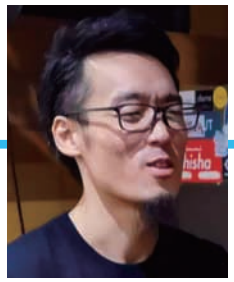
耐量子計算機暗号の現状と標準化動向



日本電信電話株式会社　社会情報研究所　草川（くさがわ）　恵太（けいた）

本稿では宇根氏の記事に引き続き、耐量子計算機暗号（PQC：Post-Quantum Cryptography）とは何か、また、米国の国立標準技術研究所（NIST：National Institute of Standards and Technology）が進めている耐量子計算機暗号の標準化について解説を行う。本号収録の宇根正志氏の記事では、暗号アルゴリズムの移行についての考え方や移行の仕方について書かれているので、参照されたい。

1. 暗号アルゴリズムと安全性

公開鍵暗号の分野において、暗号アルゴリズムが安全であるためには、安全性の根拠となる問題を解くことが現実的には困難でなくてはならない。この問題を解く際の計算ステップ数やコストの見積りに基づいて暗号アルゴリズムの安全性を定めている。

現行のRSA暗号・署名や楕円曲線暗号・署名の安全性は、素因数分解問題や楕円曲線上の離散対数問題と呼ばれる数学的問題の難しさに依拠している。幸い、現行の計算機でこれらの数学的問題を解く場合、最良のアルゴリズムを用いたとしても必要なステップ数やコストが公開鍵や秘密鍵の長さ（鍵長と呼ぶ）の指数・準指数になることが知られている。そのため、十分に鍵長を伸ばすことで、安全性が確保される。

1994年に発表されたP. Shorのアルゴリズムにより、量子計算機を用いた場合、現実的なステップ数（鍵長の多項式で書けるサイズのステップ数）で、さきほどの数学的問題が解けてしまう。そのため、攻撃者が十分に高速な大規模な量子計算機を手にした場合には、現在用いられているRSA暗号・署名や楕円曲線暗号・署名の公開鍵から秘密鍵を求められてしまい、安全性が確保できなくなってしまう。

2. 耐量子計算機暗号

そこで、量子計算機が実現した後の安全な暗号アルゴリズムの移行先として、量子計算機であっても現実的なステップ数では解けないような問題に基づいて構成された暗号、耐量子計算機暗号が有力な候補になる。近年、量子計算機の開発や後述する標準化の進展に伴い、非常に活発に研究・開発が行われている分野である。

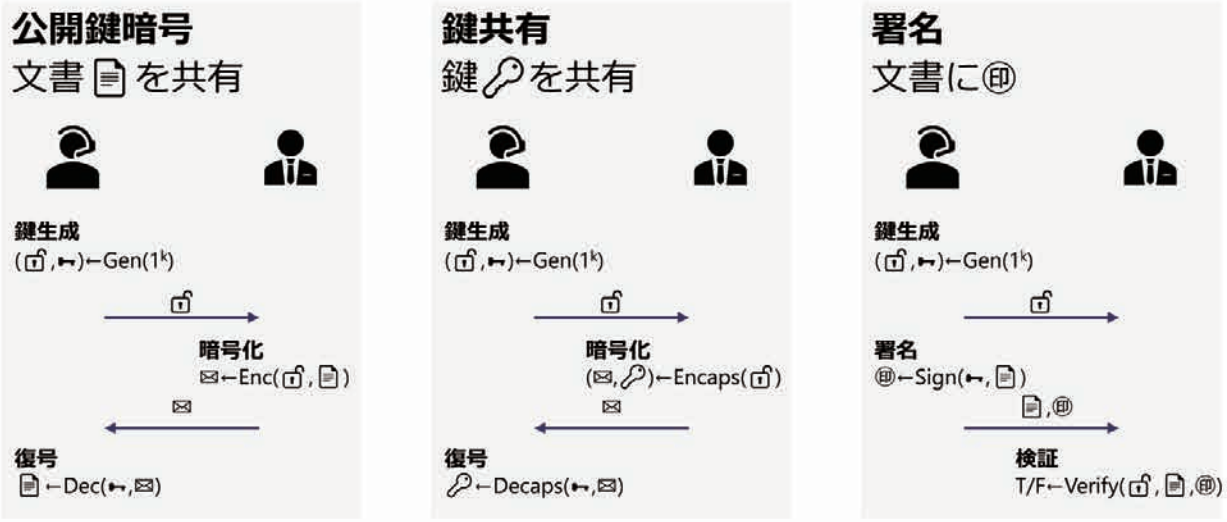
詳細な説明は行わないが、大きく分けて以下のような暗号が耐量子計算機暗号として知られている。

