耐量子計算機暗号の動向2020

本稿は2016年6月にIIR Vol.31フォーカスリサーチで取り上げた「1.4.3 耐量子暗号の動向」[*1]について2020年11月の時点でのアップデートに関して取り上げます。前回の報告では日本語訳として「耐量子暗号」という用語をあてて紹介しましたが、技術用語としてより正確性を期するために「耐量子計算機暗号」と呼ばれることが一般的となっており[*2]、本報告でもこの用語を使用することとします。

2.1 NISTコンペティション概要

前回報告では、有力なアルゴリズムとして以下の4つの数学的背景を持つカテゴリを紹介しました(IIR31 表-2 耐量子暗号の分類)。

- 格子暗号
- 符号ベース暗号
- 多変数公開鍵暗号
- ハッシュベース署名

これらのうちNISTコンペティション[*3]の最新報告でも分類で使われているカテゴリは、上記4つに加え、現在はIsogeny (同種写像)と呼ばれる暗号方式も追加されています。Isogenyに関しては2018年11月に大阪大学で開催されたECC2018[*4]でも多くの時間を割いて議論されており、Chloe Martindaleによる発表資料は美しく観ているだけでも楽しくなる図面が並んでいます。

ECDHなどの楕円曲線暗号では、公開パラメータとしてある固定された楕円曲線上の点に加法演算をうまく定義することで群構造を作り、楕円曲線上の離散対数問題という特性を用いてアルゴリズムを構成しています。ここでの安全性は点PをK回加算した点QをQ=kPとしたときPとQ=kPからkを求めることが難しいことに依拠しています。Isogenyは楕円曲線から楕円曲線への写像の一種であり、楕円曲線EとE'=Φ(E)から写像 Φ を求めることが困難であることを用いてDiffie-Hellman鍵共有法と同様の数学的構造を持つ鍵共有方法が提案されています。

2016年2月に福岡で開催された国際会議PQCrypt2016の招待講演で、Dustin MoodyによってNISTからのアナウンスがあり、耐量子計算機暗号のコンペションが開催されることになりました[*5]。2016年末には応募要項が固まり、2017年11月の期限までに82のアルゴリズムが投稿されました。書類審査を経て69のアルゴリズムが第1ラウンドの候補として審査が開始されました[*6]。更に2018年4月には第1回NIST PQC Standardization workshopが開催され集中議論が進められた後、2019年1月にはNISTIR8240[*7]と共に26のアルゴリズムが第2ラウンドに進んだことが公表されました。

2019年8月にはCRYPTO2019と併設して第2回のNIST PQC Standardization workshopが開催され、2020年7月22日に7つのファイナリストと8つの代替候補(alternates)が第3ラ

＊1 Internet Infrastructure Review vol.31「1.4.3耐量子暗号の動向」(https://www.iij.ad.jp/dev/report/iir/031/01_04.html)。
＊2 森北出版より同名の書籍が発刊されている(https://www.morikita.co.jp/books/book/3503)。
＊3 NIST Post-Quantum Cryptography(https://csrc.nist.gov/Projects/Post-Quantum-Cryptography)。
＊4 ECC18(https://cy2sec.comm.eng.osaka-u.ac.jp/ecc2018/program.html)。Chloe MartindaleによるCSIDHに関する発表スライド、CSIDH:An Efficient Post-Quantum Commutative Group Action(https://cy2sec.comm.eng.osaka-u.ac.jp/ecc2018/slide/slide_program/1121-3%20CSIDH%20Martindale.pdf)。
＊5 Dustin Moody, Post Quantum Cryptography Standardization: Announcement and outline of NIST's Call for Submissions, PQCrypto2016 (https://csrc.nist.gov/presentations/2016/announcement-and-outline-of-nist-s-call-for-submis)、(https://www.youtube.com/watch?v=nfLAVybabMs)。
＊6 Dustin Moody, The ship has sailed: the NIST Post-Quantum Cryptography competition, ASIACRYPT2017 invited talk(https://csrc.nist.gov/presentations/2017/the-ship-has-sailed-the-nist-post-quantum-cryptog)、(https://www.youtube.com/watch?v=3doS6joRYTE)。
＊7 NISTIR 8240, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process(https://csrc.nist.gov/publications/detail/nistir/8240/final)。

