性における攻撃者の生成目標）、または、すでに手に入れたメッセージとそれに対応する他の署名であってもよい[11]。このため、SUF-CMA 安全性は、UF-CMA 安全性よりも強い安全性レベルである。

一般に、デジタル署名方式を単独で利用する場合は UF-CMA 安全性を満たせば実用上は十分と考えられるが、他の暗号技術と組み合わせて利用する場合は SUF-CMA 安全性が要求されることがしばしばある（Chiba *et al*. [2011]等）[12]。米国政府標準暗号の選定では、デジタル署名の安全性レベルとして、UF-CMA 安全性以上の安全性が要求されており、現在、NIST に提出されているほとんどのデジタル署名方式は、UF-CMA 安全性を満たすかたちで設計されている。

３．利用される計算問題

量子コンピュータでも計算が困難な問題として、NP 困難問題と呼称される問題が利用され、その具体的なものとして、格子点探索問題、誤り訂正符号の復号問題、多変数連立方程式の求解問題等がある[13]。以下では、これらについて解

---

[9] UF-CMA は Unforgeability against Chosen Message Attack の略である。また、存在的偽造困難性（Existential Unforgeability against Chosen Message Attack：EUF-CMA）とも呼ばれる。

[10] SUF-CMA は Strong Unforgeability against Chosen Message Attack の略である。

[11] もっとも、このケースは、1 つのメッセージに対して複数の署名が存在しうるデジタル署名方式のケースに限られる。

[12] 例えば、Chiba *et al*. [2011]では、安全な署名付き暗号化方式（Signcryption）を構成するための基礎技術として、SUF-CMA 安全性を満たすデジタル署名が必要とされている。

[13] NP（Non-deterministic Polynomial time）とは、現代のコンピュータの標準的な計算モデルであるチューリング機械により、ある有力な「ヒント」が与えられれば多項式時間で解ける判定問題

説する。

（１）格子点探索問題

イ．概要

格子とは、ベクトル空間上に規則正しく並んでいる点の集合であり、次元nと、構成する点集合を定義するための基底**A**により記述される。ここで、n次元ベクトル空間において、基底 **A** はn個の一次独立なベクトルで与えられ、各ベクトルを整数倍し足し合わせてできるすべての点の集合が（基底**A**による）格子と定義される。基底 **A** はn個の一次独立なベクトルを並べて、$n \times n$の行列として表現される。以下では、基底 **A** によって定義される格子を L(**A**)と書く。また、L(**A**)の要素を格子点とよび、L(**A**)に含まれる零でない格子点の中で最も短い長さをλ(**A**)とする[14]。

格子点探索問題とは、L(**A**)が与えられたときに、ある条件を満たす格子点を探索する問題の総称である。以下では、その代表的な問題を解説する。

ロ．SVP と CVP

格子点探索問題のうち、最も基本的な問題は、最短ベクトル問題（SVP）と最近ベクトル問題（CVP）である[15,16]。SVP とは、L(**A**)が与えられたときに、その格子点の中で最も短い非零ベクトルを求める問題であり、NP 困難問題である（van Emde Boas [1981]、Ajtai [1998]）。SVP の条件を緩和して、一定の値以下の長さを持つ非零ベクトルを求める問題は近似 SVP と呼ばれる[17]。また、CVP とは、L(**A**)とn次元ベクトル空間の 1 点xが与えられたときに、xに最も近い格子点を探索する問題である。特に、（近似）CVP は（近似）SVP 以上に計算困難な問題であることが知られている（Goldreich *et al.* [1999]）[18]。また、CVP から派

の集まりである。NP 困難問題は、NP に属するどの問題よりも同程度以上に難しい計算問題である。ただし、チューリング機械にtビットの入力データを与えた場合に、tのべき乗t^c回（cは自然数）の演算動作で出力値を計算できるとき、多項式時間で問題が解けると呼ぶ。現在のコンピュータでは、NP 困難問題に対する多項式時間の解法はないと予想されており、また量子コンピュータであっても多項式時間の解法はないと予想されている。

[14] 格子点の長さとは、その格子点から原点までの距離をいう。

[15] SVP は Shortest Vector Problem の略である。

[16] CVP は Closest Vector Problem の略である。

[17] SVP は厳密に原点（零ベクトル）から一番近い距離λ = λ(**A**)の格子点を求める問題であるが、この条件を少し緩くして、原点（零ベクトル）から距離 γλ(γ > 0)以内にある格子点（ただし、原点は除く）を求める問題が近似 SVP であり、γは近似因子と呼ばれる。γ = 1のときの近似 SVP が SVP になる。近似 SVP は、γ が$\sqrt{n}$に比例する値（すなわち、γ = O($\sqrt{n}$)）であるとき、NP 困難である（Khot [2005]）。

[18] 近似 CVP は、近似 SVP と同様に、近似因子γにより求めることができる。γ = 1のときの近似 CVP が CVP になり、NP 困難である（van Emde Boas [1981]）。

生した BDD 問題は、L(**A**) と実数$\alpha > 0$に加えて、格子点までの最短距離が$\alpha \cdot \lambda(\mathbf{A})$未満であるようなベクトル$x$が与えられたとき、$x$に最も近い格子点を探索する問題である[19]。

ハ. LWE 問題と SIS 問題

NIST に提出されている多くの方式は、LWE 問題（Regev [2009]）またはそれに深く関係する問題を利用している[20]。これらの問題においては、格子の構造として、整数成分の$n \times n$行列A、素数qに対して、$L(A,q) = \{x \in \mathbb{Z}^n | Ax = 0 \pmod q\}$で表される格子を用いる[21]。また、LWE 問題には、厳密には探索問題と判定問題があるが、これらの計算困難性は同程度であることが知られているため、本稿では探索問題だけを紹介する[22]。

LWE 問題は、一様ランダムなベクトル$\boldsymbol{a}$と秘密のベクトル$\boldsymbol{s}$の内積$\langle \boldsymbol{a}, \boldsymbol{s} \rangle$にエラーと呼ばれる乱数値$e$を足した値が与えられたときに、$\boldsymbol{s}$を求める問題である。また、Ring-LWE 問題（Lyubashevsky, Peikert, and Regev [2010]）は、LWE 問題から派生した問題であり、一様ランダムな多項式$\boldsymbol{a}$と秘密の多項式$\boldsymbol{s}$の積$\boldsymbol{as}$に乱数値eを足した値が与えられたときに、もとの$\boldsymbol{s}$を求める問題である。Module-LWE 問題（Brakerski, Gentry, and Vaikuntanathan [2012]）は、LWE 問題と Ring-LWE 問題を一般化した問題であり、問題のパラメータ（$\boldsymbol{a}$や$\boldsymbol{s}$を選択する集合）として多項式を成分とするベクトルを選択することにより、LWE 問題と Ring-LWE 問題のいずれも（あるいはその中間的な問題も）表現できる。

LWR 問題（Banerjee, Peikert, and Rosen [2012]）とは、LWE 問題から派生した問題であり、LWE 問題におけるエラーをランダムでなく特殊な関数に基づき選択する問題である[23]。LWE 問題から Ring-LWE 問題や Module-LWE 問題が派生したのと同様に、LWR 問題から Ring-LWR 問題や Module-LWR 問題を定義することができる。また、SIS 問題（Micciancio and Regev [2007]）とは、素数qと行列 A が与えられたとき、$Az = 0 \bmod q$を満たす長さの短いベクトルzを求める問題である[24]。

---

[19] BDD は Bounded Distance Decoding の略である。

[20] LWE は Learning With Errors の略である。

[21] このようなqは、しばしばモジュラスと呼ばれる。また、qとして素数そのものだけでなく素数のべき乗を用いることもある。

[22] 一般に、判定問題とは、与えられた値がある条件を満たすか否かを判定する問題であり、その解は 2 値である（例えば、満たすなら 1、満たさないなら 0 が解となる）。

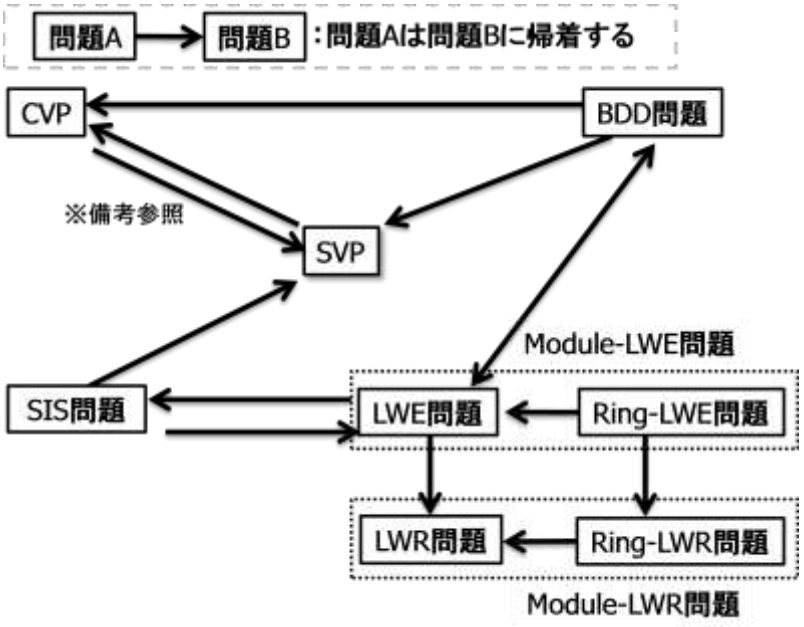
[23] LWR は Learning With Rounding の略である。LWR 問題は Rounding 関数と呼ばれる関数に基づく。Rounding 関数とは、ある整数をある自然数で割るときに、小数点以下を切り上げたり切り下げたりしながら近い整数に丸める関数である。

[24] SIS は Small Integer Solution の略である。

二．各種問題の関係性

図表 5 は、上記の問題の関係性を示している。この関係性から、上記ロ．およびハ．で挙げた各種問題の難しさを比較することができる。図表 5 から（近似）SVP と（近似）CVP の困難性は同程度であることがわかる。これらの問題は、格子に関わる問題の中では最も難しく、（近似）CVP よりも（近似）SVP の方が問題の設定が単純であるため、（近似）SVP の解読手法による安全性評価が主流となっている[25]。