- 符号暗号：誤り訂正符号に関する計算問題を基にした公開鍵暗号・署名。1970年代末に提案された。
- ハッシュベース署名：ハッシュ関数を基にしたデジタル署名。1970年代後半に提案された。
- 多変数多項式暗号：多変数の多項式からなる連立方程式に関する計算問題を基にした公開鍵暗号・署名。1980年代後半に提案された。
- 格子暗号：格子問題を基にした公開鍵暗号・署名。1990年代後半に提案された。
- 同種写像暗号：楕円曲線間の特別な写像である同種写像を基にした公開鍵暗号・署名。1990年代後半に提案された。

この中でもハッシュベースの署名安全性は、ハッシュ関数の一方向性や衝突発見困難性に依拠している。ハッシュ関数の一方向性を破る問題や衝突を発見する問題は量子計算機暗号であっても難しいと考えられており、ハッシュベース署名は非常に強固な耐量子計算機暗号であるといえる。そのため、既に先行して標準化が進んでいる。IETFはXMSS（eXtended Merkle Signature Scheme）と呼ばれるハッシュベース署名をRFC8391で、LMS（Leighton-Micali Signature）と呼ばれるハッシュベース署名をRFC8554として発行した。また、NISTは2020年にこれら2つの方式とその拡張版をNIST SP 800-208に含めており、デジタル署名を既定するFIPS186の追補として位置付けている。これらの方式の利用上の注意点として、実際に運用する際に状態を管理する必要がある点が挙げられる。（状態管理を不要にしたハッシュベース署名もあるが、筆者の知る限りまだ標準化されていない。）

3. NISTの耐量子暗号技術標準化について

NISTは、耐量子計算機暗号の標準化を進めている。現在、NIST SP 800-56A及びSP 800-56Bで公開鍵暗号・鍵共有が、FIPS 186でデジタル署名が規定されている。これらを置き換えるため、量子計算機に対しても安全であるようなデジタル署名と公開鍵暗号・鍵共有を選定し、標



■図1．デジタル署名と公開鍵暗号・鍵共有の模式図

準化するためのプロジェクトを2016年ごろから本格的に開始した（図1）。

この標準化が始まる前にNIST SP800-90Aに掲載されていた擬似乱数生成器Dual_EC_DRBGにバックドアが仕込まれていたのではないかという疑惑が持ち上がった。この方式はNSAが推奨して掲載されたものであるため、NISTの標準化の透明性が問題になった。（のちに、NIST SP800-90AからはDual_EC_DRBGが削除された）

この事件のため、NISTはコミュニティと対話を重ね、透明性を確保しながら標準化を進めている。

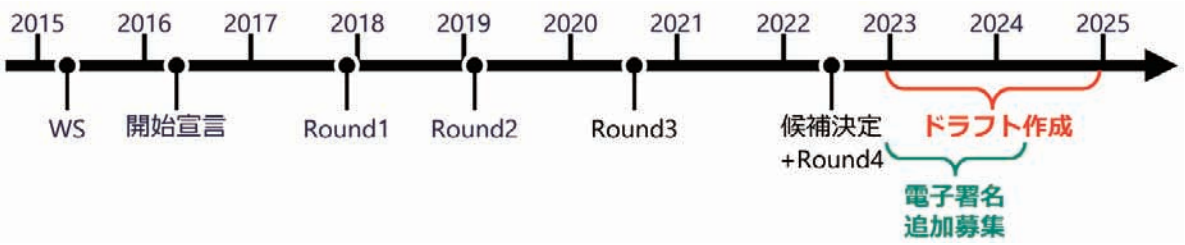
標準化のスケジュールは以下である（図2）

- 2015年4月：ワークショップ開催
- 2016年2月：耐量子暗号技術標準化開始の宣言
- 2016年8月：NISTIR 8105『Report on Post-Quantum Cryptography』の発行
- 2016年8月：募集要項及び選定基準についてのコメント募集
- 2016年12月：受付開始
- 2017年11月：受付締切
- 2017年12月：Round 1の開始
- 2018年4月：第1回耐量子暗号技術標準化会議
- 2019年1月：Round 2の開始
- 2019年8月：第2回耐量子暗号技術標準化会議
- 2020年7月：Round 3の開始
- 2022年5月以降：ドラフト掲載候補の発表、Round 4の開始
- 2022年5月以降：署名の追加募集
- 2022～2024年：ドラフト準備完了