ウンドに進んだことがアナウンスされました。詳しい選定状況はNISTIR8309にてレポートされています[*8]。この辺りの背景はDustin本人による回顧録として2020年12月に公開されています[*9]。

表-1はDustinによる最新の発表資料[*10][*11]などから作成したファイナリストと代替候補のリストとなります(括弧つきで赤文字で示されたものは代替候補)。

ファイナリスト7つのうち署名は3方式(格子暗号2、多変数公開鍵暗号1)、KEM (鍵カプセル化メカニズム)は4方式(格子暗号3、符号ベース暗号1)となっています。それぞれのアルゴリズムは第3ラウンドに入った段階で若干の修正が認められており、第3ラウンドのページ[*12]に仕様やWebサイトに関する情報が記載されています。またUpdateについてもPDFが提供されています[*13]。

本コンペティションの今後の予定は以下となっています。既に開始されている第3ラウンドは12～18ヵ月の期間で完了することが予定されており、第3ラウンド終了時には、現在格子暗号にカテゴライズされている複数のファイナリストは署名・KEMでそれぞれ1つに絞るよう選定が行われます。第3回ワークショップは2021年春または夏に開催、標準化文書は2022～2023年にドラフト、2024年には標準化文書が発行される、というスケジュールで進められます。

Horizon 2020の予算の枠組みでプロジェクト化されたPQCRYPTO projectがあります[*14]。D5.2 Standardization: Final report によると同プロジェクトからNISTコンペティションへの貢献が大きいことが分かります。PQCRYPTO projectから応募されたアルゴリズムは、第3ラウンドに進んだ15のアルゴリズムのうち11方式を占めるなど大きな存在感を持っています。

2.2 NIST策定の暗号アルゴリズムとその影響

NISTは米国政府における調達要件にも大きく関わるような各種仕様及びガイドラインを作成しています。NISTが扱う技術領域は非常に広範囲ですが、主に我々が目にするところでは情報セキュリティに関するあらゆるガイドラインが多く取り上げられています。例えばSP800-63で規定されている、パスワードに関連するドキュメント類は多くの技術者の目に触れるところとなり、パスワードに関する考え方に関して議論のト

カテゴリ／方式	署名	KEM
格子暗号	CRYSTALS-DILITHIUM、FALCON	CRYSTALS-KYBER、NTRU、SABER(FrodoKEM、NTRU Prime)
符号ベース暗号	なし	Classic McEliece(BIKE、HQC)
多変数公開鍵暗号	Rainbow(GeMSS)	なし
ハッシュベース署名	(Picnic、SPHINCS+)	N/A
Isogeny	なし	(SIKE)

表-1 ファイナリストと代替候補のリスト

*8 NISTIR 8309, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process(https://csrc.nist.gov/publications/detail/nistir/8309/final)。
*9 Dustin Moody, The Future Is Now: Spreading the Word About Post-Quantum Cryptography, December 2, 2020(https://www.nist.gov/blogs/taking-measure/future-now-spreading-word-about-post-quantum-cryptography)。
*10 NIST PQC Standardization Update - Round 2 and Beyond, September 23, 2020(https://csrc.nist.gov/Presentations/2020/pqc-update-round-2-and-beyond)。
*11 NIST PQC Standardization Update - Round 2 and Beyond, (https://www.nccoe.nist.gov/file/3-pqc-nccoepdf)。
*12 Post-Quantum Cryptography Round 3 Submissions(https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions)。
*13 History of PQC Standardization Round 3 Updates (https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/history-pqc-round-3-updates.pdf)。
*14 PQCRYPTO project(https://pqcrypto.eu.org/)、(https://cordis.europa.eu/project/id/645622)。D5.2 Standardization:Final report(https://pqcrypto.eu.org/deliverables/d5.2-final.pdf)。