図表 5. 格子問題の関係性



備考：「問題 A が問題 B に（多項式時間）帰着する」とは、問題 B の解法から問題 A の解法への多項式時間の変換が存在することを意味する。問題 A が問題 B に帰着する場合、B の方が A よりも相対的に難しい問題（あるいは同等）であることを意味する。また、図表では SVP、CVP の近似因子をγ、BDD 問題の実数パラメータ$\alpha = 1/\gamma$としている。厳密な CVP から SVP への帰着は示されていないが、この帰着はほぼ成立すると考えられている（Goldreich, Goldwasser, and Halevi [1997]）。

[25] SVP の解を求めるアルゴリズムとして、改良版 Enumeration アルゴリズム（Schnorr and Hörner [1995]、Gama, Nguyen, and Regev [2010]）、Sieving アルゴリズム（Micciancio and Voulgaris [2010]、Schneider [2011]、Pujol and Stehlé [2009]）が挙げられる。また、近似 SVP の解を求めるアルゴリズムとして、LLL アルゴリズム（Lenstra, Lenstra, and Lovász [1982]）、KZ 基底簡約アルゴリズム（Korkine and Zolotarev [1873]）、BKZ（Block Korkine-Zolotarev）アルゴリズム（Schnorr and Euchner [1994]、Chen and Nguyen [2011]）が挙げられる。

ホ．暗号を構成する仕組みと利用する問題

一般に、基底をランダムに選択した格子には特別な数学的構造が現れることは稀であるため、LWE 問題に対する更に効率的な攻撃法が発見される可能性は低いと考えられるが、その分 LWE 問題を基盤にした方式では、鍵サイズ（公開鍵、秘密鍵）と暗号文サイズが大きくなり、非効率になるという問題がある。一方、多項式で構成される格子問題（Ring-LWE 問題）は特別な数学的構造を含むため、Ring-LWE 問題を基盤にした方式では、その構造を利用して鍵サイズ（公開鍵、秘密鍵）と暗号文サイズを小さくできるという利点があるが、その数学的構造のため新たな攻撃を招く可能性がありうる。そういう意味で、LWE 問題と Ring-LWE 問題の選択は、安全性と効率性のトレードオフと捉えることができる。さらに、Module-LWE 問題に基づく方式では、安全性と効率性の組み合わせを、パラメータによって選択することが可能である。安全性と効率性の観点から、どのような格子関連の計算問題を選択するかは、方式の設計思想による。

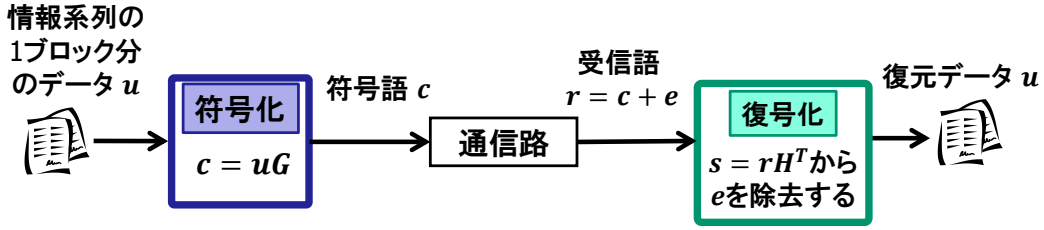
格子関連の問題を利用して IND-CPA 安全性を満たす公開鍵暗号を構成する場合、代表的な構成として、レゲフ方式（Regev [2009]）、リンドナー＝ペイカート方式（Lindner and Peikert [2011]、LP 方式と呼ぶ）、リュバシェフスキー＝ペイカート＝レゲフ方式（Lyubashevsky, Peikert, and Regev [2010]、LPR 方式と呼ぶ）が挙げられる。レゲフ方式は、格子問題（LWE 問題）に基づく初めての公開鍵暗号方式である。また、LP 方式は、LWE 問題に基づく方式であるが、圧縮による鍵サイズ（公開鍵、秘密鍵）の削減を行っており、レゲフ方式よりも鍵サイズが小さいという特長を有する。さらに、LPR 方式は、Ring-LWE 問題を利用することにより、LP 方式よりも鍵サイズ（公開鍵、秘密鍵）を削減している。

（２）誤り訂正符号の復号問題

イ．概要

誤り訂正符号は、ノイズ（雑音）が生じる通信路において高い信頼度で情報を伝達することを目的として、通信路上でノイズによって生じたエラー（誤り）を訂正する技術である。誤り訂正符号を利用した通信において、送信者は、送りたいデータ（情報系列）に符号化と呼ばれる処理を行い、変換したデータ（符号系列）を通信路を介して受信者に送信する。この間、通信路において符号系列にはエラーが生じる。受信者は、エラーのある符号系列に復号化と呼ばれる処理を行うことで、情報系列を復元することができる。代表的な誤り訂正符号である線形符号では、情報系列および符号系列をブロックに区切ったうえで符号化処理および復号化処理を行う（図表 6 を参照）。

図表 6. 線形符号の処理



線形符号では、情報系列の 1 ブロックは有限体上のk次元ベクトル$\boldsymbol{u}$で表現され、符号系列の 1 ブロックはn次元ベクトル$\boldsymbol{c}$（ただし、$k \leq n$）で表現され符号語と呼ばれる。また、符号化の処理は、生成行列と呼ばれる$k \times n$行列Gにより、$\boldsymbol{c} = \boldsymbol{u}G$で表される。さらに、復号化の処理は、パリティ検査行列と呼ばれる$(n-k) \times n$行列Hを利用して行われる。ここで、パリティ検査行列Hは、$\boldsymbol{c}H^{\mathrm{T}} = \boldsymbol{0}$で特徴づけられる行列である。通信路上でのエラーも$n$次元ベクトル$\boldsymbol{e}$で表され、受信者は符号語にエラーが加わった受信語$\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$を受信することになる[26]。このとき、$\boldsymbol{s} = \boldsymbol{r}H^{\mathrm{T}}$を受信語のシンドロームと呼ぶ。復号化処理においては、シンドローム$\boldsymbol{s} = \boldsymbol{r}H^{\mathrm{T}} = \boldsymbol{e}H^{\mathrm{T}}$からエラー$\boldsymbol{e}$を求めそれを除去することで、ベクトル$\boldsymbol{u}$を復元する。

一般に、符号化処理の後、情報系列と符号系列の対応関係がランダムにみえる場合、受信語からもとのデータを復元することは計算困難であることが知られており、誤り訂正符号の復号問題と呼ばれる。具体的には、以下に述べるシンドローム復号問題とその関連問題が知られている。

ロ．シンドローム復号問題と関連問題

シンドローム復号問題（SDP）とは、線形符号のパリティ検査行列と符号語が与えられたとき、その符号語を復号する問題である[27]。一般に、SDP は NP 困難問題である（Berlekamp, McEliece, and van Tilborg [1978]）。また、判定シンドローム復号問題（DSDP）とは、ある線形符号におけるパリティ検査行列とそれから生成される符号語の組と、ランダムに選択した行列と値の組、それぞれの確率分布を識別する判定問題である[28]。DSDP は、SDP と同程度の困難性を有している（Applebaum, Ishai, and Kushilevitz [2009]）。

---

[26] 後の復号化処理でこのエラー$\boldsymbol{e}$が除去可能なためには、$\boldsymbol{e}$はある程度小さなベクトルであるという条件が必要になる。具体的には、$\boldsymbol{e}$の非零成分の個数がある一定数以下であるという条件（ハミング距離による条件）が通常は利用される。また、$\boldsymbol{e}$を行列で表現しその階数（ランク）がある一定数以下であるという条件（ランク距離による条件）もしばしば利用される（Gabidulin [1985]）。

[27] SDP は Syndrome Decoding Problem の略である。

[28] DSDP は Decision Syndrome Decoding Problem の略である。

LPN 問題とは、2 元ベクトル$\boldsymbol{a}$（0 と 1 で構成されるベクトル）と秘密の 2 元ベクトル$\boldsymbol{s}$の内積$\langle \boldsymbol{a}, \boldsymbol{s} \rangle$にエラーの値$\boldsymbol{e}$を足した値が与えられたとき、$\boldsymbol{s}$を求める問題である[29,30]。一般に、$\boldsymbol{a}$がある線形符号の生成行列$\boldsymbol{G}$で生成され、それに$\boldsymbol{e}$ が加わったと考えれば、$\boldsymbol{s}$を求めることは線形符号の復号問題として解釈できる。そのため、2 元ベクトルを用いて符号を生成する線形符号（2 元線形符号）における SDP は LPN 問題に帰着する。

LPN 問題は、もともと機械学習理論において研究されている問題であるが、上記に説明したように線形符号の復号問題と深く関係している[31]。誤り訂正符号の復号問題の文脈では、問題の内容とその簡潔さから SDP が中心に扱われる。

また、ある特別な数学的構造を持った線形符号（以下、構造的線形符号と呼ぶ）を利用した場合の SDP や DSDP は、その構造的線形符号のパラメータを適切に選べば、NP 困難問題と同程度の計算困難問題であると期待されている。

ハ．暗号を構成する仕組みと利用する符号

誤り訂正符号の復号問題をベースに公開鍵暗号を構成する基本的な仕組みは、マクエリス（McEliece [1978]）やニーダライター（Niederreiter [1986]）により提案されている（以下、それぞれを McEliece タイプ、Niederreiter タイプと呼ぶ）。現在、これら 2 つのタイプは暗号化方式における主流の構成法である。McEliece タイプでは生成行列と符号語を基盤に構成するが、Niederreiter タイプではパリティ検査行列とシンドロームを基盤に構成する。両者には構成上の違いがあるものの、SDP および DSDP に利用する符号の種類が同じ場合には、両者の安全性は同程度である（Li, Deng, and Wang [1994]）。ただし、McEliece タイプでは$k \times n$生成行列を利用し、Niederreiter タイプでは$(n-k) \times n$パリティ検査行列を利用するため符号化や復号に必要なデータサイズは異なってくる。例えば、$k > n/2$（kはメッセージのサイズ、nは暗号文のサイズに対応）のとき、Niederreiter タイプの方が公開鍵のサイズを削減できることになる。現在、NIST に提出されている誤り訂正符号の復号問題をベースにした公開鍵暗号または KEM は、本質的に上記のいずれかのタイプの構成法に基づいている。

