特集 1.

量子計算機時代のセキュリティ
――耐量子計算機暗号の動向――

Security in the Era of Quantum Computers :
Developments in Post-quantum Cryptography

高木　剛

abstract

現在広く普及している RSA 暗号及びだ円曲線暗号は，量子計算機により危殆化することが知られている．量子計算機時代にも安全に利用できる暗号技術として，耐量子計算機暗号（PQC）の研究が活発に行われている．特に，米国標準技術研究所 NIST により，2016 年から PQC の標準化プロジェクトが進められており，2022 年 7 月には標準化方式が発表された．格子暗号では暗号化方式 CRYSTALS-Kyber，ディジタル署名 CRYSTALS-Dilithium 及び FALCON，ハッシュ関数署名では SPHINCS+ が選定された．本稿では，NIST PQC 標準化プロジェクトの概要及び標準化方式の安全性と処理性能に関して解説を行う．

キーワード：耐量子計算機暗号，格子暗号，ハッシュ関数署名，符号暗号，多変数多項式暗号

1. は　じ　め　に

公開鍵暗号として広く普及している RSA 暗号は，素因数分解問題の困難性を安全性の根拠としている．素因数分解問題を効率的に解く研究は大規模な計算機実験も含めて活発に行われてきた．現在最も漸近的に高速なアルゴリズムとして数体ふるい法が知られており，合成数 N の桁長に対して準指数時間の計算量が必要となる．例えば，現在利用される 2,048 ビットの合成数を数体ふるい法で素因数分解するためには，10^{27} FLOPS のスーパコンピュータを 1 年間占有する計算量が必要と見積もられている．最も高速なスーパコンピュータの Linpack 性能は 10^{18} FLOPS であり，2,048 ビットの素因数分解にはムーアの法則を仮定しても今後数十年以上は必要となる[(1)]．

ところが，1994 年にショアは，量子計算機を用いることにより素因数分解が高速に実行可能なアルゴリズムを発表した[(2)]．ショアの量子アルゴリズムの計算量は合成数 N の桁長に対して多項式時間であり，数体ふるい法から指数関数的なスピードアップを達成している（図 1）．つまり，量子計算機を用いると，合成数 N の桁長を大きくしたとしても，素因数分解問題の困難性は大きく増加しないことになる．このような状態は暗号の危殆化と言われて，RSA 暗号は量子計算機により理論的には解読された状態となっている．

更に，ショアの論文では，だ円曲線暗号の安全性を支える離散対数問題に対しても，量子計算機を用いて高速に解読可能となるアルゴリズムを発表している．つまり，大規模な量子コンピュータが実現すると，現在我々が利用している RSA 暗号及びだ円曲線暗号が危殆化する状況にある．そのため，量子計算機を用いても解読が困難となる数学問題を利用した耐量子計算機暗号（PQC : Post-Quantum Cryptography）の研究開発が活発に行われている．

高木　剛　正員　東京大学大学院情報理工学系研究科数理情報学専攻
E-mail　takagi@mist.i.u-tokyo.ac.jp
Tsuyoshi TAKAGI, Member (Graduate School of Information Science and Technology, The University of Tokyo, Tokyo, 113-8656 Japan).
電子情報通信学会誌　Vol.106 No.11 pp.966-970 2023 年 11 月

2. 耐量子計算機暗号

素因数分解問題や離散対数問題とは異なる計算問題を利用した公開鍵暗号の研究は，RSA 暗号が発表された 1970 年代後半から既に開始されてきた．実際，誤り訂正符号の性質を利用した McEliece 暗号は 1978 年に提案されている．1982 年にはハッシュ関数の一方向性や衝突困難性を安全性の根拠とする Merkle 署名が発表された．また，1980 年代前半から，有限体上の多変数多項式求解問題（MQ 問題）の困難性を基にした多変数多項式暗号が研究されるようになる．更には，1990 年代後半から，NTRU 暗号など格子理論を利用した暗号が提案され，2005 年には Learning with Errors（LWE）問題に基づく暗号が発表された．これらの暗号の安全性は，格子の基底に対して非零最短ベクトルを求める問題（SVP）に基づいているため格子暗号と言われる．また，1990 年代後半から同種写像暗号のアイデアが発表され，2006 年には超特異だ円曲線の同種写像の列で構成されるラマヌジャングラフの計算困難性を基にした暗号も提案された．

また，これらの代表的な数学問題は，2016 年に米国標準技術研究所 NIST が発行した報告書 NIST-IR 8105（https://doi.org/10.6028/NIST.IR.8105）にも，耐量子計算機暗号の主要な候補として記載されている．表 1 に，これらの代表的な耐量子計算機暗号とそこで使われている数学問題をまとめた．

