特集論文

耐量子計算機暗号 ―量子コンピュータによる解読にも耐え得る次世代暗号―

川合　豊*
Yutaka Kawai
廣政　良†
Ryo Hiromasa
相川勇輔‡
Yusuke Aikawa

Post－Quantum Cryptography
―Next Generation Encryption Technology Resistant to Quantum Computing―

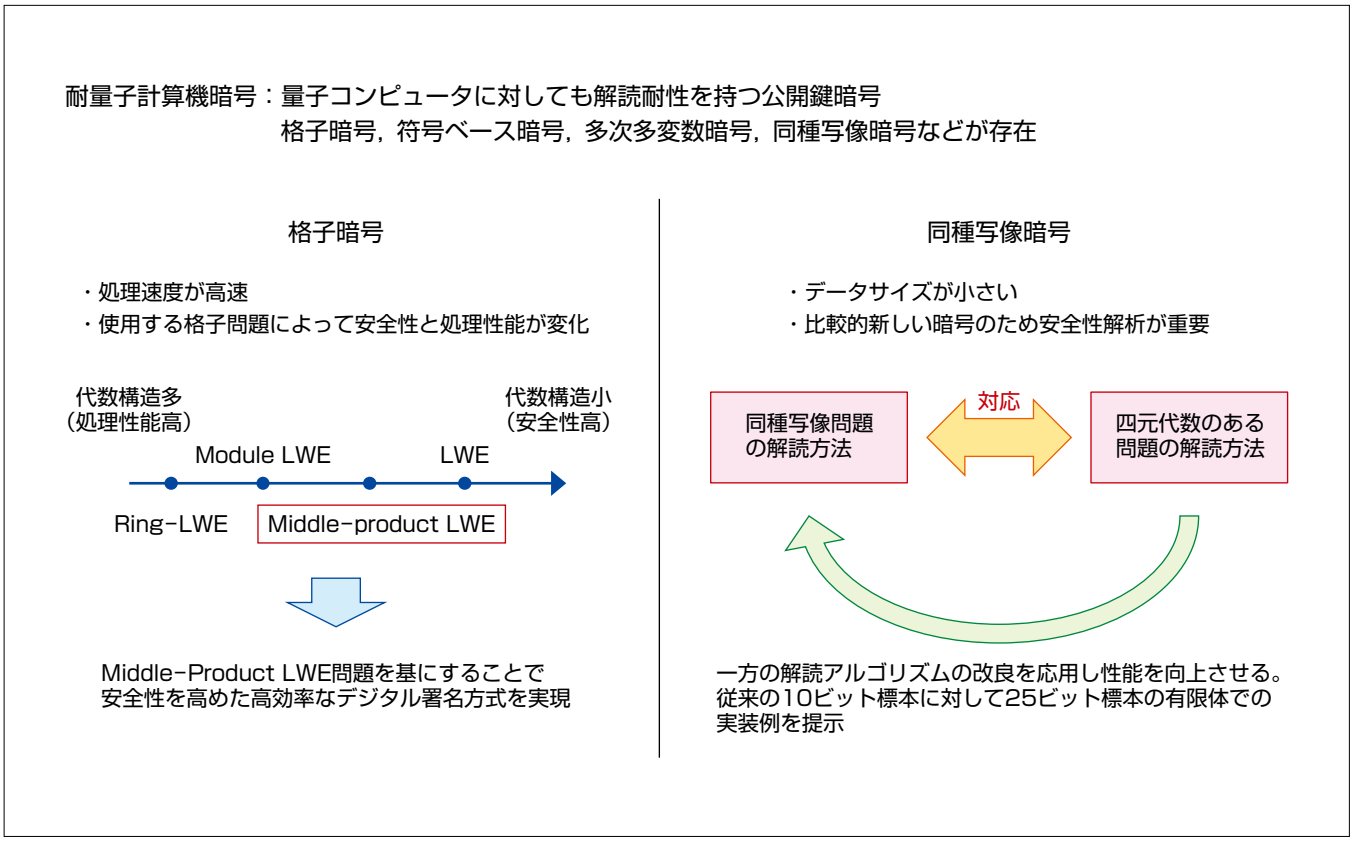
要　旨

将来，大規模な量子コンピュータが実現された場合，現在インターネットなどで広く使用されているRSA（Rivest Shamir Adleman）暗号や楕円（だえん）曲線暗号などの公開鍵暗号が解読されてしまうことが分かっている。そこで，そのような量子コンピュータが登場しても解読されないことが期待される公開鍵暗号“耐量子計算機暗号”の研究が盛んに行われている。