また、SDP または DSDP に利用される線形符号としては、ゴッパ（Goppa）符号、Quasi-Cyclic 符号、Rank Quasi-Cyclic 符号、Low Density Parity-Check 符号（LDPC 符号）、Moderate Density Parity-Check 符号（MDPC 符号）、Low Rank Parity

---

[29] LPN は Learning Parity with Noise の略である。

[30] ベルヌーイ分布と呼ばれる確率分布に基づいて$\boldsymbol{e}$を選ぶ。ベルヌーイ分布とは、1 ビットの値に対して、確率p $(0 < p < 1)$で 1 を、確率$1-p$で 0 をとる確率分布である。

[31] 機械学習理論とは、データベース等から、ある数のサンプルデータ集合を入力して解析を行い、そのデータから有用な規則、知識表現、判断基準等を抽出し、アルゴリズムを発展させることを目的とする理論計算機科学の学問領域である。

Check 符号（LRPC 符号)、あるいはこれら符号の性質を組み合わせた符号（例えば、Quasi-Cyclic Goppa 符号等）が考えられる（図表 7 を参照)。NIST に提出された方式においても、これらの線形符号が利用されている。

これまでは Goppa 符号を利用するのがが主流であったが、Goppa 符号を利用する場合には、鍵サイズ（公開鍵、秘密鍵）が大きくなることが課題とされている。この課題を解決するため、Goppa 符号よりも、生成行列やパリティ検査行列のサイズが小さくて済む構造的線形符号を利用する方式が提案されている。具体的には、例えば、行列の一部があるベクトルの成分を 1 つずつシフトする規則によって作られる Quasi-Cyclic 符号を利用する方式がある。Quasi-Cyclic 符号は、行列成分すべてではなく一部の成分とその規則だけを記憶することにより、生成行列やパリティ検査行列を圧縮することができ、この特徴を持つ線形符号に基づいた McEliece タイプや Niederreiter タイプの方式では鍵サイズの削減が可能となる（Aguilar-Melchor *et al.* [2018]等)。もっとも、符号化と復号化に必要な行列のサイズの削減度合いは、利用する誤り訂正符号の性質により異なることに注意を要する。

図表 7. 利用する線形符号と暗号構成における特徴

名称	説明	暗号構成に及ぼす影響
Goppa 符号	有限体上の代数曲線を使って構築される線形符号の一種	これまで、誤り訂正符号の復号問題に基づく公開鍵暗号の構成によく用いられてきた。効率的に復号可能であるが、鍵サイズ（公開鍵、秘密鍵）が大きいことが課題。
Quasi-Cyclic 符号	生成行列やパリティ検査行列の一部が、あるベクトルの成分を 1 つずつシフトする規則によって作られている線形符号	生成行列やパリティ検査行列の行列成分すべてではなく、一部の成分とその規則だけを記憶することにより、対象の行列を圧縮し、鍵サイズ（公開鍵、秘密鍵）を削減可能。
Rank Quasi-Cyclic 符号	Quasi-Cyclic 符号においてハミング距離ではなく、ランク距離を導入した線形符号	Quasi-Cyclic 符号と同様に鍵サイズを削減可能。一般に、ランク距離による線形符号は、ハミング距離による線形符号に比べて計算時間の少ない復号を設計することは難しいが、復号エラーを抑えたり既存の攻撃法を適用困難にさせる特徴をもつ。
LDPC 符号	パリティ検査行列がランダムな疎行列（成分に 0 が多い行列）である線形符号	線形符号として効率的な復号化が可能なため、暗号文の復号も効率的となる特徴をもつ。ただし、ある種のパラメータ選択に対しては安全性の面で脆弱であることが指摘されている。
MDPC 符号	LDPC 符号に比べ、パリティ検査行列の非零成分を増やした形の行列を利用する線形符号	LDPC 符号の疎行列の利用を避けることで、安全性に影響する脆弱なパラメータの選択が起こらないようにしているが、復号の効率性は LDPC 符号を利用する場合に比べ劣る。
LRPC 符号	LDPC 符号においてハミング距離ではなく、ランク距離を導入した線形符号	上記の LDPC 符号とランク距離を利用する利点を活かすことを目的に考案された。これにより復号処理の計算時間と安全性の面でバランスをとった構成と考えられる。

（３）多変数連立方程式の求解問題

一般に、複数の「多変数多項式=0」として構成される連立方程式を解く問題は計算困難であり、多変数 2 次多項式に制限した連立方程式であっても NP 困難であることが知られている。したがって、多変数連立方程式の求解問題に基づく公開鍵暗号方式やデジタル署名方式においては、利用する連立方程式の求解問題が計算困難になるように多変数多項式（特に、多変数 2 次多項式）を構成する必要がある。

この仕組みにより公開鍵暗号やデジタル署名を構成する研究は、松本＝今井による構成法（Matsumoto and Imai [1988]）から始まった。その後、多変数多項式を構成する方法について多くの改良がなされ、現在の有力な構成法としては、HFE（Hidden Field Equation）手法（Patarin [1996]）と Oil & Vinegar 手法（Kipnis, Patarin, and Goubin [1999]）が知られている。HFE 手法は、複数の多変数多項式を合成する手法であり、合成の際に特殊な演算処理を行うことにより、合成後の多変数多項式からもとの多変数多項式を求めることを困難にする。ここで、合成後の多変数多項式は公開鍵に対応し、もとの多変数多項式が秘密鍵に対応する。また、Oil&Vinegar 手法は、複数の変数が従属関係となる多項式と独立関係となる多項式が混在するように多変数多項式を生成する方法である。一般に、連立方程式を解く手法として XL アルゴリズム（Courtois *et al*. [2000]）やグレブナ基底による解法（Faugére [1999, 2002]等）が知られており、これらの解法により効率的に解かれないようにパラメータを選択することが必要である[32,33]。

（４）その他の問題

上記に説明した計算問題のほか、量子コンピュータでも計算困難な問題として、メルセンヌ低ハミング組合せ探索問題、同種写像探索問題、共通鍵暗号・ハッシュ関数に関わる問題等が挙げられる（図表 8 を参照）。

---

[32] XL アルゴリズムは、Extended Linearization（eXtended Linearization）アルゴリズムの略であり、変数の積を 1 つの変数とみなし、連立 1 次方程式に変換してガウスの消去法等により効率的に解くアルゴリズムである。ただし、XL アルゴリズムを適用するには、ある種の条件が必要になる。

[33] グレブナ基底は、共通解を持つ方程式の集合の中で解きやすい形をしている方程式の集合である。与えられた多変数連立方程式を解くとき、事前にグレブナ基底を求めることにより、解を効率よく求めることができるため、どのような多変数連立方程式の求解問題の解法としても利用できるが、一般にその計算量は理論的には 2 重指数関数時間（例えば、$y = 2^{2^x}$のように、指数関数における指数がさらに指数関数で表される計算量）である。しかし、多くの入力値（多変数連立方程式）に対して現実的な時間内に解を導出できると報告されている。

図表 8. その他の問題

問題の名称	内容
メルセンヌ低ハミング組合せ探索問題	整数をメルセンヌ素数[34]で割った余りを要素とする集合（有限体）において、秘密値とランダム値の積にノイズを加えた値から、もとの秘密値を探索する問題
同種写像探索問題	2 つの楕円曲線の点同士の対応関係（同種写像）を探索する問題
多変数不定方程式の求解問題	単一の多変数高次方程式の解を求める問題
ブレイド群と有限体の関係探索問題	複数存在する点同士のつながり方を要素とする集合（ブレイド群）と、整数をある素数で割った余りを要素とする集合（有限体）の間にある関係性（写像とその逆写像）を探索する問題
共通鍵暗号・ハッシュ関数に関わる問題	量子コンピュータに対する共通鍵暗号の解読問題、ハッシュ関数の衝突探索問題[35]
ランダムウォーク問題	ある空間上の点に対するランダムウォークを複数回繰り返した後、その点が存在する位置を探索する問題

４．米国における標準化動向

（１）標準化のプロセスと評価項目

米国政府は、量子コンピュータでも解読できない暗号技術の米国政府標準暗号を、今後、数年かけて決定する計画である。NIST は、2017 年 11 月末を期限に全世界から標準化候補の方式を募集し、最初の選考過程（第 1 ラウンド）を経て、2019 年 1 月末に、次の選考過程（第 2 ラウンド）に進む方式を公表した（National Institute of Standards and Technology [2019]）。NIST の最終選考過程を通過した方式は[36]、米国政府標準暗号に選定され、標準化ドラフトが作成される計画である。第 2 ラウンドの選考には、1 年から 1 年半を要することが想定されており、米国政府標準暗号の選定は、最初の募集から 3 年から 5 年をかけて行われる計画になっている。

第 1 ラウンドおよび第 2 ラウンドでは、公開鍵暗号、KEM、デジタル署名の各区分ごとに、各種方式のアルゴリズムと、それらの方式が満たすと主張する安全性レベルや効率性が評価される。特に、安全性レベルとしては、公開鍵暗号や KEM であれば IND-CPA 安全性または IND-CCA 安全性のいずれかが要求され、デジタル署名であれば UF-CMA 安全性以上の安全性レベルが要求される（2 節参照）[37]。また、効率性の評価は、ソフトウェア実装またはハードウェア実装したものについて、各種方式に必要なアルゴリズムの計算時間や、データサイズの観点から行われる。特に、公開鍵暗号や KEM であれば、鍵生成・暗号化・

[34] メルセンヌ素数とは、$p = 2^n - 1$（nは自然数）の形をした素数のことである。
[35] 同じハッシュ値となる異なる入力値を探索する計算問題。
[36] 必要があれば、3 度目の選考過程（第 3 ラウンド）を設けることも想定されている。
[37] ただし、公募にあたり、方式の提出者は、自らの提案方式が主張する安全性レベルを充足することの証明を付すことは求められていない。

復号のアルゴリズム実行に必要な計算時間、公開鍵（暗号化鍵）・秘密鍵（復号鍵）のサイズ、暗号文のサイズが評価項目として挙げられている[38]。また、デジタル署名においては、鍵生成・署名生成・署名検証アルゴリズム実行に必要な計算時間、公開鍵（署名検証鍵）・秘密鍵（署名生成鍵）のサイズ、署名のサイズが評価される[39]。