2017年11月締切時点で82件の投稿があった。2017年12月のRound 1開始時点では、書類・形式審査に残った69件の候補が発表された。

2019年1月、Round 2が開始され、暗号化・鍵共有の候補が17件、署名の候補が9件発表された。結果はNISTIR 8240に詳しくまとまっている。

2021年7月、Round 3が開始され、このときに最終候補（Finalists）として暗号化・鍵共有の候補が4件、署名の候



■図2．米国標準技術研究所（NIST）標準化スケジュール

■表．Round 3の標準化候補

技術ベース	公開鍵暗号・鍵共有	電子署名
格子	CRYSTALS-KYBER NTRU SABER FrodoKEM NTRU Prime	CRYSTALS-DILITHIUM FALCON
符号	Classic McEliece BIKE HQC	
多変数多項式		Rainbow GeMSS
同種写像	SIKE	
ハッシュ		SPHINCS+
その他		Picnic

赤：Round3 最終候補
黒：Round3 補欠候補

補が3件残った。また、補欠候補（Alternates）として暗号化・鍵共有の候補が5件、署名の候補が3件残っている。これらの方式とその種類をまとめると表のようになる。どのようにしてこれらの方式を選んだかについてはNISTIR 8309を参照されたい。

当初、2021年の年末～2022年年始にかけてドラフト掲載候補の発表が行われる予定であったが、NISTの事情により延期されている。

Round 3開始以降、様々な動きがあった。特筆すべき事件としては、1）多変数多項式署名に対する新たな攻撃、2）格子暗号に対する特許利用料の主張事件、が挙げられる。

1）多変数多項式署名に対する新たな攻撃の進展

多変数多項式ベースの署名方式であるRainbowに対して、新たな攻撃が提案されている。2020年にW. BeullensがRainbowに対して提案した新たな攻撃[1]により、RainbowチームはRound 3においてパラメータの再設定を余儀なくされた。さらに2022年に、W. BeullensがRainbowに対して新たな攻撃を提案した[2]。パラメータ再設定前のAES128相当と思われていたパラメータに対し、ラップトップPCで3日程度かければ攻撃できることを実証した。改定後のパラメータに対しても既存の攻撃を改良しており、Rainbowチームはまたパラメータの再設定を予告している。

2）格子暗号に対する特許利用料の主張

フランスの研究機関であるCNRSは文献[3]で、NIST耐量子計算機暗号の標準化候補の一部が、CNRSが持つ特許の請求項の範囲内であると主張し、特許利用料を請求する可能性があると発表した。文献[3]では、どの特許が該当するのか不明であるが、関係者の調査によりGaboritとAguilar-Melchorが発明した特許[4]であろうと推測されている。この特許により、格子暗号ではKyber、Saber、NTRU Primeの一部が、符号暗号ではBIKEとHQCが対象となる可能性がある。BIKEとHQCは提案者に発明者を含むため問題はないと思われている。一方、Kyber及びSaberには問題が生ずる可能性がある。特許[4]が有効かどうか、また、KyberやSaberは特許[4]の請求項の範囲なのかどうかの議論・裁判がどのように進むかを注視する必要がある。

4．今後の進展

2022年5月時点でのNISTからの発信をまとめると以下のようになる。

- 暗号化・鍵共有カテゴリの格子暗号3つ（CRYSTALS-KYBER, NTRU, Saber）からは高々1つが選ばれる予定である。
- 署名カテゴリの格子暗号2つ(CRYSTALS-DILITHIUMとFALCON）からは高々1つが選ばれる予定である。
- その他の方式については、各々決定が下される。
- 補欠候補に関してはRound 4を行う。
- 署名の追加募集を行う（現在、2023年1月〆切予定。Round 4とは別トラック）。

2022年5月23日の執筆時点では、まだドラフト掲載候補は決まっておらず、今後の進展を注視する必要がある。

参考文献

[1] Ward Beullens. “Improved Cryptanalysis of UOV and Rainbow”（EUROCRYPT 2021）

[2] Ward Beullens. “Breaking Rainbow Takes a Weekend on a Laptop”（Cryptology ePrint Archive：Report 2022/214）

[3] CNRS Innovation. https://www.cnrsinnovation.com/?lang=en

[4] Philippe Gaborit and Carlos Aguilar-Melchor. “Cryptographic method for communicating confidential information”, 2010