量子コンピュータでも解読が困難な暗号技術「耐量子計算機暗号」の動向

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
篠原（しのはら）　直行（なおゆき）

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
盛合（もりあい）　志帆（し　ほ）

1. はじめに

暗号技術は現代社会を支える身近な基盤技術であり、例えばネットショッピングやカードバンキング、交通系ICカード、無線LANなどで日常的に利用されている。現在、広く使用されている代表的な公開鍵暗号としてRSA暗号や楕円曲線暗号が挙げられる。近年、量子計算機の開発が活発に進められており、様々な分野への応用が期待されているが、十分な計算能力を持つ量子計算機が登場することによってRSA暗号や楕円曲線暗号の安全性が大きく低下してしまうことが問題となっている。その対策として、現在使われている計算機のみならず、量子計算機を利用しても安全性が保たれる暗号技術「耐量子計算機暗号」（Post-Quantum Cryptography：PQC）の開発及び標準化が進められている。本稿では、その世界的な動向について紹介する。

2. 現在利用されている公開鍵暗号方式の安全性に対する量子計算機の影響

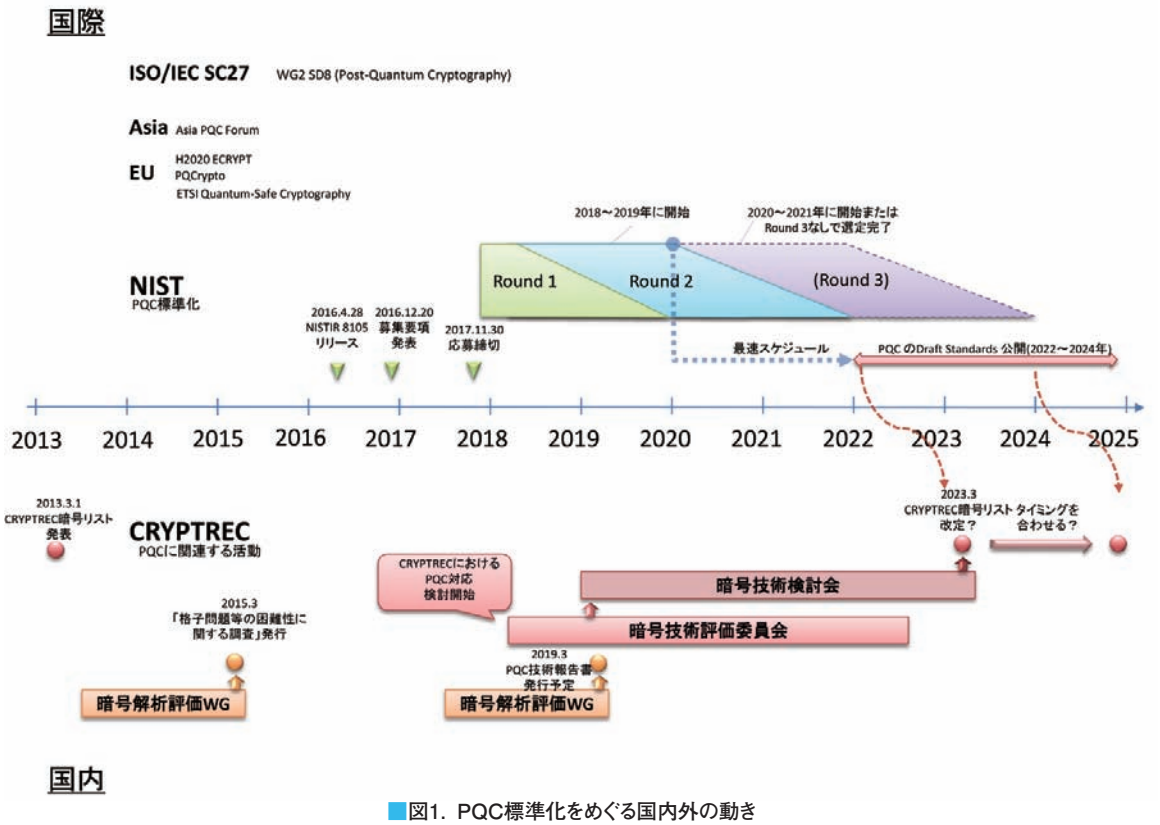
現在使用されている、もしくは開発が進められている公開鍵暗号方式は、数学的な問題を解く計算の困難性を根拠にして、その安全性を保証している。例えば、最も広く利用されている公開鍵暗号方式であるRSA暗号では、同じビット長の大きな二つの素数が秘密鍵として使用され、その積である合成数が公開鍵として公開される。したがって、誰でも入手可能なその合成数が素因数分解されてしまうと、その秘密鍵が取得され、その鍵を使用するRSA暗号は解読されてしまう。もう一つの代表的な公開鍵暗号方式である楕円曲線暗号の安全性は、楕円曲線上の離散対数問題を解く計算の困難性に関連付けられている。即ち、楕円曲線上の離散対数問題を解くことで楕円曲線暗号の秘密鍵が入手されてしまう。量子計算機の開発が進むことでRSA暗号や楕円曲線暗号の安全性が低下する理由は、1994年にShorにより発表された量子計算機用のアルゴリズムがあり、それを使用することで整数の素因数分解や離散対数問題を解く計算を高速に実行できるようになるからである。