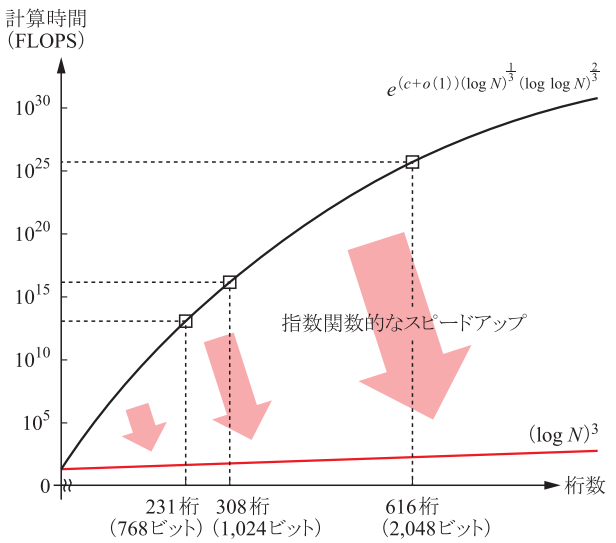

図 1　ショアの量子計算機による計算時間

これらの流れを受けて，2006 年から耐量子計算機暗号を専門とする国際会議 Post-Quantum Cryptography（PQCrypto）がスタートした．更に，2015 年 4 月には，米国標準技術研究所 NIST により，NIST Workshop on Cybersecurity in a Post-Quantum World が開催された．2015 年以降は，耐量子計算機に特化したワークショップや国際会議が数多く開催されるようになる．特に，2016 年 2 月には，筆者がプログラム委員長を務め，九州大学西新プラザにおいて第 7 回目の PQCrypto 2016 を主催した[3]．PQCrypto2016 では，NIST から耐量子計算機暗号の標準化の具体的な計画が示されて，参加者が 240 名を超えるなど，会場は熱気に包まれた状態であった（図 2）．

3. NIST PQC 標準化プロジェクト

2015 年 8 月にアメリカ国家安全性保障局 NSA は耐量子計算機暗号への移行を表明し，2016 年 2 月には米国標準技術研究所 NIST が耐量子計算機暗号の標準化計画を発表した．NIST の耐量子計算機暗号の標準化では，公開鍵暗号プリミティブを対象として，SP 800-56，FIPS PUB 186-4 で規格化されている暗号方式（Public-key Encryption），鍵交換方式（Key Exchange），ディジタル署名（Digital Signature）の耐量子版の公募を行った．NIST による耐量子計算機暗号の標準化に関する情報は，NIST Post-Quantum Crypto Project のホームページ（http://nist.gov/pqcrypto）で入手可能である．

最初に，標準的な安全性評価モデルとして，暗号方式では選択暗号文攻撃に対する識別不可能性（IND-CCA），ディジタル署名では選択平文攻撃に対する存在的偽造不可能性（EUF-CMA）が用いられる．また，暗号方式の効率性の評価基準としては，公開鍵・暗号文・署名などのサイズ，鍵生成・公開鍵・秘密鍵を利用した演算スピード，復号の失敗確率などが用いられる．一方，実社会で利用を想定して，サイドチャネル攻撃・完全前方秘匿性・乱数再利用攻撃などに対する安全性評価もオプションとして考察される．更に，規格化された暗号が現在利用されている標準的な暗号規格に簡単に置

表 1　代表的な耐量子計算機暗号と数学問題

暗号方式	提案年代	数学問題
符号暗号	1970 年代後半から	誤り訂正符号に関する問題
ハッシュ関数署名	1980 年代前半から	ハッシュ関数の衝突問題
多変数多項式暗号	1980 年代前半から	多変数多項式求解問題（MQ 問題）
格子暗号	1990 年代後半から	最短ベクトル問題（SVP）
同種写像暗号	1990 年代後半から	同種写像問題