リガーとなりました。定期的にパスワード変更することの是非や2要素認証もしくは多要素認証におけるSMSメッセージを使った認証方式の是非に関して、有益なディスカッションが日本でも行われました。

また、暗号アルゴリズムの利用そのものやその利用に携わる技術者においては、NISTから発行されるFIPSやSPが世界的にもリードし続けていることを知る人も多いと思います。現在広く利用されているハッシュ関数の仕様群SHA-2もNISTによる策定が行われている一方で、米国政府の息がかかっていることからバックドアが存在するのではないかという懸念は1970年代に策定されたDES発行の頃から指摘されています。そのため最近ではNIST Curveと呼ばれる楕円曲線暗号方式に使われる公開パラメータにおける同様の懸念から、草の根活動としてのIETFで標準化された暗号方式を好む人たちが一定量いることも事実です。ただし暗号資産で利用されているブロックチェーンなどで実装されているハッシュ関数アルゴリズムはNISTに策定されたものも多く含まれています。暗号技術に精通していないエンジニアが独自に設計・実装したことで、暗号資産そのものの存続に関わる問題に発展した事例もあり、SHA-2は十分に精査された枯れた技術で安全であると認識されているようにも見受けられます。

2.3 耐量子計算機暗号における安全性の考え方

RSA暗号の安全性は素因数分解の困難性に依存していますが、例えば100程度までの合成数であれば誰でも簡単に素因数分解できます（例えば2、3、5、7、11、13くらいで割れるかを確認すれば良い）。RSA暗号は計算量的安全性に基づくため、ある程度大きな素数を用いなければ安全に利用することはできません。現在、1024ビット×2=2048ビット以上の合成数Nを用いることが推奨されていますが、この鍵長に関するコンセンサスは時代と共に変化してきました。この事例のように、暗号アルゴリズムそのものの安全性に依拠するパラメータ設定はとても重要となります。RSA暗号は現在も安全と認識されていますが、それは十分鍵長を保っているからであり、この前提のもと正しく実装されることで初めて安全に利用することができます。

耐量子計算機暗号においても同じようにパラメータ設定の課題があります。暗号方式そのものが安全と認識されていても、例えば鍵長に類する情報などがどのようなデータを利用すれば安全になるかという検討が必要です。こうした背景から、暗号アルゴリズム、特に現在利用されている計算量安全性に基づく公開鍵暗号方式は、鍵長が重要な事項となります。これと同様に、今後策定される耐量子計算機暗号アルゴリズムにおいても各種パラメータをどのように設定して安全性を確保するかが重要となります。そのため、一部のカテゴリに関しては現在の計算機環境において利用に適しているかどうかを判断するために解読コンペティションが開かれており、最新の攻撃手法を共有することで研究コミュニティを盛り上げる・維持するケースも見受けられます。

耐量子計算機暗号のうち多変数公開鍵暗号としてカテゴライズされる分野においては2015年からコンペティションが開催されており、このくらいのパラメータで十分と思われていた暗号アルゴリズムが急激な研究の進展によって我々が考えていたよりも安全でなくなった事例も多く見られます。例えばCRYPTO2019に併催された第2回PQC Standardization

Conference[*15]においてJintai Ding[*16]による講演で大きくパラメータ変更見直しが必要となりました。

2.4 ビットセキュリティ

耐量子計算機暗号とは対照的に、現在多く利用されている暗号アルゴリズムは古典的アルゴリズムと呼ばれています。古典的アルゴリズムにおいては、各種パラメータを選択することにより、あるビットセキュリティを確保することで安全性を担保するという考え方が一般的です。このビットセキュリティという考え方は共通鍵暗号やハッシュ関数などにおいては理解しやすい概念となっており、過去のIIRレポートにおいて暗号危殆化や等価安全性に関する解説を行っています[*17]。

