耐量子暗号技術の研究動向

量子計算機の実現が近いとの観測が広まり耐量子暗号の研究が活発になっています．本稿では，耐量子暗号（ポスト量子暗号：Post-Quantum Cryptography）の研究開発の中心的役割を担っている米国国立標準技術研究所（NIST）の耐量子暗号標準化プロジェクトと，それに対するNTTの取り組みおよび独自研究を紹介します．

草川 恵太（くさがわ けいた）
NTTセキュアプラットフォーム研究所

耐量子暗号技術

現在のインターネット上では，プライバシ情報やクレジットカード番号等の機密性の高い情報が多くやり取りされています．通信内容を秘匿するためには，共通鍵暗号や公開鍵暗号が使われています．相手先や送信内容の真正性を確認するために，電子署名やメッセージ認証符号（MAC）といった認証技術が使われています．公開鍵暗号やデジタル署名の中でも現在広く使われているのが，素因数分解問題の困難性に基づく暗号アルゴリズム（RSA暗号，RSA署名など）や離散対数問題の困難性に基づく暗号アルゴリズム（Diffie-Hellman鍵交換，楕円曲線Diffie-Hellman鍵共有，DSAなど）です．

1994年，Peter Williston Shor氏はこの2つの問題を効率良く解く量子コンピュータ用のアルゴリズムを提案しました．大規模かつ安定して計算が行えるような量子コンピュータが完成すると，現在広く用いられている暗号アルゴリズムは安全でなくなります．そのため，量子コンピュータが完成する前に，量子コンピュータを用いても解読や偽造ができないような暗号技術の研究・開発・標準化が盛んになっています．公開鍵暗号技術の中でも，量子コンピュータが苦手とすると考えられている問題を基に暗号アルゴリズムが設計されているものを，耐量子公開鍵暗号技術と呼びます．

耐量子暗号技術の標準化動向

耐量子暗号技術への移行を検討する必要があるかどうかについては，Michele Mosca氏提案の計算式が参考になります．

- x＝今後生成される情報の安全性を保ちたい年数
- y＝耐量子暗号アルゴリズムへの移行（研究開発，標準化，普及）に必要な年数
- z＝大規模量子コンピュータが完成するまでの年数

x＋y＞zであれば，y年後に「x年間安全性を保ちたい」と思って暗号化した暗号文は，x年未満に量子コンピュータによって破られる可能性があります．したがって，現時点でx＋y＞zだと考えられるのであれば，耐量子暗号技術の標準化や耐量子暗号技術への移行を真剣に検討する必要があります．

昨今の量子コンピュータの開発状況からzが現実的な年数になるのではないかと考えられており，各国のいろいろな組織や標準化団体が移行の検討を進めています．

- 日本のCRYPTREC（Cryptography Research and Evaluation Committees）*は，2014年ごろに「格子問題等の困難性に関する調査」として耐量子暗号技術の調査報告を行っています．
- 米国国立標準技術研究所（NIST）は，2015年春ごろからワークショップを開催し始め，2016年には耐量子公開鍵暗号技術の標準化活動を行うことを宣言しました．
- 米国国家安全保障局（NSA）は，2015年8月，機密情報の保護のために用いる暗号アルゴリズムのリストSuite Bについて，耐量子暗号技術への移行が将来的に行われることを表明しました．
- 欧州電気通信標準化機構（ETSI）は2013年ごろから量子暗号と耐量子暗号技術のワークショップを毎年開催しています．
- 国際標準化機構（ISO）と国際電

＊CRYPTREC：電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクト．

気標準会議（IEC）は2015年ごろから耐量子暗号技術に関する議論の時間を設けています．

・IETFでも，耐量子署名のプロジェクトが進んでおり，RFCとして公開され始めています（RFC8391: XMSS: eXtended Merkle Signature Schemeなど）．

これらの動きの中でも世界の暗号技術標準に強い影響力を持つNISTの耐量子暗号技術標準化プロジェクトを紹介します．

NISTの耐量子暗号技術標準化プロジェクト

NISTの耐量子暗号技術標準化プロジェクトは2016年ごろから本格的に開始しました．デジタル署名，公開鍵暗号，鍵共有の3つのカテゴリの暗号アルゴリズムを選定し標準化するためのプロジェクトです．NISTのスケジュールは以下のとおりです（**図**）．