2017 年 11 月末までに提出された各種方式のうち、応募要件を満たしたのは 69 方式であり、このうち、公開鍵暗号または KEM が 47 方式、デジタル署名が 22 方式であった。その後、第 1 ラウンドにおいて、2 つの方式が 1 つに統合され、5 方式が取下げになった。また、第 2 ラウンドへ移行する方式は全体で 26 方式であり、公開鍵暗号または KEM が 17 方式、デジタル署名が 9 方式である。

以下では、第 1 ラウンドにおいて選考対象であった方式の特徴について解説する。ただし、応募案件 69 方式のうち、第 1 ラウンドにおいて、既に安全性に関する脆弱性の指摘等により取下げになった方式 5 方式は対象外とする。

（２）公開鍵暗号単独にかかる各種方式

公開鍵暗号単独で提案している方式は、Compact LWE、McNie、LEDApkc、Giophantus、PostQuantum RSA、Guess Again である（図表 9 参照）。なお、図表９中の一番右の列は、各種方式が第 2 ラウンドに進んだか否かを示している。

Compact LWE は、秘密鍵サイズや暗号文サイズを小さくできるように LWE 問題を少し変形して利用しており、IND-CCA 安全性を満たすと主張されている。

McNie、LEDApkc は、誤り訂正符号（構造的線形符号）の復号問題を利用して構成されており、IND-CCA 安全性を満たすと主張されている。このうち、LEDApkc は、Quasi-Cyclic LDPC 符号（QC-LDPC 符号）を利用することで秘密鍵サイズを減らし、復号が効率的になるように設計されており、他方、McNie は、Quasi-Cyclic LRPC 符号（QC-LRPC 符号）を利用することで、鍵サイズを小さくすると共に暗号文サイズも小さくしている。LEDApkc は、McEliece タイプに基づいて OW-CPA 安全性を満たすように構成されているのに対し、McNie は、McEliece タイプと Niederreiter タイプの両方を組み合わせて OW-CPA 安全性を満

[38] 公開鍵サイズは、暗号化処理において最低限必要なメモリの目安になり、またサイズが小さいほど暗号化処理時間が短くなる傾向にある。同様に、秘密鍵サイズは、復号処理において最低限必要なメモリの目安になり、またサイズが小さいほど復号時間が短くなる傾向にある。さらに、暗号文は通信路を介して送受信されるため、暗号文サイズが小さいほど通信路に流れるデータ量を削減できる。

[39] 公開鍵サイズは、署名検証において最低限必要なメモリの目安になり、またサイズが小さいほど署名検証時間が短くなる傾向にある。同様に、秘密鍵サイズは、署名生成において最低限必要なメモリの目安になり、またサイズが小さいほど署名生成時間が短くなる傾向にある。さらに、署名は通信路を介して送受信されるため、署名サイズが小さいほど通信路に流れるデータ量を削減できる。

図表 9. 公開鍵暗号の各種方式

	方式名	提出した組織（代表）	利用する計算問題	安全性	第 2 ラウンド
格子系	Compact LWE	Commonwealth Scientific and Industrial Research Organisation (CSIRO)	LWE 問題	IND-CCA	－
符号系	McNie	Sogang University	QC-LRPC 符号の SDP	IND-CCA	－
	LEDApkc	Università Politecnica Delle Marche	QC-LDPC 符号の SDP	IND-CCA	LEDAkem,LEDApkc を統合した LEDAcrypt が候補
その他	Giophantus	東芝	高次不定方程式の求解問題	IND-CCA	－
	PostQuantum RSA	University of Illinois at Chicago	素因数分解問題	IND-CCA	－
	Guess Again	The City College of NewYork	ランダムウォーク問題	IND-CCA	－

たすように構成されている。これらの 2 方式は、古原＝今井による変換手法（Kobara and Imai [2001]）を適用し、ランダムオラクルモデルにおいて IND-CCA 安全性を満たす構成となっている[40]。

また、Giophantus は、単一の多変数高次方程式の求解問題を利用して公開鍵暗号を構成しており、秘密鍵サイズは比較的小さいが暗号文サイズが比較的大きいという特徴をもつ。Giophantus は、IND-CPA 安全性を満たすと主張されている。またこの構成に FO 変換を適用して IND-CCA 安全性を満たす方式が構成できることが述べられている。

PostQuantum RSA は、量子アルゴリズムでも現実的な時間で解読できない、桁数が大きく多くの素数の積で表される素因数分解問題を利用して構成されている。その結果、鍵サイズ（公開鍵、秘密鍵）や暗号文サイズは比較的大きくなる。PostQuantum RSA は、IND-CCA 安全性を満たすと主張されている。

Guess Again は、ランダムウォーク問題を利用して構成されており、その問題に用いるパラメータの影響から暗号文サイズが比較的大きくなっている。Guess Again は、IND-CCA 安全性を満たすと主張されている。

（3）KEM にかかる各種方式

図表 10 は、NIST に、KEM 方式として提出され、第 1 ラウンドにおいて選考対象であった方式を整理している。なお、図表 10 中の一番右の列は、各種方式

[40] 2 節(3)で説明した汎用的な変換法（FO 変換等）と異なり、古原＝今井による変換法は McEliece タイプの構成に対してだけ適用できる変換法であるが、変換後の暗号文サイズをより小さくできる利点がある。

図表 10. KEM の各種方式

	方式名	提出した組織(代表)	利用する計算問題	安全性	第 2 ラウンド
格子系	FrodoKEM	University of Michigan	LWE 問題	IND-CCA	候補
	Ding Key Exchange	University of Cincinnati	Ring-LWE 問題	IND-CPA	－
	NewHope	Infineon Technologies		IND-CCA	候補
	EMBLEM/ R. EMBLEM	Korea University	LWE 問題/ Ring-LWE 問題	IND-CCA	－
	CRYSTALS-KYBER	Radboud University	Module-LWE 問題	IND-CCA	候補
	Three Bears	Rambus 社		IND-CCA	候補
	Saber	KU Leuven	Module-LWR 問題	IND-CCA	候補
	NTRU-HRSS-KEM	University of Waterloo	最短ベクトル問題 (SVP)	IND-CCA	NTRUEncrypt,NTRU-HRSS-KEM を統合した NTRU が候補
	NTRU prime	TU Eindhoven		IND-CCA	候補
符号系	Classic McElice	TU Eindhoven	Goppa 符号の SDP	IND-CCA	候補
	LAKE/LOCKER	University of Limoges	LRPC 符号の SDP	IND-CPA	LAKE,LOCKER,Ouroboros-R を統合した ROLLO が候補
	Big Quake	INRIA	Quasi-Cyclic Goppa 符号の SDP	IND-CCA	－
	NTS-KEM	PQ Solutions 社		IND-CCA	候補
	BIKE	Intel 社	QC-MDPC 符号の SDP	IND-CPA	候補
	QC-MDPC KEM	ISARA 社		IND-CCA	－
	LEDAkem	Università Politecnica Delle Marche	QC-LDPC 符号の SDP	IND-CCA	LEDAkem,LEDApkc を統合した LEDAcrypt が候補
	RLCE-KEM	University of North Carolina at Charlotte	線形符号の SDP	IND-CCA	－
	RQC	University of Limoges	Rank Quasi-Cyclic 符号の SDP	IND-CCA	候補
	Ouroboros-R	University of Limoges		IND-CPA	LAKE,LOCKER,Ouroboros-R を統合した ROLLO が候補
	HQC	University of Limoges	Quasi-Cyclic 符号の SDP	IND-CCA	候補
	Lepton	Shanghai Jiao Tong University	LPN 問題	IND-CCA	－
	DAGS	Florida Atlantic University	QD-GS 符号の SDP	IND-CCA	－
連立方程式系	DME	Universidad Computense de Madrid	HFE 手法で構成された多変数連立方程式の求解問題	IND-CPA	－
	CFPKM	Sorbonne Université	ノイズ付き非線形連立方程式の求解問題	IND-CPA	－
その他	Mersenne-756839	Sorbonne Université	メルセンヌ低ハミング組合せ探索問題	IND-CCA	－
	Ramstake	KU Leuven		IND-CCA	－

が第 2 ラウンドに進んだか否かを示している。

イ．格子関連の計算問題を利用した方式

格子関連の計算問題を利用している方式は、FrodoKEM、Ding Key Exchange、NewHope、EMBLEM/R.EMBLEM、CRYSTALS-KYBER、Three Bears、Saber、

NTRU-HRSS-KEM、NTRU Prime である。これらの方式の安全性レベルについては、それぞれの提案者により、Ding Key Exchange は IND-CPA 安全性を満たし、他の方式は IND-CCA 安全性を満たすと主張されている。また、安全性の根拠となる計算問題として、FrodoKEM と EMBLEM は標準的な LWE 問題、Ding Key Exchange、NewHope、R.EMBLEM は Ring-LWE 問題、CRYSTALS-KYBER、Three Bears は Module-LWE 問題[41]、Saber は Module-LWR 問題、NTRU-HRSS-KEM と NTRU Prime は SVP をそれぞれ利用している。

FrodoKEM は、公開鍵暗号である LP 方式の考え方を取り入れながら、LWE 問題を利用した Bos らの鍵配送方式（Bos *et al*. [2016]）を基盤にして、KEM を構成している。この方式は LWE 問題の困難性を基盤としていることから、効率性よりも安全性を重視した設計になっている一方で、格子を構成するための行列の生成法を工夫することで公開鍵サイズを削減している。

Ding Key Exchange は、Ring-LWE 問題を基盤とする鍵配送方式であり、KEM としても表現可能である。この方式では、送受信者間での共有鍵の一致確率を高めるための reconciliation 技術（Ding, Xie, and Lin [2012]）が用いられている[42]。

NewHope は、LPR 方式とアルキム（Alkim）らの方式（Alkim *et al*. [2016]）を組み合わせ、さらに暗号文サイズの削減技術（Pöppelmann and Güneysu [2013]）を利用した方式である。