例えば広く使われているAES-128と呼ばれる共通鍵暗号アルゴリズムでは128ビット長の鍵が使われており、復号のための鍵を同定するには2^{128}の施行を必要とするため、128ビット安全もしくは128ビットセキュリティを確保しているといわれています。ビットセキュリティの考え方は公開鍵暗号アルゴリズムにも適用することができ、ある鍵パラメータを用いた各種暗号アルゴリズムが、どの程度の安全性を確保できているかを比較対照できるようになっています。このような鍵長に関する対応表で有名なものとしてNISTによるSP 800-131A[*18]がよく取り上げられますが、同じRSA鍵長を用いてもステークホルダーによってどのくらいビットセキュリティと見なせるか少々ブレがあるのが面白いところです(例えば、本レポートのVol.8 1.4.1 表-1を参照)。

このように策定された団体や組織の思惑に依存して強度が変化する同じようなケースが、過去にも耐量子計算機暗号に関するレポートで見られました。前回の耐量子計算機暗号に関するレポートを執筆した際に紹介したGroverのアルゴリズムは、nビットセキュリティを確保する共通鍵暗号方式においてその鍵長の半分の強さしか持たないことが示されています。しかしステークホルダーによっては共通鍵暗号方式はすべてゼロビットセキュリティに低下するという判断を下しているレポートも見受けられました。現在は共通鍵暗号において、解読に必要な計算量2^nの肩に乗ったnの値が半減するという考え方が広く受け入れられています。NISTによりKEMやデジタル署名などの公開鍵暗号方式のコンペティションが行われているため、耐量子計算機暗号としての共通鍵暗号方式がフォーカスされることは少ないですが、いくつかの独立したペーパーが発行されており興味深い結果が得られています。例えば現在一般的に使われているAES暗号に対して量子計算機がどのくらい脅威となるかに関する文献があります[*19]。古典計算機でも量子計算機でも大きなセキュリティマージンを持っているとの解析結果を主張していますが、その見通しや判断は読者に任せることとします。

2.5 量子暗号と耐量子計算機暗号について

量子暗号と耐量子計算機暗号という2つのキーワードはその意味や背景が異なりますが、一般の方から見ると混乱を引き起こしているような記事が見受けられます。前者としては例えばQKDとして知られる量子通信における鍵配送などがありますが、耐量子計算機暗号とは異なる概念です。本稿で扱う技術対象は後者の耐量子計算機暗号と呼ばれる分野に関する話題であり、量子通信など量子力学を直接的に扱う技術的話題は行いません。

*15 Second PQC Standardization Conference(https://csrc.nist.gov/events/2019/second-pqc-standardization-conference)。
*16 Jintai Ding, New Attacks on Lifted Unbalanced Oil Vinegar(https://csrc.nist.gov/Presentations/2019/new-attacks-on-lifted-unbalanced-oil-vinegar)。
*17 暗号危殆化の事例や、ビット安全性、等価安全性に関する解説は本レポートのVol.8(https://www.iij.ad.jp/dev/report/iir/pdf/iir_vol08.pdf)の「1.4.1 暗号アルゴリズムの2010年問題」にて紹介している。
*18 NIST Special Publication 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019.(https://doi.org/10.6028/NIST.SP.800-131Ar2)。
*19 Xavier Bonnetain et.al, Quantum Security Analysis of AES(https://tosc.iacr.org/index.php/ToSC/article/view/8314)。FSE2020にて発表(https://fse.iacr.org/2020/program.php)。

耐量子計算機暗号を議論する際に用いられる仮定は、量子計算機が今後実装され普及した際に現在使われている暗号アルゴリズムがどのような影響を及ぼすかという点が焦点となっています。そのため読者の中には耐量子計算機暗号が既にブラウザなどで実装されていることに非常に大きな驚きをもって捉えられるでしょう[*20]。報道などにより、既に量子計算機が商用で流通していると伝えられると、そのような量子計算機上で動作する暗号アルゴリズムが実装されていると勘違いされるかもしれません。しかし我々が扱うモデルは、量子計算機を持つ攻撃者のみが量子計算機を使い莫大な計算量を持っている、一方で大多数の方々が古典的計算機で使って利用しているという前提で攻撃が行われると理解していただければと思います。