・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：募集要項およ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：書類および形式審査を行い，Round 1の開始
・2018年4月：第1回耐量子暗号技術標準化会議
・2018～2019年：Round 2の開始
・2019年8月：第2回耐量子暗号技術標準化会議の予定
・2020～2021年：Round 3の開始またはアルゴリズム選定
・2022～2024年：ドラフト準備完了

2017年11月締切時点では82の投稿があり，署名の提案が23件，暗号化・鍵共有の提案が59件でした．その後，1カ月ほど書類や形式の審査を行い，2017年12月にRound 1が開始されました．このとき，69件が残りました．のちに5件取り下げがあり，現時点では64件が残っています．署名の提案が19件，暗号化・鍵共有の提案が45件残っています．

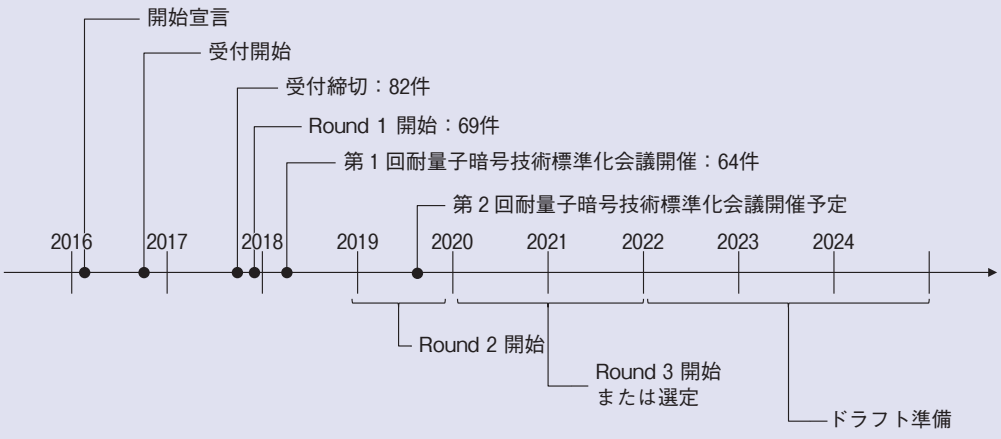

図　タイムライン

すでに書いたとおり，書類および形式を審査した結果がRound 1の候補である69件です．

そのため，Round 1に進んだからといって，安全であるとは限りません．

Round 1の候補が公開された直後から，NISTのpqcメーリングリストにおいて，各方式の安全性について激しい議論が交わされました．

その中でも，以下のように実際に破れることが示された例が多数あります．

・Guess Again（その他・暗号）
・RaCoSS（符号・署名）
・RVB（その他・暗号）→取り下げ
・HK17（その他・暗号）→取り下げ
・CFPKM（多変数多項式・暗号）
・SRTPI（多変数多項式・暗号）→取り下げ
・Edon-K（符号・暗号）→取り下げ
・Comact LWE（格子・暗号）
・WalnutDSA（その他・暗号）
・RankSign（符号・署名）→取り下げ

今後も，Round 2に進むまでに安全性評価手法が改良されることが想定されるため，注視が必要です．

NTTの取り組み

NTTでは，NISTの耐量子暗号標準化活動には独自のアルゴリズムを提出していません．

しかし，安全性強化手法の提案や第三者的立場での安全性評価というかたちで参加し，適切なアルゴリズムが選ばれるよう協力しています．

またNISTの耐量子暗号標準化は耐量子公開鍵暗号技術のみを対象にしていますが，NTTでは独自に耐量子共通鍵暗号技術についても研究を進めています．

■安全性強化手法

実際の通信状況下で安全な暗号通信を行う場合，公開鍵暗号はメッセージを秘匿するだけでなく，メッセージの改ざんを防止する等のより強い安全性が必要です．専門的には，これをCCA安全性と呼びます．現在では，CCA安全性を持つことが現実に使用する公開鍵暗号のための必須の条件とされています．

CCA安全性を持たない公開鍵暗号をCCA安全性を持つ公開鍵暗号へと強化する手法は古くから研究されてきましたが，2010年ごろからこれらの手法が量子コンピュータを利用した攻撃に対しても安全であるかどうかが研究され始めました．