量子計算機上でShorのアルゴリズムを利用した素因数分解の解読実験におけるこれまでの世界記録は21（=3×7）の素因数分解であるため、現時点ではまだ量子計算機はRSA暗号や楕円曲線暗号に対する深刻な脅威とはなっていない。しかし、2016年に発行された米国国立標準技術研究所（National Institute of Standards and Technology：NIST）のInternal Report 8105において、スケーラブルな量子計算機が実現される時期は不明であるが、現在使われているRSA-2048を素因数分解できる量子計算機が2030年までに実現される可能性があると量子計算機の研究者らが見積もっていると記載された。このような背景により、量子計算機に対しても、現在使用されている計算機に対しても、安全性を確保できる暗号技術が必要とされ、耐量子計算機暗号PQCとして急速に開発・標準化に向けた取組みが活発化してきた。

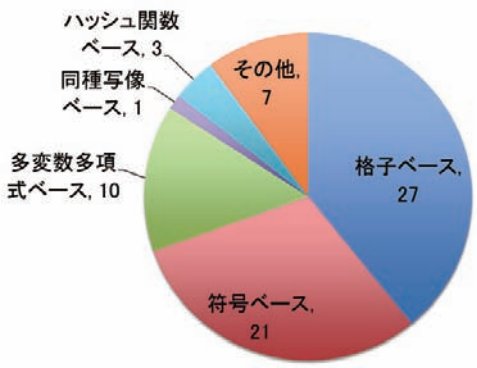
3. 耐量子計算機暗号の開発及び標準化の動向

現在使用されている暗号技術の多くは、提案されてから広く普及するまでに20年近く必要としてきた。したがって、耐量子計算機暗号が2030年までに使用できるようになるためには、耐量子計算機暗号の開発及び標準化に向けた準備は2010年ごろから開始されている必要がある。耐量子計算機暗号の研究開発の歴史は古いが、奇しくも、耐量子計算機暗号にフォーカスを当てた学術的国際会議PQCryptoの第1回が開催されたのは2006年であった。PQCryptoの開催は2018年で9回目を迎えており、耐量子計算機暗号の開発は適切な時期に本格化したと言ってよいであろう。

次に、PQC標準化に向けた国内外の動きについて紹介する（**図1**参照）。米国では、2015年に米国国家安全保障局（National Security Agency：NSA）が耐量子計算機暗号への移行計画を発表した。さらに、NISTが耐量子計算機