2.6 耐量子計算機暗号の意味するところ

耐量子計算機暗号の定義は明瞭ではなく、ある提案アルゴリズムが耐量子計算機暗号かどうかの線引きは非常に難しいところではありますが、過去の一般的な暗号アルゴリズムで使われているような計算量的安全性の仮定ではないところに安全性を置いているアルゴリズムと考えれば良いということになります。つまり、古典的な計算機上でも実装可能なアルゴリズムが新たに取って替わると考えることができます。

そのためかなり昔に遡り、例えば1970年代に提案されている暗号アルゴリズムであっても現在それらが再評価され、耐量子計算機暗号としてフィーチャーされているものもあります。一方、ここ数年で急速に研究が進んだものもあり、暗号研究業界において1つの大きなトピックとしても認識されています。

暗号研究が進むトリガーとして、今まで普通に使われていたアルゴリズムが使えなくなるような攻撃が見つかる（これを暗号アルゴリズムの危殆化と呼ぶ）、あるいは今後使えなくなるような大きなインパクトのある攻撃が見込まれるといった2つの要因があります。後者の一例としては、例えばSHA-3と呼ばれる新しいハッシュ関数の策定があります。SHA-1やSHA-2ハッシュ関数の設計で見られるような数学的構造とは異なる設計方針が採択された提案アルゴリズムがNISTからFIPS仕様として標準化されています。しかしSHA-2はまだまだ安全に利用できると信じられており、SHA-3への移行はほとんど進んでいません。耐量子計算機暗号も後者に該当するものとして認識されており、危殆化が進んでいるというよりも将来に備えての準備を行っているという意味合いが強いです。

暗号アルゴリズムにおけるAgilityと呼ばれる考え方では、異なるアイデアやバックグラウンドに基づいた設計を持つ暗号アルゴリズムの「別の引き出しを持っておく」ことが重要とされており、今回のように耐量子計算機暗号の策定においても様々なバックグラウンドを持つアルゴリズムが勢揃いしていると考えることができます。その中でも2000年代から研究されてきた格子ベースの暗号アルゴリズムが有力であり、ファイナリストとして残留しているアルゴリズムの多くを占めていることが分かります。

*20 qTESLA（https://qtesla.org/）とNewHope（https://www.imperialviolet.org/2018/04/11/pqconftls.html）はRound3に組み込まれなかった。一方でSIDH（https://blog.cloudflare.com/introducing-circl/）がRound3に残留している。

2.7 量子計算機に伴う共通鍵暗号方式とハッシュ関数への影響

耐量子計算機暗号は、NISTのコンペティションで対象となるアルゴリズムを見る限り、公開鍵暗号方式のみに注力されているように見受けられますが、実際の利用場面を考えるとそればかりではありません。例えば、共通鍵暗号方式による暗号化と共に公開鍵暗号方式による暗号化が行われるなど、ハイブリッドに利用されています。デジタル署名と呼ばれる技術においても、暗号学的ハッシュ関数と公開鍵暗号方式による署名の2つのアルゴリズムが併用されています。このようなハイブリッドな利用方法においては、2つのアルゴリズムのバランスが重要で、それぞれのアルゴリズムに対してnビット安全性を有しているかどうか考える必要があります。そのため量子計算機の登場による共通鍵暗号方式と暗号学的ハッシュ関数の影響も考慮する必要があります。Groverのアルゴリズムにより、nビットの鍵を持つ共通鍵暗号方式ではその半分のビット長の強度しか持たないことが知られています。具体的にいえば、256ビットセキュリティを持つ暗号アルゴリズムを利用することにより、いずれ量子計算機が登場しても128ビット長の鍵を用いる古典的な暗号アルゴリズムと同じ強度を持つことになります[*21]。