その結果，これらの手法は効率性を落とせば，量子コンピュータに対しても有効であることが証明されました．

しかし，効率性を犠牲にしないで量子コンピュータに対しても有効であるような安全性強化手法は知られていませんでした．

そこでNTTでは，CCA安全性を持たない耐量子公開鍵暗号を，CCA安全性を持つ耐量子公開鍵暗号へ変換し，安全性を強化する新たな手法を開発しました[(1)]．

これにより，世界最高水準の耐量子公開鍵暗号方式を高効率に構成できます．また，今回の手法は汎用性が高く，さまざまな既存の耐量子公開鍵暗号に対しても適用可能です．NIST標準化候補暗号方式でも，少なくとも7件に適用可能であることが分かっています．

この技術に基づく耐量子公開鍵暗号を用いることで，量子コンピュータ実現後の時代においても，既存方法と同程度の負荷で暗号通信が可能になります．

■外部からの安全性評価

69候補の中にGiophantusという暗号アルゴリズムがあります．

これは，もともとはIECという名前で論文発表されていました．IECも安全性証明を持っており，ある問題が難しいということに安全性が依拠しています．また，ある問題が難しいというためには問題のパラメータが大きいことが必要となります．しかし，IECは鍵サイズや暗号文長が短くなるように設計されていたため，基にしている問

題も相当パラメータが小さいことが課題になっていました．

私たちは，さらに小さなパラメータの問題を解いた場合でも安全性が破れるような新しい攻撃手法を考案しました[(2)]．今回の攻撃手法を用いて解読実験を行った結果，デスクトップPCでも30～40秒程度で解読が行えることが分かりました．今回の研究の結果，NISTへの投稿版であるGiophantusではパラメータが大幅に設定し直されています．

■耐量子共通鍵暗号技術

⑴　安全性評価手法

共通鍵暗号に対する汎用的な量子アルゴリズムは今のところ知られていません．そのため，データベース探索に用いるGroverのアルゴリズムを適用した攻撃が，最良のものとして知られています．そこで共通鍵暗号の内部まで詳しく解析することで，Groverアルゴリズムを超えるような量子攻撃手法を考案し，安全性評価を行っています．NTTでは，中間者一致攻撃と量子アルゴリズムを組み合わせることで，世界初の成果や既存の研究よりも優れた成果を得ることに成功しています[(3), (4)]．

また，一部の共通鍵暗号やMACについては，攻撃者が暗号化アルゴリズムやMACアルゴリズムに量子的にアクセスできる場合に安全性が破れてしまうことが知られています．NTTでもそのような攻撃を研究し，一部の共通鍵暗号を量子関連鍵攻撃で破れることを示しています[(5)]．

⑵　安全性証明手法

前述のとおり，共通鍵暗号技術が，量子的にアクセスするような攻撃者を考えても安全かどうかを判定・証明することは非常に重要です．NTTでは，量子クエリができる攻撃者を考えたときであっても，ハッシュ関数の耐量子安全性を証明する技法を開発しています[(6)]．

今後の展開

安全性強化手法や安全性評価手法を取りそろえ，量子コンピュータの完成後も安心・安全な暗号通信技術の開発・実用化に向けた検討を進めていく予定です．

■参考文献

⑴ T. Saito, K. Xagawa, and T. Yamakawa：“Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model,” EUROCRYPT 2018 Part III, LNCS, Vol.10822, pp.520-551, 2018.

⑵ K. Xagawa：“Practical Cryptanalysis of a Public-key Encryption Scheme Based on Non-linear Indeterminate Equations at SAC 2017,” PQCrypto 2018, LNCS, Vol.10786, pp.142-161, 2018.

⑶ A. Hosoyamada and Y. Sasaki：“Cryptanalysis Against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations,” CT-RSA 2018, LNCS, Vol.10808, pp.198-218, 2018.

⑷ A. Hosoyamada and Y. Sasaki：“Quantum Demiric-Selçuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions,” SCN 2018, LNCS, Vol.11035, pp.386-403, 2018.

⑸ A. Hosoyamada and K. Aoki：“On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers,” IWSEC 2017, LNCS, Vol.10418, pp.3-18, 2017.

⑹ A. Hosoyamada and K. Yasuda：“Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions,” Asiacrypt 2018 Part I, LNCS, Vol.11272, pp.275-304, 2018.

草川 恵太

NTTセキュアプラットフォーム研究所では，暗号技術の研究開発を通じて，安心・安全なサービスの実現をめざします．

◆問い合わせ先

NTTセキュアプラットフォーム研究所
データセキュリティプロジェクト
セキュリティ基盤研究グループ
TEL　0422-59-3321
FAX　0422-59-4015
E-mail　keita.xagawa.zv@hco.ntt.co.jp