耐量子計算機暗号の研究は米国標準技術研究所（National Institute of Standards and Technology：NIST）の標準化計画を中心に様々な研究が進んでいる。耐量子計算機暗号は安全性を保証するために利用する数学的問題の違いから様々な種類の暗号がある。

これらの背景の下，処理速度が高速な“格子暗号”と，鍵のデータ長などが小さい“同種写像暗号”に着目し研究を進めている。これまでに格子暗号では，公開鍵暗号の一つの用途であるデジタル署名方式について，高安全化を実現した。同種写像暗号は格子暗号と比べて安全性解析の研究途上の暗号である。そこで安全性や効率性に関して，理論と実装の両面から解析を進めて，同種写像暗号の安全性や効率に関する知見を得た。

NISTの標準化選定が途中段階であることなどからも分かるように，耐量子計算機暗号はまだまだ研究途上の分野であり，研究動向の注視と，解析・設計技術の向上が必要不可欠である。そこで，今後も高安全かつ高効率な耐量子計算機暗号の実現を行い，安心・安全な社会の実現に貢献していく。



耐量子計算機暗号の種類と格子暗号・同種写像暗号の安全性解析の結果

量子コンピュータに解読耐性を持つと期待される耐量子計算機暗号のうち，処理速度が高速という特長を持つ格子暗号と，データサイズが小さいという特長を持つ同種写像暗号に関して効率化や安全性解析を行った。格子暗号に関しては比較的新しいMiddle-product LWE（Learning With Errors）問題を基にしたデジタル署名を実現し，同種写像暗号では他の代数（四元代数）の問題に置き換えて解析を実施し従来より長いビット長に対する攻撃を成功させた。

*情報技術総合研究所（博士（科学））　†同研究所（博士（情報学））
‡同研究所（博士（理学））

1. まえがき

現在，個人情報などの重要な情報がインターネット上などでやり取りされる際，それらを守るために様々な暗号技術が使用されている。中でも公開鍵暗号は，データの秘匿だけでなく，通信相手が正規のユーザーであるかを検証する相手認証などに広く利用されている。現在広く使用されている公開鍵暗号として，RSA暗号や楕円曲線暗号がある。RSA暗号は素因数分解問題，楕円曲線暗号は楕円離散対数問題が利用されており，これらの問題が現在のコンピュータでは現実的な時間で解読不可能であることから安全性の保証になっている。しかし，これらの問題は大規模な量子コンピュータが実現された場合，Shorのアルゴリズムによって現実的な時間で解読されてしまうことが知られている。

そこで，量子コンピュータに対しても解読耐性を持つことが期待される耐量子計算機暗号の研究が盛んである。耐量子計算機暗号の研究はNISTが主導する標準化選定を中心に動いている[1]。NISTでは2017年11月まで標準化候補の方式募集を行った。その後２回の選定が行われ，現在第３回の選考（第３ラウンド）中である[注1]。締切り時点では82方式の投稿があったが，第３ラウンドでは最終候補７候補と次点候補８候補まで選定されている。第３回の選考は2023年頃までに終了すると言われており，2024年頃には耐量子計算機暗号の標準規格を選定する計画になっている（**図１**）。

耐量子計算機暗号は，格子暗号，符号ベース暗号，多次多変数暗号，同種写像暗号などの種類が存在する。このうち，本稿では，処理が高速な格子暗号，データサイズが小さい同種写像について述べる（**表１**）。

（注１） 2022年５月現在。７月に第３ラウンドが終了し，CRYSTALS-KYBER，CRYSTALS-DILITHIUM，FALCON，SPHINCS+の標準化が決定した。