次にハッシュ関数についてはどう考えるべきでしょうか。暗号学的ハッシュ関数には2つの暗号学的な機能を持つことが求められています。1つは耐衝突性(コリジョンレジスタンス)を持つこと、もう1つが原像計算困難性を持つことです。古典計算機においてはnビット長の出力を持つハッシュ関数は、耐衝突性としてn/2ビット安全性、原像計算困難性としてnビット安全性を持つことが知られています。後者についてはそのままGroverのアルゴリズムが最適なアルゴリズムであり、nビット出力のハッシュ関数における現像攻撃に必要な計算量は$2^{n/2}$まで落ちることが知られています。

量子計算機を用いた衝突探索に必要な計算量はBHTと呼ばれる効率的なアルゴリズムを用いると$2^{n/3}$になりますが、この攻撃には$2^{n/3}$というサイズの非常に多くの量子メモリの利用が前提となるため現実的ではありません[*22]。

CRYPTREC Report 2019(CRYPTRECにおいて2019年度の成果を集約したドキュメント群)[*23]によると、細山田氏の解説においてCNSのアルゴリズム[*24]が最も現実的に影響を及ぼすと考えられるという記載があり、CNSのアルゴリズムは$2^{2n/5}$の計算量で衝突発見が行われると報告されています。これは例えばSHA-256が古典的計算機では(耐衝突性として)128ビット安全性を持つアルゴリズムですが、このときCNSアルゴリズムで攻撃したとしても2^{100}以上の計算量が必要となるため現実的な脅威となるとは考えづらいという結論で締めくくられています。このように、共通鍵暗号方式及びハッシュ関数においては、量子計算機の登場による影響は公開鍵暗号方式に比べれば少ないと考えられています。既に策定・普及しているアルゴリズムを用いることで対策できるという意味では、現時点では備えるべきことは少ないといえます。

*21 Internet Infrastructure Review(IIR)Vol.31, 1.4.3 耐量子暗号の動向(https://www.iij.ad.jp/dev/report/iir/031/01_04.html)。
*22 Gilles Brassard et al., Quantum cryptanalysis of hash and claw-free functions. SIGACT News, 28(2):14–19, 1997.
*23 細山田 光倫, 量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価, CRYPTREC EX-2901-2019, 2020年1月. (https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf)。
*24 Andre Chailloux et al., An efficient quantum collision search algorithm and implications on symmetric cryptography, LNCS10625, pp.211-240, ASIACRYPT2017, 2017.

2.8 CRYPTRECによる量子計算機の脅威に関する考え方

2020年2月にCRYPTREC暗号技術評価委員会から注意喚起に関する文書が発行されました[*25]。これは当時ネイチャー誌に掲載された、量子コンピュータが量子超越を実現したと主張する論文[*26]に対し、技術的側面からCRYPTRECの見解を述べたものです。文書によれば、発表された論文により現在広く利用されている公開鍵暗号方式の安全性が大きく低下することが懸念されるようになったが、近い将来にCRYPTREC暗号リスト記載の暗号アルゴリズムが危殆化する可能性は低いと報告されています。その根拠として、取り上げられた論文では量子誤りが一切ない理想的な環境下を想定しており、2048ビットRSA暗号が8時間で解けると主張している論文[*27]においても2000万量子ビットが必要であるという見積もりもあり、現在の量子計算機の実装進捗とは大きく乖離している点が挙げられています。

この注意喚起レポートは、暗号アルゴリズムの脆弱性情報を検知した際の情報発信フローの情報分類B「正確で信頼性の高い情報を発信することによる過剰反応防止」を目的に発出されました。この背景や情報発信フローに関する詳細については前述のCRYPTREC Report 2019の第1章にて紹介されています。