EMBLEM は、LP 方式に復号エラーを小さくするための工夫を施し、LWE 問題に基づいて IND-CPA 安全性を満たす公開鍵暗号を構成した後、HHK 変換により IND-CCA 安全性を満たす KEM を構成している。また、LWE 問題の代わりに Ring-LWE 問題を利用して同じように構成した方式が R.EMBLEM である。

CRYSTALS-KYBER は、Ring-LWE 問題を利用して構成されていた LPR 方式において、Ring-LWE 問題の代わりに Module-LWE 問題を利用した方式であり、パラメータの選択により効率性と安全性のどちらを重視するかを選択可能な方式である。

Three Bears は、Ring-LWE 問題を利用して構成されていた LPR 方式において、Ring-LWE 問題の代わりに Module-LWE 問題を利用しており、CRYSTALS-KYBER と同様、パラメータの選択により効率性と安全性のどちらを重視するかを選択可能な方式である[43]。

また、NTRU-HRSS-KEM は NTRU 方式を高速な KEM に改良した方式である

[41] 正確には、CRYSTALS-KYBER は多項式で表現された格子の Module-LWE 問題、Three Bears は一般メルセンヌ素数で割った剰余の集合における Module-LWE 問題（Integer Module-LWE 問題）である。

[42] 鍵配送方式や KEM において、送受信者間で共有されるべき鍵が不一致となる確率を小さくする技術である。

[43] 正確には、Three Bears では Integer-Module-LWE 問題を利用する。

（Hülsing *et al*. [2017]）。NTRU Prime は、NTRU 方式に対して、既存の攻撃法が適用されないように、格子を定義する多項式の選択方法に改良を加えた方式である。

FrodoKEM 、 NewHope 、 CRYSTALS-KYBER 、 Three Bears 、 Saber 、 NTRU-HRSS-KEM は、OW-CPA 安全性（または IND-CPA 安全性）を満たす方式を構成した後、デント変換または HHK 変換を適用して、（量子）ランダムオラクルモデルにおいて IND-CCA 安全性を満たす方式を構成している。さらに、格子関連の計算問題を利用する多くの方式では、（多項式同士の）乗算に NTT 法（Number Theoretic Transform）を利用し、鍵生成、暗号化、復号等の処理の高速化を実現している（例えば、CRYSTALS-KYBER、NewHope 等）[44]。

上記のうち、秘密鍵サイズが比較的小さいのは Three Bears であり、公開鍵サイズおよび暗号文サイズが比較的小さいのは NewHope、CRYSTALS-KYBER、Three Bears、Saber、NTRU-HRSS-KEM である。

ロ．誤り訂正符号の復号問題を利用した方式

誤り訂正符号の復号問題を利用した方式は、Classic McElice、LAKE/LOCKER、Big Quake、NTS-KEM、BIKE、QC-MDPC KEM、LEDAkem、RLCE-KEM、RQC、Ouroboros-R、HQC、Lepton、DAGS である。これらの方式は、McEliece タイプや Niederreiter タイプ（あるいはそれらの変形版）の構成法に基づいており、計算問題として SDP や DSDP の困難性を仮定している。ただし、SDP や DSDP における符号の種類を制限することで、鍵サイズを削減する方式も多くみられる。

従来、Goppa 符号が利用されてきたが、近年、効率性（鍵サイズや暗号文サイズの削減）を向上させることを目的として、構造的線形符号を利用する研究も多く行われている。しかし、構造的線形符号が有する特徴を利用した攻撃がこれまで多く提案されてきたことから（Aguilar-Melchor *et al*. [2018]等）、安全性を確保するためには攻撃に利用されうる特徴を有さない構造的線形符号を利用する必要がある。この点、NIST の応募に提出されている各種方式をみると、安全性を重視して構造的線形符号に制限しない方式や、効率性を重視して特定の構造的線形符号に制限する方式などさまざまなものがあり、方式の構成から提案者の設計思想が伺える。

利用されている誤り訂正符号については、Classic McElice は従来からの Goppa 符号、HQC は Quasi-Cyclic 符号、RQC は Rank Quasi-Cyclic 符号、Big Quake は

[44] 現在、一般的な乗算アルゴリズム（2 次の多項式オーダのアルゴリズム）よりも高速な乗算アルゴリズムとして、FFT 法（高速フーリエ変換法＜Fast Fourier Transform＞）、Karatsuba 法、Toom-Cook 法などが知られている。NTT は有限体上の乗算（したがって、有限体上の多項式の乗算）に適用可能な FFT 法のことである。

Quasi-Cyclic Goppa 符号、LEDAkem は QC-LDPC 符号、QC-MDPC KEM は Quasi-Cyclic MDPC 符号（QC-MDPC 符号）、DAGS は Quasi-dyadic generalized Srivastava 符号（QD-GS 符号）をそれぞれ使用している。また、Classic McElice、HQC、RQC、Big Quake、QC-MDPC KEM、DAGS は、OW-CPA 安全性（または IND-CPA 安全性）を満たす方式を直接的に構成した後、FO 変換、デント変換、TU 変換、あるいは HHK 変換を適用して、（量子）ランダムオラクルモデルにおいて IND-CCA 安全性を満たす方式を構成している。

ハ．その他の問題を利用した方式

連立方程式の求解問題を利用した方式は、DME と CFPKM である。DME は HFE 手法で構成された多変数連立方程式の求解問題を利用して KEM を構成している。また、CFPKM は、多変数多項式にノイズを付加した式を複数生成し、非線形連立方程式に対しての求解問題に基づいて KEM を構成している。CFPKM は、このようなノイズを利用した構成にすることで秘密鍵サイズを小さくしている。

Mersenne-756839（Aggarwal *et al*. [2018]）は、メルセンヌ素数による整数の剰余環において、ノイズ（またはエラー）を加えて暗号化する仕組みを利用した方式である[45]。また、Ramstake は、メルセンヌ素数による整数の剰余環において、ノイズが加わった場合の Diffie-Hellman 鍵配送方式の仕組みを利用する方式である。また、仮定する計算問題の困難性として、Mersenne-756839 はメルセンヌ低ハミング組合せ探索問題の計算困難性を、Ramstake はこの問題の Diffie-Hellman 版の計算困難性を仮定している[46]。

（４）公開鍵暗号および KEM の両方を提案する各種方式

図表 11 は、公開鍵暗号および KEM の両方を提案している方式を整理している。なお、図表 11 中の一番右の列は、各種方式が第 2 ラウンドに進んだか否かを示している。

公開鍵暗号および KEM の両方を構成する方式のうち、SIKE 以外は、格子関連の計算問題を利用している。SIKE 以外の方式は、格子関連の計算問題を利用して IND-CPA 安全性を満たす公開鍵暗号または KEM を構成し、IND-CCA 安全性を達成するために FO 変換、TU 変換、デント変換、HHK 変換のいずれかを適用して、（量子）ランダムオラクルモデルにおいて安全な方式を構成している。

---

[45] Mersenne-756839 方式では、メルセンヌ素数$p = 2^n - 1$として$n = 756839$を設定しており、このことが方式名になっている。

[46] 各ユーザ$i(\mathrm{i} = 1,2)$は、自身の秘密値x_i, y_iと公開されたランダム値Gから、$F_i = x_i G + y_i$を計算し他者に送る。ユーザ 1 は$x_1 F_2$を計算して近似し、ユーザ 2 は$x_2 F_1$を計算して近似することで、各ユーザはそれぞれ$x_1 x_2 G$を共有する仕組みのことである。

図表 11. 公開鍵暗号&KEM の各種方式

	方式名	提出した組織（代表）	利用する計算問題	安全性	第 2 ラウンド
格子系	LOTUS	情報通信研究機構	LWE 問題	IND-CCA（KEM） IND-CCA（PKE）	－
	Lizard	Seoul National University	LWE 問題, LWR 問題 Ring-LWE 問題，もしくは Ring-LWR 問題	IND-CCA（KEM） IND-CPA（PKE）	－
	LIMA	KU Leuven	Ring-LWE 問題	IND-CCA（KEM） IND-CCA（PKE）	－
	KINDI	TU Darmstadt	Module-LWE 問題	IND-CCA（KEM） IND-CPA（PKE）	－
	OKCN/AKCN/CNKE	Fudan University	LWE 問題, Ring-LWE 問題, Module-LWE 問題, もしくは LWR 問題	IND-CCA（KEM） IND-CCA（PKE）	－
	Round5	Philips 社, HILA5 Project Team	Module-LWR 問題	IND-CPA（KEM） IND-CCA（PKE）	候補
	NTRU Encrypt	Onboard Security 社	最短ベクトル問題 (SVP)	IND-CCA（KEM） IND-CCA（PKE）	NTRUEncrypt,NTRU-HRSS-KEM を統合した NTRU が候補
	Odd Manhattan	University of Wollongong	BDD 問題	IND-CCA（KEM） IND-CCA（PKE）	－
	LAC	Chinese Academy of Science	Ring-LWE 問題	IND-CCA（KEM） IND-CPA（PKE）	候補
	Titanium	Monash University	LWE 問題	IND-CCA（KEM） IND-CPA（PKE）	－
その他	SIKE	University of Waterloo	同種写像探索問題	IND-CCA（KEM） IND-CPA（PKE）	候補

LOTUS では、青野らの代理人再暗号化方式（Aono *et al*. [2013]）から代理人再暗号化機能を取り除くことで、IND-CPA 安全性を満たす公開鍵暗号を構成している[47]。これは、LP 方式の構成を参考にしている。そして、IND-CCA 安全性を実現するにあたっては FO 変換を適用している。LOTUS における KEM は、LOTUS における公開鍵暗号の平文を乱数に置き換えた方式である。

Lizard は、レゲフ方式の考え方を参考に LWE 問題または LWR 問題を利用して IND-CPA 安全性を満たす公開鍵暗号を構成したうえで（Cheon *et al*. [2016, 2018]）HHK 変換を適用し IND-CCA 安全な KEM を構成している。また、Ring-LWE 問題および Ring-LWR 問題を利用した同様な方式も提案に含まれている。

LIMA は、アルブレヒト（Albrecht）らの方式（Albrecht *et al*. [2017]）に基づいて IND-CPA 安全性を満たす公開鍵暗号および KEM を構成している。また、これらから FO 変換を適用して IND-CCA 安全性を満たす公開鍵暗号を構成し、デント変換を適用して IND-CCA 安全性を満たす KEM を構成している。