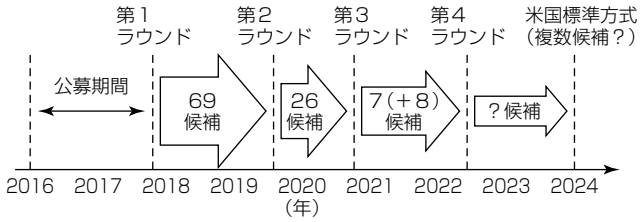


図１．NIST標準化の流れ

表１．格子暗号と同種写像暗号の比較

	格子暗号	同種写像暗号
鍵サイズ	従来の楕円曲線暗号と比較して10倍以上	従来の楕円曲線暗号と同程度
処理速度	高速	低速
NIST標準化候補	最終候補に５方式が選定（CRYSTALS-KYBER，NTRU，SABER，CRYSTALS-DILITHIUM，FALCON）	次点候補に１方式が選定（SIDH）

SIDH：Supersingular Isogeny Diffie-Hellman

2. 格子暗号

2.1 格子暗号概要

格子暗号は，格子（線形独立なベクトルの整数線形結合で表されるベクトルの集合）に関する計算問題（格子問題）の解読困難性を安全性の根拠とする暗号技術である。この章では格子暗号の安全性の根拠になる様々な問題（Module LWE問題，NTRU問題，Module LWR（Learning With Rounding）問題など）が登場するが，問題によって異なるものの，それぞれが特殊な格子に関連する計算問題である。

NISTの耐量子計算機暗号標準化では，最も候補方式の数が多いのが格子暗号である。また，NISTは公開鍵暗号とデジタル署名について，格子暗号の候補方式の中から少なくとも一つずつは標準化方式として選出するであろうと明言しており，耐量子計算機暗号の標準化方式として非常に期待されている暗号技術である。

2.2 NIST標準化候補方式（格子暗号）

格子暗号の第3ラウンド候補は，最終候補としてCRYSTALS-KYBER，NTRU，SABER，CRYSTALS-DILITHIUM，FALCONの５種類の方式が選ばれており，次点候補としてFrodoKEM，NTRU Primeの２種類の方式が選ばれている。

(1) CRYSTALS-KYBER

CRYSTALS-KYBER方式はModule LWE問題と呼ばれる格子問題の解読困難性を安全性の根拠とする公開鍵暗号方式である。多くのアプリケーションで利用可能な効率性を達成しており，また，特定のパラメータを増減させるだけで効率性と安全性のトレードオフを容易に調整可能であるという特長を備える。

(2) NTRU

NTRU方式は，NTRU問題と呼ばれる格子問題の解読困難性を安全性の根拠とする公開鍵暗号方式である。NTRU問題は長い歴史を持つ格子問題であり，長い期間，安全性を精査されている。しかし，鍵生成が他の格子暗号方式に比べて低速であるという欠点がある。

(3) SABER

SABER方式は，Module LWR問題の解読困難性を安全性の根拠とする公開鍵暗号方式である。CRYSTALS-KYBER方式に匹敵する効率性を持つ。

(4) CRYSTALS-DILITHIUM

CRYSTALS-DILITHIUM方式は，Module LWE問題とModule SIS（Small Integer Solution）問題の解読困難性を安全性の根拠とするデジタル署名方式である。鍵サ

イズと署名サイズや，各種アルゴリズム（鍵生成，署名生成・検証）の効率性のバランスが取れているという特長を備える。

⑸ FALCON

FALCON方式は，NTRU問題の解読困難性を安全性の根拠とするデジタル署名方式である。署名生成と署名検証アルゴリズムは非常に効率的であるが，鍵生成アルゴリズムが低速であるという特徴を備える。一方で，公開鍵サイズと署名サイズの総和は，CRYSTALS-DILITHIUM方式よりも小さいという特長を持つ。

2.3 高安全なデジタル署名方式の構成

三菱電機では，2015年から格子暗号の研究開発に取り組んでいる。代表的な成果を次に簡単に述べる。これは格子問題を安全性の根拠とするデジタル署名方式の高安全化に寄与する成果である。