図 2　国際会議 PQCrypto 2016 の集合写真

表 2　NIST PQC 標準化プロジェクトへの応募暗号（2017 年 11 月）

格子暗号（25 件） Compact LWE, CRYSTALS-DILITHIUM, CRYSTALS-KYBER, Ding Key Exchange, DRS, EMBLEM and R. EMBLEM, FALCON, Frodo, HILA5, KINDI, LAC, LIMA, Lizard, LOTUS, NewHope, NTRU-HRSS-KEM, NTRU Prime, NTRUEncrypt, Odd Manhattan, pqNTRUSign, qTESLA, Round2, SABER, Titanium, Three Bears
符号暗号（18 件） BIG QUAKE, BIKE, Classic McEliece, DAGS, Edon-K, HQC, LAKE, LEDAkem, LEDApkc, LOCKER, McNie, NTS-KEM, pqsigRM, QC-MDPC KEM, RaCoSS, Ramstake, RLCE-KEM, RQC
多変数多項式暗号（10 件） CFPKM, DME, DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow, SRTPI
ハッシュ関数署名（2 件） Gravity-SPHINCS, SPHINCS+
同種写像暗号（1 件） SIKE
その他（13 件） Giophantus, Guess Again, HK17, Lepton, Mersenne-756839, OKCN/AKCN/CNKE, Ouroboros-R, Picnic, Post-quantum RSAEncryption, Post-quantum RSASignature, RankSign, RVB, WalnutDSA

き換えることが可能な（Drop-in-replacement）方式が望まれている．NIST PQC 標準化プロジェクトに提案する場合は，以上の安全性及び効率性を自己評価したデータを含む必要があった．

NIST による PQC 標準化プロジェクトの公募は 2017 年 11 月に締め切られ，公募条件を満たした方式は 69 件となった（表 2）．そのうち，格子暗号 25 件，符号暗号 18 件，多変数多項式暗号 10 件，ハッシュ関数署名 2 件，同種写像暗号 1 件であった．全ての提案暗号は，NIST PQC 標準化プロジェクトのホームページで公開されている．提案暗号を機能別に分類すると，鍵交換を含む暗号化方式は 49 件，ディジタル署名方式は 20 件となった．応募は世界中の 25 か国からあり，国別では北米とヨーロッパからの応募が多く，アジアからは日本，韓国，中国，台湾，シンガポール，オーストラリアから提案された．提案者は合計で 278 人に及び，そのうち 67 人は 2 件以上の方式を応募していた．日本からの提案は，KDDI 総合研究所，東芝研究開発センター，情報通信研究機構，そして筆者の東京大学からのグループとなった．

NIST PQC 標準化プロジェクトでは，公開されたメーリングリストが準備されており，2018 年 12 月までに 600 件以上のメールが投稿されるなど，提案方式の安全性などに関して多く活発な議論が交わされた．2019 年 1

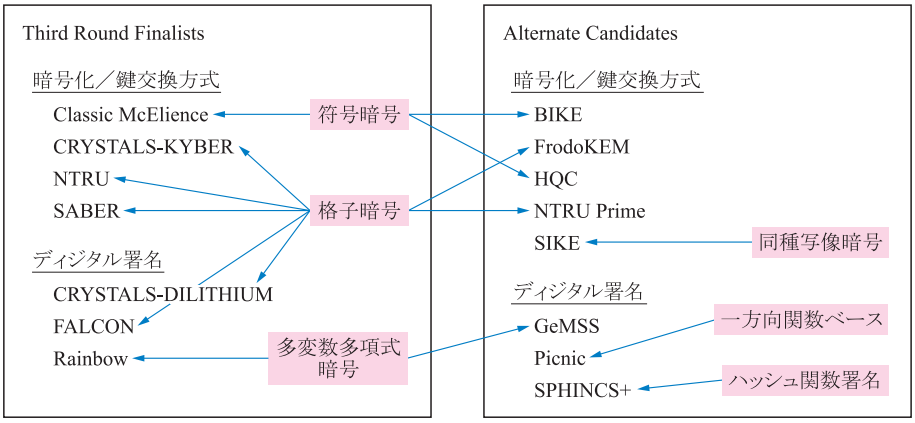

図 3　NIST PQC 標準化プロジェクト第 3 ラウンド選出方式（2020 年 7 月）

月に PQC 標準化プロジェクトの第 2 ラウンドへ進む 26 方式が発表され，2020 年 7 月には第 3 ラウンドの方式が選出された（図 3）．第 3 ラウンドには，最終候補（Finalists）として 7 方式，代替方式（Alternate Candidates）として 8 方式が選出された．最終候補において，格子暗号が暗号化 3 方式及びディジタル署名 2 方式と主要な候補となった．その他の最終候補として符号暗号・多変数多項式暗号が選出され，代替方式として同種写像暗号・ハッシュ関数署名・一方向関数ベースの方式が選ばれた．NIST は格子暗号だけを標準化方式として選出するのではなく，安全性や性能の特性を考慮して他の基本問題を基にした方式も標準化する予定としている．