KINDI は、エルバンサハニ（El Bansarkhani）による方式（El Bansarkhani [2017]、

[47] 代理人再暗号化方式は、高機能暗号の一種で、暗号文の状態のままで正規の受信者を変更できる機能を持った公開鍵暗号の方式である。

El Bansarkhani, Dagdelen, and Buchmann [2014]）に基づいて IND-CPA 安全性を満たす公開鍵暗号を構成して、これに HHK 変換を適用し、IND-CCA 安全性を満たす KEM を構成している。

OKCN/AKCN/CNKE は、従来の LWE 問題や Ring-LWE 問題に特化した reconciliation 技術を一般的に拡張しパラメータ設定に幅を持たせることで、さまざまな格子問題（LWE 問題, Ring-LWE 問題, Module-LWE 問題, または LWR 問題）を安全性の根拠として利用できるように設計されている（Jin and Zhao [2017]）。

Round5 は、Round2 と Hila5 を統合して新たに提出されている[48]。Round5 は、Module-LWR 問題を利用することで、LWR 問題や Ring-LWR 問題において幅広くパラメータを選択できるように設計されている（Saarinen [2017]）。また、IND-CPA 安全性を満たす公開鍵暗号として構成されており、これに FO 変換を適用することにより IND-CCA 安全性を満たす公開鍵暗号として構成されている。

NTRU Encrypt は、NTRU 方式に対して、既存の攻撃法が適用されないように改良した方式である[49]。

Odd Manhattan は、BDD 問題に基づいて OW-CPA 安全性を満たす公開鍵暗号を構成しているが、特別な数学的構造を有さない格子を利用するため、鍵サイズ（公開鍵、秘密鍵）や暗号文サイズが比較的大きいという特徴がある。また、これにデント変換を適用して、IND-CCA 安全性を満たす KEM を構成している。

LAC は、LP 方式に基づくものであるが、計算問題としては Ring-LWE 問題を利用して、比較的小さなモジュラス q を選ぶことで、鍵サイズ（公開鍵、秘密鍵）や暗号文サイズの削減を目指した IND-CPA 安全性を満たす公開鍵暗号を構成している。また、これに HHK 変換を適用して、IND-CCA 安全性を満たす KEM を構成している。

Titanium は、レゲフ方式に基づくものであるが、ロスカ（Roşca）ら（Roşca *et al.* [2017]）による多項式演算による LWE 問題を利用して、IND-CPA 安全性を満たす公開鍵暗号を構成しており、秘密鍵サイズが小さいという特徴がある。また、これに HHK 変換を適用し、IND-CCA 安全性を満たす KEM を構成している。

SIKE は、楕円曲線の同種写像探索問題を利用して構成されている。格子系の問題を利用した構成に比べて、暗号化等の計算時間が大きいものの、鍵サイズ

[48] Mudule-LWR 問題を利用した方式 Round2 に、Ring-LWE 問題に対する Hila5 の reconciliation 技術をうまく組み込むことにより、Round5 では復号エラーが更に改善している。

[49] NTRU 方式は、ホフスタイン（Hoffstein）、ピファー（Pipher）、シルバーマン（Silverman）によって提案された公開鍵暗号である（Hoffstein, Pipher, and Silverman [1998]）。NTRU 方式は、特殊な構造を有する格子（NTRU 格子とも呼ばれる）を利用するため、既にいくつかの攻撃が指摘されている（Coppersmith and Shamir [1997]等）。NTRU 方式は格子点探索問題（SVP）を安全性の根拠としているが、方式の安全性と格子点探索問題の難しさが同程度であるかについては知られていない。

（公開鍵、秘密鍵）や暗号文サイズが短いという特徴を有する。

上記の方式の中で、秘密鍵サイズが比較的小さいのは Titanium、Lizard 、Round5、SIKE であり、公開鍵サイズや暗号文サイズが比較的小さいのは LAC、KINDI、NTRU Encrypt、SIKE である。

（５）デジタル署名にかかる各種方式

図表 12 は、NIST に提出され第 1 ラウンドにおいて選考対象であったデジタル署名方式を整理している。なお、図表 12 中の一番右の列は、各種方式が第 2 ラウンドに進んだか否かを示している。

格子関連の計算問題を利用している方式は、qTESLA、CRYSTALS-DILITHIUM、FALCON、pqNTRUsign、DRS の 5 方式である。これらの方式が利用する計算問題はすべて異なっており、qTESLA は Ring-LWE 問題、CRYSTALS-DILITHIUM は Module-LWE 問題、FALCON は SIS 問題、pqNTRUsign は SVP、DRS は BDD 問題を利用している。想定する安全性レベルは、CRYSTALS-DILITHIUM だけが SUF-CMA 安全性であり、その他はすべて UF-CMA 安全性である。この中で、

図表 12. デジタル署名の各種方式

	方式名	提出した組織（代表）	利用する計算問題	安全性	第 2 ラウンド
格子系	qTESLA	qTesla Team	Ring-LWE 問題	UF-CMA	候補
	CRYSTALS-DILITHIUM	IBM 社	Module-LWE 問題	SUF-CMA	候補
	FALCON	Thales Communication & Security 社	SIS 問題	UF-CMA	候補
	pqNTRUsign	Onboard Security 社	SVP	UF-CMA	－
	DRS	University of Wollongong	BDD 問題	UF-CMA	－
符号系	pqsigRM	Seoul National University	Modified Reed-Muller 符号の SDP	UF-CMA	－
	RaCoSS	KDDI 社	ランダム線形符号の SDP	SUF-CMA	－
ハッシュ関数系	Gravity-SPHINCS	Ecole Polytechnique Federale de Lausannel	SHA-256 の衝突探索問題	UF-CMA	－
	SPHINCS+	TU Eindhoven		UF-CMA	候補
連立方程式系	GeMMS	Sorbonne Université - LIP6	HFE 手法で構成された多変数連立方程式の求解問題	UF-CMA	候補
	Gui	Universite de Versailles		UF-CMA	－
	DME	Universidad Complutense de Madrid		UF-CMA	－
	DualModeMS	Sorbonne Université		UF-CMA	－
	LUOV	KU Leuven	Oil&Vinegar 手法で構成された多変数連立方程式の求解問題	UF-CMA	候補
	Rainbow	University of Cincinnati		UF-CMA	候補
	MQDSS	Radboud University		UF-CMA	候補
	HiMQ-3	National Institute for Mathematical Sciences	HFE 手法と Oil&Vinegar 手法の組合せで構成された多変数連立方程式の求解問題	UF-CMA	－
その他	WalnutDSA	SecureRF 社	ブレイド群と有限体の関係探索問題	UF-CMA	－
	Post-Quantum RSA Signature	University of Illinois at Chicago	素因数分解問題	UF-CMA	－
	Picnic	Microsoft 社	共通鍵暗号の解読問題	SUF-CMA	候補

秘密鍵サイズが比較的小さいのは pqNTRUsign、qTESLA であり、公開鍵サイズが比較的小さいのは CRYSTALS-DILITHIUM、FALCON であり、署名サイズが比較的小さいのは FALCON である。

誤り訂正符号の復号問題を利用して構成されている方式は、pqsigRM と RaCoSS である。安全性については、ともに SDP の困難性を利用しており、pqsigRM は UF-CMA 安全性を、RaCoSS は SUF-CMA 安全性を満たすことが提案者により主張されている。SDP に用いられる誤り訂正符号は、pqsigRM は Modified Reed-Muller 符号、RaCoSS はランダム線形符号である[50]。これらの方式では、秘密鍵サイズや署名サイズが比較的大きいという特徴がある。

ハッシュ関数ベースで構成されている方式は、Gravity-SPHINCS, SPHINCS＋の 2 方式であり、いずれも UF-CMA 安全性を満たすと提案者により主張されている。これらは、他の方式のような四則演算を用いた演算処理（整数、行列、多項式の乗算等）に依拠しておらず、ハッシュ関数の計算を中心とした効率的な構成が可能になっている。Gravity-SPHINCS は、公開鍵サイズは小さいが秘密鍵サイズが比較的大きい、また SPHINCS＋は秘密鍵と公開鍵のサイズは小さいが、署名サイズは大きいという特徴を有する。

多変数連立方程式の求解問題を利用して構成している方式は、GeMSS、Gui、DME、DualModeMS、 LUOV、Rainbow、MQDSS、HiMQ-3 の 8 方式である。これらの方式はすべて UF-CMA 安全性を満たすと提案者により主張されている。GeMSS、DualModeMS、HiMQ-3、Gui は HFE 手法に基づいて構成され、LUOV、Rainbow、MQDSS は Oil&Vinegar 手法で構成され、HiMQ-3 は両方の手法を組み合わせて構成されている。特に、GeMSS は松本＝今井構成法（Matsumoto and Imai [1988]）をもとに考案された QUARTZ（Patarin, Courtois, and Goubin [2001]）をさらに改良した方式である[51]。この中で、秘密鍵サイズが比較的小さいのは LUOV、MQDSS であり、公開鍵サイズが比較的小さいのは DualModeMS、MQDSS であり、署名サイズが比較的小さいのは GeMSS、HiMQ-3、Gui、Rainbow である。

そして、上記以外のデジタル署名方式として、WalnutDSA、Post-Quantum RSA Signature、Picnic の 3 方式がある。このうち、Picnic が主張する安全性は SUF-CMA 安全性であり、その他の 2 方式は UF-CMA 安全性を満たすと提案者により主張されている。WalnutDSA は、安全性の観点からブレイド群と呼ばれる数学的構造を利用しており（3 節の図表 8 を参照）、秘密鍵や公開鍵のサイズは比較的小さい。Post-Quantum RSA Signature は、公開鍵暗号 Post-Quantum RSA の仕組みをデジタル署名に利用した方式であり、Post-Quantum RSA と同様の特徴（公開鍵、

[50] 正確には、ベルヌーイ分布に基づくランダムな線形符号を生成している。
[51] QUARTZ は、公開鍵サイズは大きいが、署名サイズが小さいという特徴をもつデジタル署名方式である。