LWE問題，Module LWE問題，Ring-LWE問題など，格子暗号には様々な格子問題が存在し，それらは問題で使用される格子を定義する多項式による違いがある。特定の多項式を用いることで処理速度が向上することなどが知られる一方で，安全性の低下を招くおそれがあり，どのような多項式に対して構成するかは非常に重要である。そこで，Middle-product LWE問題と呼ばれる比較的新しい格子問題を安全性の根拠として高安全なデジタル署名方式を設計した。Middle-product LWE問題の解読困難性は，様々な多項式に関連して定義される格子問題の解読困難性の下で保証されるという性質を持つ。現在，格子暗号として利用されている暗号技術の安全性は，ある固定された多項式について定義される格子問題の解読困難性によって保証されているため，先に述べた安全性上の問題があるが，Middle-product LWE問題を使用することで，特定の多項式に関連して定義されていないような格子問題を安全性の根拠にできる，先に述べたリスクを回避した高安全なデジタル署名方式を構成できる[(2)]。

2.4 格子暗号の今後の展望

2023年までには，NISTによる標準化ドラフトの公開が予定されており，数年以内には標準化方式が策定される。どの格子暗号方式が標準化方式に策定されるにせよ，暗号技術を安全に運用するためには格子暗号に関する深い知見が必要不可欠であるため，研究開発を促進し格子暗号技術への理解を深めることが重要である。また，格子暗号で使用される技術は暗号化したままデータの情報処理が可能な準同型暗号への応用も期待されているため，次世代暗号技術の開発には非常に重要な技術である。

3. 同種写像暗号

3.1 楕円曲線暗号から同種写像暗号へ

素数pが与えられると，0から$p-1$までのp個の整数からなる和と積の定まった有限の数の世界$\mathbb{F}_p$を構成できる。これを標数pの有限体と呼ぶ。a，bを$\mathbb{F}_p$の元として方程式

$$Y^2 = X^3 + aX + b$$

を楕円曲線と呼ぶ。この楕円曲線上には楕円点$P_1=(x_1, y_1)$，$P_2=(x_2, y_2)$が存在し，これら楕円点に対して加算を定義できる。すなわち，二つの楕円点，$P_1=(x_1, y_1)$，$P_2=(x_2, y_2)$を与えると，三つ目の解$P_3=(x_3, y_3)$を$\mathbb{F}_p$上の演算を利用してx_1，y_1，x_2，y_2から計算ができる。加算が定義できるため楕円点は群（有利点群）を成して，この性質を利用して楕円曲線暗号は実現されている。楕円曲線での有理点群上の楕円離散対数問題を，現在の計算機で効率的に解くアルゴリズムは知られておらず，楕円曲線暗号の安全性の根拠になっている。しかし，楕円離散対数問題はShorのアルゴリズムによる大規模な量子コンピュータによって解読されてしまうことが分かっている。

このような状況に対して，量子コンピュータによる解読にも耐え得る楕円曲線の数論を用いた新たな暗号方式の研究が進められている。それは楕円曲線の同種写像を基礎に置く暗号方式群であり，同種写像暗号と総称される。同種写像とは複数の楕円曲線間の代数的な表現を持つ群準同型写像のことである。一つの楕円曲線E_1が与えられたとき，その有限部分群Gを一つランダムに選ぶと，それに対応した同種写像とその像$f_G : E_1 \rightarrow E_2$が定まり，かつ計算が可能である。一方で，楕円曲線$E_1$と$E_2$が与えられたとき，それらの間の同種写像に対応する$E_1$の有限部分群$G$を計算することは計算量的に困難な問題であると考えられている。この問題を同種写像問題という。同種写像暗号のアイデアの核心は，同種写像の像の情報E_2を公開鍵に利用し，E_1からE_2への同種写像を与える有限部分群Gの情報を秘密鍵に利用するというものである。

3.2 同種写像暗号方式とNIST標準化候補方式

重要な同種写像暗号方式として2011年に提案されたSIDHと2018年に提案されたCSIDH（Commutative SIDH）がある。どちらも格子暗号に比べると効率性は劣るが，鍵サイズが著しく小さい鍵共有方式になっている（**表1**）。例えば，SIDHの公開鍵のサイズは330バイト程度であり，CSIDHでは64バイトである。CSIDHはNISTによる耐量子計算機暗号の標準化が始まった後の提案であったが，SIDHはこれを基にした暗号化であるSIKE（Supersingular