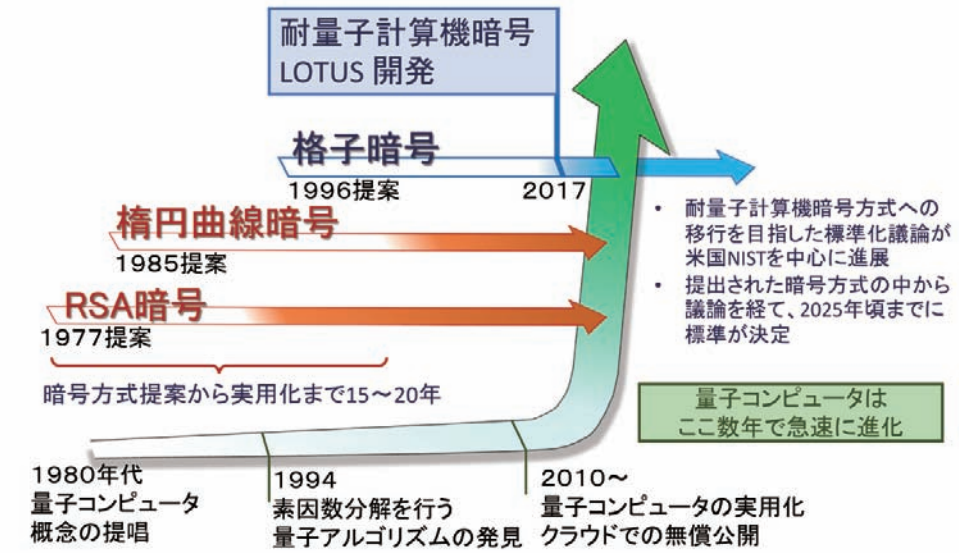
■図1. PQC標準化をめぐる国内外の動き



■図2. NIST PQC標準化における69候補方式
（ベースとなる技術で分類）

暗号の公募を2016年から開始し、これに対して世界中から2017年11月末の締め切りまでに82件の暗号方式が提案された。このうちの69件が書類選考を通過し、その後、現在までに5件の暗号方式が取り下げられている（図2参照）。NISTは候補となる暗号方式の安全性や実装性能等を評価し、2022～2024年には耐量子計算機暗号の標準ドラフトを公開する予定となっている。欧州では欧州電気通信標準化機構（European Telecommunications Standards Institute：ETSI）が耐量子計算機暗号の動向調査などを行っている。また、国際標準化機構（International Organization for Standardization：ISO）及び国際電気標準会議（International Electrotechnical Commission：IEC）においても、ISO/IEC JTC 1/SC27にて標準化に向けた議論が行われている。

国内でも耐量子計算機暗号の標準化に向けた取組みが進められている。総務省、経済産業省、国立研究開発法人情報通信研究機構（NICT）、独立行政法人情報処理推進機構（IPA）の4者で運営されるCRYPTREC（Cryptography Research and Evaluation Committees）プロジェクトでは、各府省が情報システム調達のために参照すべき暗号のリスト（電子政府推奨暗号リスト）の安全性の評価及び監視を行い、暗号技術の適切な実装法及び運用法の調査及び検討を実施している。このプロジェクトでは、耐量子計算機暗号の標準化を見据えて、2014年度から耐量子計算機暗号の有力な候補の一つである格子に基づく暗号技術及びその安全性に関する数学的な問題（格子問題）について研究動向調査を実施し、技術報告書としてまとめたものを公開している。格子に基づく暗号技術の他にも耐量子計算機暗号の有力な候補がいくつかあり、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術等



■図3. NICTで開発した耐量子計算機暗号LOTUS

がその代表として挙げられる。CRYPTRECでは、耐量子計算機暗号のこれら4種類の暗号技術について2017年度から調査を行っており、調査結果をまとめたものを技術報告書として2019年に公開する予定である。

4. NICTにおける耐量子計算機暗号LOTUSの開発

NICTでは暗号技術の開発及びその安全性評価に関する研究を長年にわたり実施している。耐量子計算機暗号については、格子に基づく暗号技術に分類される新公開鍵暗号方式LOTUS（ロータス）を開発し、NISTの耐量子計算機暗号の標準化プロジェクトへ2017年に提案した（図3参照）。本方式は書類選考を通過し、現時点まで大きな安全性上の欠点は指摘されておらず、標準化プロジェクトにおける候補として評価が続けられている。

LOTUSは、量子計算機を利用しても解読が困難な性質を持つだけではなく、ブラウザやデータベースなどに組み込み可能な暗号学的な汎用性を持つ。暗号学的な汎用性とは、複数の暗号技術を組み合わせて構成した暗号技術全体の安全性に関する概念である。暗号技術はまず単体として安全でなければならない。そして、暗号技術を実際に使用する場合には、他の暗号技術と組み合わせた複合体として使用することがあり、その組み合わせ方によって複合体に脆弱性が生じないようにしなければならない。暗号学的な汎用性を持たない暗号方式を組み合わせた場合は、各暗号方式の安全性を証明した後で、その複合体全体の安全性も証明する必要がある。

この性質を持たない暗号方式を使う場合、組み合わせ方を間違えるとそこに脆弱性（攻撃者が付け入る余地）が生まれてしまい、システム全体が破たんする危険性があった。システム全体の安全性を保証するためには、暗号一つ一つの安全性を証明した後に、全体の安全性を証明するという二段階の手順を踏む。しかし、複雑なシステムでは専門家が何日もかけて検証しなければならず、また、その複雑さゆえに誤りが発生しやすい等の問題点があった。暗号を設計する段階で、汎用性という性質を持たせることで、このような危険を避けることができる。汎用性を持った暗号方式同士を組み合わせたシステムは、安全であることが数学的に証明されているため、全体の安全性を証明するステップが省略可能となる。今回NICTで開発したLOTUSでは、ベースとなる格子暗号に対して、復号の際に暗号文の構造をチェックする機構を追加することで、データ破損への耐性を持たせた。このチェック機構により、他の暗号方式と組み合わせ可能な汎用性を持つことが数学的に証明されるため、開発した暗号を基に様々なシステムを構築し、社会の様々な場面で活用することができる。

さらに、格子に基づく暗号技術の安全性評価手法を同時に開発し、暗号の長期利用に適したパラメータの設定が可能になった。この安全性評価手法は、他の格子に基づく暗号技術を評価することも可能であるため、現在、NIST での標準化プロジェクトに多数提案されている候補方式を統一的な基準で評価することにより、公平な安全性評価に貢献できると考えている。