秘密鍵、署名のサイズが大きい）を有する。また、Picnic は、共通鍵暗号を利用しており、秘密鍵や公開鍵のサイズは小さいが、署名サイズは大きい。

５．おわりに

米国連邦政府は、2022 年頃までに耐量子計算機暗号の連邦政府標準暗号を策定し、現在使用している公開鍵暗号を 2026 年頃までに耐量子計算機暗号へ移行する計画を示している。2019 年 1 月末に第 1 ラウンドが終了し、第 2 ラウンドに進む 26 の方式については、2019 年 3 月中旬までに方式の仕様および実装結果を更新した文書を提出することが認められている。

NIST の応募に提出されている耐量子計算機暗号は、一定水準の安全性を確保しながらも、①利用する計算問題として特別な数学的構造が現れない問題（LWE 問題、Goppa 符号の SDP 等）を利用することで新たな攻撃法登場のリスクを少なくする設計方針、②特別な数学的構造をもつ問題（Ring-LWE 問題、Quasi-Cyclic 符号の SDP 等）を利用してデータサイズの効率化をめざす設計方針、あるいは③両者のバランスを考慮できるような計算問題（Module-LWE 問題、LRPC 符号の SDP 等）を利用する設計方針というように、各種方式の設計方針には安全性と効率性のトレードオフの間でさまざまな組み合わせが見受けられる。

NIST に提出されている耐量子計算機暗号の技術的課題として、ほとんどの方式が（量子）ランダムオラクルを仮定しているため、今後、利用されるハッシュ関数の量子コンピュータに対する安全性の解析が必要であろう[52]。また、KEM が DEM（共通鍵暗号）と組み合わせて利用される場合、その利用形態から共通鍵暗号（AES 等）の量子コンピュータに対する安全性の解析も必要である。実際、量子コンピュータによる攻撃への対策として、どのような共通鍵暗号においても鍵の伸長は必要不可欠であるが、一部の共通鍵暗号については、そうした対策だけでは有効なものとならないことを示唆する研究成果が報告されている（清藤・四方［2019］）。

本稿の冒頭で述べたように、耐量子計算機暗号の重要性が認識されたのは、量子コンピュータにより素因数分解問題を高速に解く手法が示されたからである（Shor [1994, 1997]）。この手法は量子ゲート型コンピュータを利用するアルゴリズムであるが、近年、量子アニーリング型コンピュータを利用して素因数分解問題を解く研究報告も行われている（Jiang *et al.* [2018]、清水ら [2019]等）。今後、量子ゲート型および量子アニーリング型それぞれの研究開発がさらに進展し、それらが実際に暗号の解析に使用された研究報告が増えていくものと考

[52] ランダムオラクルを仮定する場合、理想的にはランダム関数を利用するべきであるが、これを実現することは難しいため、現在広く利用されている多くの暗号は、ハッシュ関数で代用しており、その出力値が乱数となるための工夫が施されている。

えられる（山口ら[2019]等）。

また、米国以外での耐量子計算機暗号に対する取り組みとして、欧州連合（EU）においても、耐量子計算機暗号の標準化に向けたロードマップの検討を開始している（European Telecommunications Standards Institute [2017]）。わが国においても、CRYPTREC（Cryptography Research and Evaluation Committees）において、研究動向調査が開始され、今後、政府機関等を中心に量子コンピュータへの対策に関する検討が進められていくものと考えられる（情報通信研究機構・情報処理推進機構［2018］）。

金融分野においても、安全かつ安定的な金融サービスの提供を中長期的に実現していく観点から、耐量子計算機暗号の標準化を巡る世界の動きをフォローしつつ、現行システムからの移行に向けた検討を計画的に進める準備を行っていくことが望ましいと考えられる。

以　上

参考文献

清水俊也・伊豆哲也・篠原直行・盛合志帆・國廣昇、「アニーリング計算による素因数分解について」、2019 年暗号と情報セキュリティシンポジウム発表論文、電子情報通信学会、2019 年

情報通信研究機構・情報処理推進機構、「CRYPTREC Report 2017 暗号技術評価委員会報告」、情報通信研究機構・情報処理推進機構、2018 年（https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2017.pdf、2019 年 3 月 5 日）

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暗号アルゴリズム『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、2015 年、135～170 頁

――――・四方順司、「量子コンピュータが共通鍵暗号の安全性に与える影響」、『金融研究』第 38 巻第 1 号、日本銀行金融研究所、2019 年、45～72 頁

山口純平・マンダルアブラディップ・モンゴメリーハート・ロイアーナブ・清水俊也・大堀龍一・下山武司、「アニーリングを用いた格子問題の求解」、2019 年暗号と情報セキュリティシンポジウム発表論文、電子情報通信学会、2019 年

Aggarwal, Divesh, Antoine Joux, Anupam Prakash, and Miklos Santha, "A New Public-Key Cryptosystem via Mersenne Numbers," *Proceedings of CRYPTO 2018 Part 3, Lecture Notes in Computer Science*, 10993, Springer-Verlag, 2018, pp. 459-482.

Aguilar-Melchor, Carlos, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor, "Efficient Encryption from Random Quasi-Cyclic Codes," *IEEE Transactions on Information Theory*, 64 (5), IEEE, 2018, pp. 3927-3943.

Ajtai, Miklós, "The Shortest Vector Problem in L2 is NP-Hard for Randomized Reductions," *Proceedings of ACM Symposium on Theory of Computing (STOC) 1998*, Association for Computing Machinery, 1998, pp. 10-19.

Albrecht, Martin R., Emmanuela Orsini, Kenneth G. Paterson, Guy Peer, and Nigel P. Smart, "Tightly Secure Ring-LWE Based Key Encapsulation with Short Ciphertexts," *Proceedings of European Symposium on Research in Computer Security (ESORICS) 2017, Lecture Notes in Computer Science*, 10492, Springer-Verlag, 2017, pp. 29-46.

Alkim, Erdem, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe, "Post-Quantum Key Exchange -- A New Hope," *Proceedings of USENIX Security Symposium 2016*, Advanced Computing Systems Association, 2016, pp. 327-343.

Aono, Yoshinori, Xavier Boyen, Le Trieu Phong, and Lihua Wang, "Key-Private Proxy Re-Encryption under LWE," *Proceedings of INDOCRYPT 2013, Lecture Notes*

in Computer Science, 8250, Springer-Verlag, 2013, pp. 1-18.

Applebaum, Benny, Yuval Ishai, and Eyal Kushilevitz, "Cryptography with Constant Input Locality," *Journal of Cryptology*, 22 (4), Springer-Verlag, 2009, pp. 429-469.

Banerjee, Abhishek, Chris Peikert, and Alon Rosen, "Pseudorandom Functions and Lattices," *Proceedings of EUROCRYPT 2012, Lecture Notes in Computer Science*, 7237, Springer-Verlag, 2012, pp. 719-737.

Berlekamp, Elwyn R., Robert J. McEliece, and Henk C. A. van Tilborg, "On the Inherent Intractability of Certain Coding Problems," *IEEE Transactions on Information Theory*, 24 (3), IEEE, 1978, pp. 384-386.

Bos, Joppe, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila, "Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE," *Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS) 2016*, Association for Computing Machinery, 2016, pp. 1006-1018.

Brakerski, Zvika, Craig Gentry, and Vinod Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," *Proceedings of Innovations in Theoretical Computer Science Conference (ITCS) 2012*, Association for Computing Machinery, 2012, pp. 309-325.

Chen, Yuanmi, and Phong Q. Nguyen, "BKZ 2.0: Better Lattice Security Estimates," *Proceedings of ASIACRYPT 2011, Lecture Notes in Computer Science*, 7073, Springer-Verlag, 2011, pp. 1-20.

Cheon, Jung Hee, Kyoohyung Han, Jinsu Kim, Changmin Lee, and Yongha Son, "A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE," *Proceedings of International Conference on Information Security and Cryptology (ICISC) 2016*, *Lecture Notes in Computer Science*, 10157, Springer-Verlag, 2016, pp. 51-74.

————, Duhyeong Kim, Joohee Lee, and Yongsoo Song, "Lizard: Cut off the Tail! A Practical Post-Quantum Public-Key Encryption from LWE and LWR," *Proceedings of International Conference on Security and Cryptography for Networks (SCN) 2018*, *Lecture Notes in Computer Science*, 11035, Springer-Verlag, 2018, pp. 160-177.

Chiba, Daiki, Takahiro Matsuda, Jacob C. N. Schuldt, and Kanta Matsuura, "Efficient Generic Constructions of Signcryption with Insider Security in the Multi-User Setting," *Proceedings of Applied Cryptography and Network Security (ACNS) 2011*, *Lecture Notes in Computer Science*, 6715, Springer-Verlag, 2011, pp.

220-237.

Coppersmith, Don, and Adi Shamir, “Lattice Attacks on NTRU,” *Proceedings of EUROCRYPT 1997, Lecture Notes in Computer Science*, 1233, Springer-Verlag, 1997, pp. 52-61.

Courtois, Nicolas, Alexander Klimov, Jacques Patarin, and Adi Shamir, “Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations,” *Proceedings of EUROCRYPT 2000, Lecture Notes in Computer Science*, 1807, Springr-Verlag, 2000, pp. 392-407.

Cramer, Ronald, and Victor Shoup, “Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack,” *SIAM Journal of Computing*, 33 (1), Society for Industrial and Applied Mathematics, 2004, pp. 167-226.

Dent, Alexander W., “A Designer's Guide to KEMs,” *Proceedings of IMA International Conference on Cryptography and Coding 2003, Lecture Notes in Computer Science*, 2898, Springer-Verlag, 2003, pp. 133-151.

Ding, Jintai, Xiang Xie, and Xiaodong Lin, “A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem,” Cryptology ePrint Archive, 2012/688, International Association for Cryptologic Research, 2012.

El Bansarkhani, Rachid, “LARA - A Design Concept for Lattice-Based Encryption,” Cryptology ePrint Archive, 2017/049, International Association for Cryptologic Research, 2017.

————, Özgür Dagdelen, and Johannes Buchmann, “Augmented Learning with Errors: The Untapped Potential of the Error Term,” Cryptology ePrint Archive, 2014/733, International Association for Cryptologic Research, 2014.

European Telecommunications Standards Institute, “ETSI TC Cyber Working Group for Quantum Safe Cryptography Chairman’s Report,” ETSI IQC Quantum Safe Workshop, European Telecommunications Standards Institute, 2017.