Isogeny Key Encapsulation)が標準化に投稿されて第3ラウンドの次点候補になっている。

格子暗号を含めた他の耐量子計算機暗号では鍵サイズや暗号文サイズの小さい暗号化方式を構成することは難しいため，SIKEは有望な方式の一つである。しかし，効率性及び安全性の面に課題を抱える。効率性に関しては，暗号化に同種写像計算という複雑な処理が必要であり，格子暗号と比較して暗号化が10倍程度低速という問題がある。安全性に関しては，同種写像暗号は提案から10年程度しか経(た)っていないという点から，数学的な研究及び解析が研究途上であるという点に問題がある。したがって，今後同種写像暗号を実用していくためには，同種写像計算の数学への深い理解とそれによる計算の効率化及び同種写像問題への様々な数学的アプローチによる理解が必須になる。

3.3 同種写像暗号に関する安全性と効率性解析

当社では，同種写像暗号の安全性や効率性の解析を行っている。まず，安全性に関して，四元代数と呼ばれる代数的構造を利用した解析を行った。楕円曲線とある四元代数の極大オーダーが一対一に対応するというドイリング対応というものが存在する。これの対応を用いて，四元代数側で同種写像の対応物を計算し，それを楕円曲線側に戻して同種写像問題を解くアルゴリズムを構成することで安全性解析を行うというものである。前者を解く数論アルゴリズムとしてKLPTアルゴリズムが，後者を解く数論アルゴリズムとして構成的ドイリング対応アルゴリズムが知られている。まずKLPTアルゴリズムの性能向上を行い，さらに，その結果を構成的ドイリング対応アルゴリズムの性能向上へ応用した。その結果，従来10ビット標数の有限体上での動作が限界であったが25ビット標数での実装例を構成した[3]。これは今後，安全な同種写像暗号のビット長を選定する際に考慮すべき結果になると考えられる。

効率性に関して，これまで様々なタイプの楕円曲線に対して個々に同種写像計算公式が構成され，それらの間の実装性能比較が行われてきたが，どの計算方式を利用しても数％程度の性能差しかないことが知られていた。そこで，これまで個々の楕円曲線に応じて調べられてきた同種写像計算を統一する理論的枠組み(一般化モンゴメリー座標の理論)を構築し，それを用いて一般の楕円曲線に適用できる公式を導いた。この公式は既存研究の多くを含んで，更に一般化を行い既存研究で示された“公式間の性能差は数％程度”という事実を数学的に説明することに成功した。つまり，この結果は同種写像計算が特別高速になるような楕円曲線のタイプは存在しないということの一つの証拠を与えた[4]。

3.4 同種写像暗号の今後の展望

2010年頃から研究が始まった同種写像暗号は，このように数学と深く交わりながら著しく発展を続けている。実用化へ向けて特に重要な研究は安全性解析であり，暗号の安全性を保証するために様々な数学的技術を駆使した解析及び実装データ収集が求められる。処理の効率性に関しては，同種写像計算という重い処理を含むため抜本的な進展を得ることは難しいように思われるが，データサイズが小さいという強みを生かしたユースケースの検討も考えられ，そのためのデータサイズ圧縮技術の研究なども重要になる。また，同種写像暗号の欠点の一つに代数性の乏しさがあり，それによって格子暗号のように高い機能を暗号方式に持たせることが難しい。今後，同種写像暗号の高機能化の研究も重要性が増していくものと思われる。

4. む す び

量子コンピュータに対しても解読耐性のある耐量子計算機暗号のうち，格子暗号と同種写像暗号に関してその概要と，格子暗号について高安全なデジタル署名方式を，同種写像暗号について安全性解析の改良と効率性に関する証拠を述べた。

今後も安全性解析と設計とを行い，安心・安全な社会の実現に貢献していく。

参 考 文 献

(1) NIST：Post-Quantum Cryptography
https://csrc.nist.gov/Projects/post-quantum-cryptography

(2) Bai，S.，et al.：MPSign: A Signature from Small-Secret Middle-Product Learning with Errors，PKC 2020，66～93 (2020)

(3) Kambe，Y.，et al.：Solving the Constructive Deuring Correspondence via the Kohel-Lauter-Petit-Tignol Algorithm，Mathematical Cryptology，**1**，No.2，10～24 (2021)

(4) Moriya，T.，et al.：The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography，IACR Cryptology ePrint Archive，**2022**，150 (2022)