2022 年 7 月に最初の標準化方式が発表され，暗号化・鍵交換方式は格子暗号の CRYSTALS-Kyber，ディジタル署名は格子暗号の CRYSTALS-Dilithium と FALCON，そしてハッシュ関数署名の SPHINCS+ が選定された（図 4 上側）．第 3 ラウンドの格子暗号の暗号化 3 方式から，演算が効率的であり安全性評価が十分に議論された点から CRYPTALS-Kyber が標準化方式となった．ディジタル署名では格子暗号から 2 方式が同時に選ばれたが，CRYSTALS-Dilithium の署名長が比較的大きいため，短い署名長を必要とするシステムでは FALCON が利用できる．また，ハッシュ関数署名 SPHINCS+ は高い安全性を実現する方式だが，署名長が大きい点や署名生成の回数に上限があるため，ソフトウェア配布など限定的用途を想定している．

同時に，第 4 ラウンドの方式も発表され，符号暗号の 3 方式 BIKE，HQC，Classic McEliece，同種写像暗号の SIKE が選出された．この符号暗号の 3 方式から暗号化の標準方式が選出される予定である（図 4 下側）．SIKE に関しては 2022 年 8 月に高次元多様体の構造を利用した多項式時間の解読法が提案された．一方，ディジタル署名は再公募されることになり，署名長が短く署名検証が高速な方式を募集していたが，2023 年 7 月に公募条件を満たした 40 方式が公開されている．3 ラウンドまでの情報は報告書 NIST.IR.8413-upd1（https://doi.org/10.6028/NIST.IR.8413-upd1）に詳しい情報がある．

図 4　NIST PQC 標準化方式と第 4 ラウンド方式（2022 年 7 月）

表 3　NIST PQC 標準化スケジュール

2017 年 12 月～2018 年 12 月：第 1 ラウンド評価期間
2019 年 1 月～2020 年 7 月：第 2 ラウンド評価期間
2020 年 7 月～2022 年 6 月：第 3 ラウンド評価期間
2022 年 7 月：NIST PQC 標準方式選出 ※暗号方式第 4 ラウンド開始， ディジタル署名方式再公募
2024 年：NIST PQC 標準方式規格決定
2030 年まで　SP 800-56, FIPS PUB 186-4 を利用可能

最後に，2022 年 7 月に選出された方式は，パブリックコメントを受け付けた後に 2024 年に NIST PQC 標準方式（ML-KEM，ML-DSA，SLH-DSA）として規格化される予定である．現在利用される暗号システムの移行措置として，2030 年までは SP 800-56，FIPS PUB 186-4 で規定されている古典的安全性で 128，192，256 ビットの安全性強度を持つ RSA 暗号・だ円曲線暗号も利用可能としている（表 3）．しかし，2031 年以降に耐量子計算機暗号に移行するための準備期間は限られてお

り，現在普及している RSA 暗号・だ円曲線暗号と耐量子計算機暗号をハイブリッドで利用することも検討されている．

4. おわりに

本稿では，量子計算機の時代でも安全に利用可能となる耐量子計算機暗号の最新動向に関して解説した．特に，耐量子計算機暗号の代表的な方式を説明し，米国標準技術研究所 NIST による PQC 標準化プロジェクトの概要を紹介した．2022 年 7 月に格子暗号 3 方式とハッシュ関数署名 1 方式が NIST PQC 標準暗号として選出され，追加の方式も第 4 ラウンド及び再公募として標準化活動が続いている．今後は，標準化される耐量子計算機暗号への移行に際して生じる問題に対応することが課題となる．

文　献

（1） 高木　剛，暗号と量子コンピュータ，オーム社，東京，2018.
（2） P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comput., vol. 26, no. 5, pp. 1484-1509, 1997.
（3） 7th international workshop on post-quantum cryptography-PQCrypto 2016, T. Takagi, ed., Lect. Notes Comput. Sci., vol. 9606, Springer, 2016.

（2023 年 5 月 31 日受付　2023 年 6 月 19 日最終受付）

高木（たかぎ）　剛（つよし）（正員）

平 5 名大・理・数学卒．平 7 同大学院修士課程了．同年日本電信電話株式会社入社．平 13 ドイツ・ダルムシュタット工科大・助教授．平 29 東大大学院情報理工学系研究科教授．暗号数理に関する研究に従事．Dr.rer.nat．平 25 本会業績賞，第 11 回日本学術振興会賞各受賞．

12 月号小特集予定目次

「そのとき研究の歴史が動いた――画像認識の発展の歴史を振り返って――」

「「共生社会」実現に資する「誰でも参加」の学会・研究会を共につくろう
――「論文作成・発表アクセシビリティガイドライン」の活用――」