Faugére, Jean-Charles, “A New Efficient Algorithm for Computing Gröbner Bases (F_4),” *Journal of Pure and Applied Algebra*, 139(1-3), Elsevier, 1999, pp. 61 - 88.

————, “A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F_5),” *Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC) 2002*, Association for Computing Machinery, 2002, pp. 75-83.

Fujisaki, Eiichiro, and Tatsuaki Okamoto, “Secure Integration of Asymmetric and Symmetric Encryption Schemes,” *Proceedings of CRYPTO 1999, Lecture Notes in Computer Sciences*, 1666, Springer-Verlag, 1999, pp. 537-554.

Gabidulin, Érnest Mukhamedovich, “Theory of Codes with Maximum Rank Distance,” *Problemy Peredachi Informatsii*, 21 (1), Russian Academy of Sciences, 1985, pp. 3-16.

Gama, Nicolas, Phong Q. Nguyen, and Oded Regev, “Lattice Enumeration Using Extreme Pruning,” *Proceedings of EUROCRYPT 2010*, *Lecture Notes in Computer Science*, 6110, Springer-Verlag, 2010, pp. 257-278.

Goldreich, Oded, Shafi Goldwasser, and Shai Halevi, “Public-Key Cryptosystems from Lattice Reduction Problems,” *Proceedings of CRYPTO 1997*, *Lecture Notes in Computer Science*, 1294, Springer-Verlag, 1997, pp. 112-131.

————, Daniele Micciancio, Shmuel Safra, and Jean-Pierre Seifert, “Approximating Shortest Lattice Vectors is Not Harder than Approximating Closest Lattice Vectors,” *Information Processing Letters*, 71 (2), Elsevier, 1999, pp. 55-61.

Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” *Proceedings of Algorithmic Number Theory Symposium (ANTS) 1998*, *Lecture Notes in Computer Science*, 1423, Springer-Verlag, 1998, pp. 267-288.

Hofheinz, Dennis, Kathrin Hövelmanns, and Eike Kiltz, “A Modular Analysis of the Fujisaki-Okamoto Transformation,” *Proceedings of Theory of Cryptography Conference (TCC) 2017*, *Lecture Notes in Computer Science*, 10677, Springer-Verlag, 2017, pp. 341-371.

Hülsing, Andreas, Joost Rijneveld, John Schanck, and Peter Schwabe, “High-Speed Key Encapsulation from NTRU,” *Proceedings of Cryptographic Hardware and Embedded Systems (CHES) 2017*, *Lecture Notes in Computer Science*, 10529, Springer-Verlag, 2017, pp. 232-252.

Jiang, Shuxian, Keith A. Britt, Alexander J. McCaskey, Travis S. Humble, and Sabre Kais, “Quantum Annealing for Prime Factorization,” *Scientific Reports*, 8, Nature, 2018, Article No. 17667 (available at: https://www.nature.com/articles/s41598-018-36058-z.pdf、2019 年 3 月 6 日).

Jin, Zhengzhong, and Yunlei Zhao, “Optimal Key Consensus in Presence of Noise,” Cryptology ePrint Archive, 2017/1058, International Association for Cryptologic Research, 2017.

Khot, Subhash, “Hardness of Approximating the Shortest Vector Problem in Lattices,” *Journal of the ACM*, 52(5), Association for Computing Machinery, 2005, pp. 789-808.

Kipnis, Aviad, Jacques Patarin, and Louis Goubin, “Unbalanced Oil and Vinegar Signature Schemes,” *Proceedings of EUROCRYPT 1999*, *Lecture Notes in*

Computer Science, 1592, Springer-Verlag, 1999, pp. 206-222.

Kobara, Kazukuni, and Hideki Imai, "Semantically Secure McEliece Public-Key Cryptosystems - Conversions for McEliece PKC -," *Proceedings of Public Key Cryptography (PKC) 2001*, *Lecture Notes in Computer Science*, 1992, Springer-Verlag, 2001, pp. 19-35.

Korkine, Alexander and Yegor Ivanovich Zolotarev, "Sur les Formes Quadratiques," *Mathematische Annalen*, 6 (3), Springer-Verlag, 1873, pp. 366-389.

Lenstra, Arjen K., Hendrik W. Lenstra, Jr., and László Lovász, "Factoring Polynomials with Rational Coefficients," *Mathematische Annalen*, 261 (4), Springer-Verlag, 1982, pp. 515-534.

Li, Yuan Xing, Robert H. Deng, and Xin Mei Wang, "On the Equivalence of McEliece's and Niederreiter's Public-Key Cryptosystems," *IEEE Transactions on Information Theory*, 40 (1), IEEE, 1994, pp. 271-273.

Lindner, Richard, and Chris Peikert, "Better Key Sizes (and Attacks) for LWE-Based Encryption," *Proceedings of Cryptographers' Track at the RSA Conference (CT-RSA) 2011*, *Lecture Notes in Computer Science*, 6558, Springer-Verlag, 2011, pp. 319-339.

Lyubashevsky, Vadim, ————, and Oded Regev, "On Ideal Lattices and Learning with Errors over Rings," *Proceedings of EUROCRYPT 2010*, *Lecture Notes in Computer Science*, 6110, Springer-Verlag, 2010, pp. 1-23.

Matsumoto, Tsutomu, and Hideki Imai, "Public Quadratic Polynominal-Tuples for Efficient Signature-Verication and Message-Encryption," *Proceedings of EUROCRYPT 1988*, *Lecture Notes in Computer Science*, 330, Springer-Verlag, 1988, pp. 419-453.

McEliece, Robert J., "A Public-Key Cryptosystem Based on Algebraic Coding Theory," Deep Space Network Progress Report, DSN PR 42-44, National Aeronautics and Space Administration, 1978, pp. 114-116.

Micciancio, Daniele, and Oded Regev, "Worst-Case to Average-Case Reductions Based on Gaussian Measures," *SIAM Journal on Computing*, 37 (1), Society for Industrial and Applied Mathematics, 2007, pp. 267-302.

————, and Panagiotis Voulgaris, "Faster Exponential Time Algorithms for the Shortest Vector Problem," *Proceedings of ACM-SIAM Symposium on Discrete Algorithms (SODA) 2010*, Society for Industrial and Applied Mathematics, 2010, pp. 1468-1480.

National Institute of Standards and Technology, "Post-Quantum Cryptography: Post-Quantum Cryptography Standardzation," National Institute of Standards

and Technology, 2017 (available at: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization、2019 年 3 月 5 日).

————, "PQC Standardization Process: Second Round Candidate Announcement," National Institute of Standards and Technology, 2019 (available at: https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates、2019 年 3 月 5 日).

Niederreiter, Harald, "Knapsack-Type Cryptosystems and Algebraic Coding Theory," *Problems of Control and Information Theory*, 15 (2), Akadémiai Kiadó, 1986, pp. 159-166.

Patarin, Jacques, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms," *Proceedings of EUROCRYPT 1996*, *Lecture Notes in Computer Science*, 1070, Springer-Verlag, 1996, pp. 33-48.

————, Nicolas Courtois, and Louis Goubin, "QUARTZ, 128-Bit Long Digital Signatures," *Proceedings of Cryptographers' Track at the RSA Conference (CT-RSA) 2001*, *Lecture Notes in Computer Science*, 2020, Springer-Verlag, 2001, pp. 282-297.

Pöppelmann, Thomas, and Tim Güneysu, "Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware," *Proceedings of Selected Areas in Cryptography (SAC) 2013*, *Lecture Notes in Computer Science*, 8282, Springer-Verlag, 2013, pp. 68-85.

Pujol, Xavier, and Damien Stehlé, "Solving the Shortest Lattice Vector Problem in Time $2^{2.465n}$," Cryptology ePrint Archive, 2009/605, International Association for Cryptologic Research, 2009.

Regev, Oded, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," *Journal of the ACM*, 56 (6), Association for Computing Machinery, 2009, Article No. 34.

Rivest, Ronald L., Adi Shamir, and Leonard Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM*, 21(2), Association for Computing Machinery, 1978, pp. 120-126.

Roşca, Miruna, Amin Sakzad, Damien Stehlé, and Ron Steinfeld, "Middle-Product Learning With Errors," *Proceedings of CRYPTO 2017 Part 3*, *Lecture Notes in Computer Science*, 10403, Springer-Verlag, 2017, pp. 283-297.

Saarinen, Markku-Juhani O., "HILA5: On Reliability, Reconciliation, and Error Correction for Ring-LWE Encryption," *Proceedings of Selected Areas in*

Cryptography (SAC) 2017, *Lecture Notes in Computer Science*, 10719, Springer-Verlag, 2017, pp.192-212.

Schneider, Michael, "Analysis of Gauss-Sieve for Solving the Shortest Vector Problem in Lattices," *Proceedings of International Workshop on Algorithms and Computation (WALCOM) 2011*, *Lecture Notes in Computer Science*, 6552, Springer-Verlag, 2011, pp. 89-97.

Schnorr, Claus Peter, and Martin Euchner, "Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems," *Mathematical Programming*, 66 (2), Springer-Verlag, 1994, pp. 181-199.

————, and Horst Helmut Hörner, "Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction," *Proceedings of EUROCRYPT 1995*, *Lecture Notes in Computer Science*, 921, Springer-Verlag, 1995, pp. 1-12.

Shor, Peter W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings of IEEE Symposium on Foundations of Computer Science (SFCS) 1994*, IEEE, 1994, pp. 124-134.

————, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, 26 (5), Society for Industrial and Applied Mathematics, 1997, pp. 1484-1509.

Shoup, Victor, "Using Hash Functions as a Hedge against Chosen Ciphertext Attack," *Proceedings of EUROCRYPT 2000*, *Lecture Notes in Computer Science*, 1807, Springer-Verlag, 2000, pp. 275-288.

Targhi, Ehsan Ebrahimi, and Dominique Unruh, "Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms," *Proceedings of Theory of Cryptography (TCC) 2016 Part 2*, *Lecture Notes in Computer Science*, 9986, Springer-Verlag, 2016, pp. 192-216.

van Emde Boas, Peter, "Another NP-Complete Partition Problem and the Complexity of Computing Short Vectors in a Lattice," *Technical Report 81-04*, Mathematics Department, University of Amsterdam, 1981.