2.9 NISTとの個人的な対話を通して

EUROCRYPT2016の併設ワークショップ[*28]で、NISTのLily Chenと耐量子計算機暗号を含む暗号政策に関して議論する機会に恵まれました。その際にNISTが暗号政策に関して耐量子計算機暗号と軽量暗号という2つの相異なる方向性を持っていることを指摘しています。当時の私は共通鍵暗号方式のポストクォンタム対応は鍵長を倍にするなどの延命技術による対策しか考えておらず、例えばAES-512などの新しいアルゴリズムを開発する、またはTriple AES（TripleDESのように3つの鍵で繋ぐ方法）などの対応を行うといった対策を、今後検討するのか尋ねてみました。その際の回答としては、既にAES-256があり、当時でも安全に利用可能であるし2030年以降も利用可能な鍵長は128ビットセキュリティを持つ暗号方式であるので、AES-256でも十分に量子暗号計算機耐性を持つと認識しているとのことでした。

また、共通鍵暗号方式での対策において公開鍵暗号方式と同じように新しいバックグラウンドに基づく暗号方式の導入という考え方が私には想像できませんでしたが、実際FSE2020では耐量子計算機対応共通鍵暗号方式「Saturnin」に関する発表が行われました[*29]。Saturninは軽量暗号でもあり耐量子暗号でもあるという2つの側面を持つ暗号方式です。軽量暗号はNIST

*25 CRYPTREC 暗号技術評価委員会, 現在の量子コンピュータによる暗号技術の安全性への影響, 2020年2月17日, CYPTREC ER-0001-2019.（https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html）。

*26 Frank Arute et al., Quantum supremacy using a programmable superconducting processor, Nature volume 574, pp.505-510, 23 October 2019.（https://doi.org/10.1038/s41586-019-1666-5）。

*27 Craig Gidney et.al, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits（https://arxiv.org/abs/1905.09749）。

*28 9th International View of the State-of-the-Art of Cryptography and Security and its Use in Practice（https://www.iacr.org/conferences/eurocrypt2016/ViennaMay13-2016.pdf）。

*29 Anne Canteaut et.al., Saturnin: a suite of lightweight symmetric algorithms for post-quantum security, FSE2020（https://iacr.org/cryptodb/data/paper.php?pubkey=30514）。FSE2020（https://fse.iacr.org/2020/program.php）にて発表。Saturninプロジェクト（https://project.inria.fr/saturnin/）。

で標準化のためのコンペティションが同様に開催されており、IoT機器での利用など非力なデバイスを想定した暗号アルゴリズムの総称として知られています。鍵長としては80ビット程度が想定されており安全性は一般的に用いられるアルゴリズムよりも弱い方式が採用されています。CRYPTRECでも2013年度から2016年度にかけて軽量暗号WGが設置され、軽量暗号の適切な利用を支援することを目的としてCRYPTREC暗号技術ガイドライン(軽量暗号)が2017年6月に発行されています[*30]。軽量暗号においても格子暗号などで見られるように独自にコンペティションを開催することで、自らの方式が安全かを検証する試みがなされており、今後の進展が個人的にも大変楽しみな研究分野の1つです。

このように、様々な利用場面において暗号アルゴリズムの標準化が行われています。既に述べたように量子計算機の登場が即座に影響を及ぼすことはありませんが、最新動向についてはCRYPTRECのサイトでキャッチアップできますので、活用していただければと思います。

執筆者:
須賀 祐治(すが ゆうじ)
IIJ セキュリティ本部 セキュリティ情報統括室 シニアエンジニア。2008年7月より現職。暗号と情報セキュリティ全般に関わる調査・研究活動に従事。CRYPTREC暗号技術活用委員会 委員。暗号プロトコル評価技術コンソーシアム 幹事。情報処理学会 CSEC研究会 幹事。IWSEC2021 General co-chair。AsiaCCS'22 General co-chair。Cryptoassets Governance Task Force(CGTF) Security WG member。APSIPA Multimedia Security and Forensics Technical Committee member。BGIN(Blockchain Governance Initiative Network) co-initial contributor。

*30 CRYPTREC 軽量暗号WG, CRYPTREC 暗号技術ガイドライン(軽量暗号)(https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf)。
CRYPTRECシンポジウム2017 軽量暗号ガイドライン紹介(https://www.cryptrec.go.jp/symposium/20171218_cryptrec-lw.pdf)。