耐量子計算機暗号の最新技術動向

車載システムセキュリティ部、車載コアテクノロジー開発統括部、オートモーティブソリューション事業本部
ルネサス エレクトロニクス株式会社

森山　大輔

イントロダクション

多くの暗号研究者や政府系機関は量子コンピュータが容易に利用できるようになった場合に現在広く利用されている暗号アルゴリズムが危殆化すると予想している。そして主要な企業はこの量子コンピュータ時代の到来を予測しており、量子コンピュータに対しても安全性が維持されるアルゴリズムを望んでいる。本ホワイトペーパーでは、今の公開鍵暗号の安全性がどのように評価され、どのくらい量子コンピュータが発展すると危ぶまれるのかを説明する。また、耐量子計算機暗号の標準化プロジェクトの最新動向および、各国政府や企業が耐量子計算機暗号の導入に向けてどのような動きを見せているのかについて解説する。

身近に使われている暗号技術

暗号技術は私達が気が付かない様々な場面で身近に利用されている。PC やスマーd トフォンによって Web サイトを閲覧するとき、近年では多くの Web サーバはセキュアな通信がデフォルトで選ばれるように設定している。多くの Web ブラウザでは、セキュアな通信が行われている場合には URL に閉じた錠前を表示させており、これはブラウザ内で Hypertext Transfer Protocol (HTTP)を拡張した Hypertext Transfer Protocol Secure (HTTPS)が実行されていることを意味している。HTTPS をデフォルトとする Web サーバは 2018 年においては 27%であったが、2022 年時点では 80%に増えている [1]。安全な通信のためには少なくともサーバ側が信頼できる相手であることを確認する必要があり、電子証明書がその役割を担っている。電子証明書にはサーバ側の公開鍵に対しての電子署名や、どの暗号アルゴリズムによってその電子署名が作られているかの情報が含まれている。そしてクライアント側が規定された演算を実行することでサーバの正当性を検証することができる。例えば、https://www.renesas.com にアクセスし証明書の情報を確認すると、図 1 のように暗号アルゴリズムとして RSA や SHA-256 を利用してウェブサイトに紐づく電子証明書が生成されていることを読み取ることができる。

また、Web サーバとクライアントによって一定のデータを安全に送受信する場合、Transport Layer Security (TLS)は暗号学的に安全な鍵交換プロトコルや鍵配送スキームといった公開鍵暗号を用いて二者のみが知ることができる共通の値を導出させ、その上で共通鍵暗号を用いてメッセージを暗復号する仕組みを設けている。セキュア通信は IoT 製品にとっては必要不可欠であり、私達が提供している RX マイコンでは wolfSSL ライブラリをサポートしている [2][3]。また、このような公開鍵暗号と共通鍵暗号の組み合わせは Web ブラウジングのみに限定されたメカニズムではなく、安全な通信のために多くの場面で利用されている。自動車ネットワークにおいては、通信相手が事前に決定している状態ではない Vehicle-to-Vehicle (V2V)や Vehicle-to-Infrastructure (V2I)通信において有効活用されることが想定される。

電子署名はネットワーク通信を伴う状況以外にも、近年のマイクロコントローラや PC 等では内部動作においても利用されている。例えば起動シーケンスを実行する際、基本的な機能に対しては改ざん検知や信頼性の検証を必要とする場合がある。そのためには、一般的に Root of Trust として電子署名を内部に組み込んでおき、証明書から導かれるトラストチェーンが次の起動対象プログラムへ信頼性を繋げている。そのためこのアーキテクチャによって不正なプログラムの実行を防ぐことができる。私達の車載製品に対してのセキュアブートのアーキテクチャに関してはルネサスのウェブサイトのブログに詳細を載せている[4][5]。また、IoT 製品に対してもセキュアブートのメカニズムを載せており、例えば RA ファミリマイコン向けの Renesas Flexible Software Package ではオプションとして安全なブートローダーを提供している [6][7]。

このように、公開鍵暗号や共通鍵暗号は私達の身の回りの様々な場面で安全を確保することに利用されている。一方で、最近量子コンピュータの発展に伴い、既存のコンピュータで一万年以上かかる計算が数秒で解けるようになった、といったニュースを目にした読者もいるであろう。本ホワイトペーパーでは、現在の暗号の安全性がどのように評価されており、量子コンピュータによる影響がどのようなものか、量子コンピュータの進展や耐量子計算機暗号についての最新動向と国や企業の取り組みについて解説する。

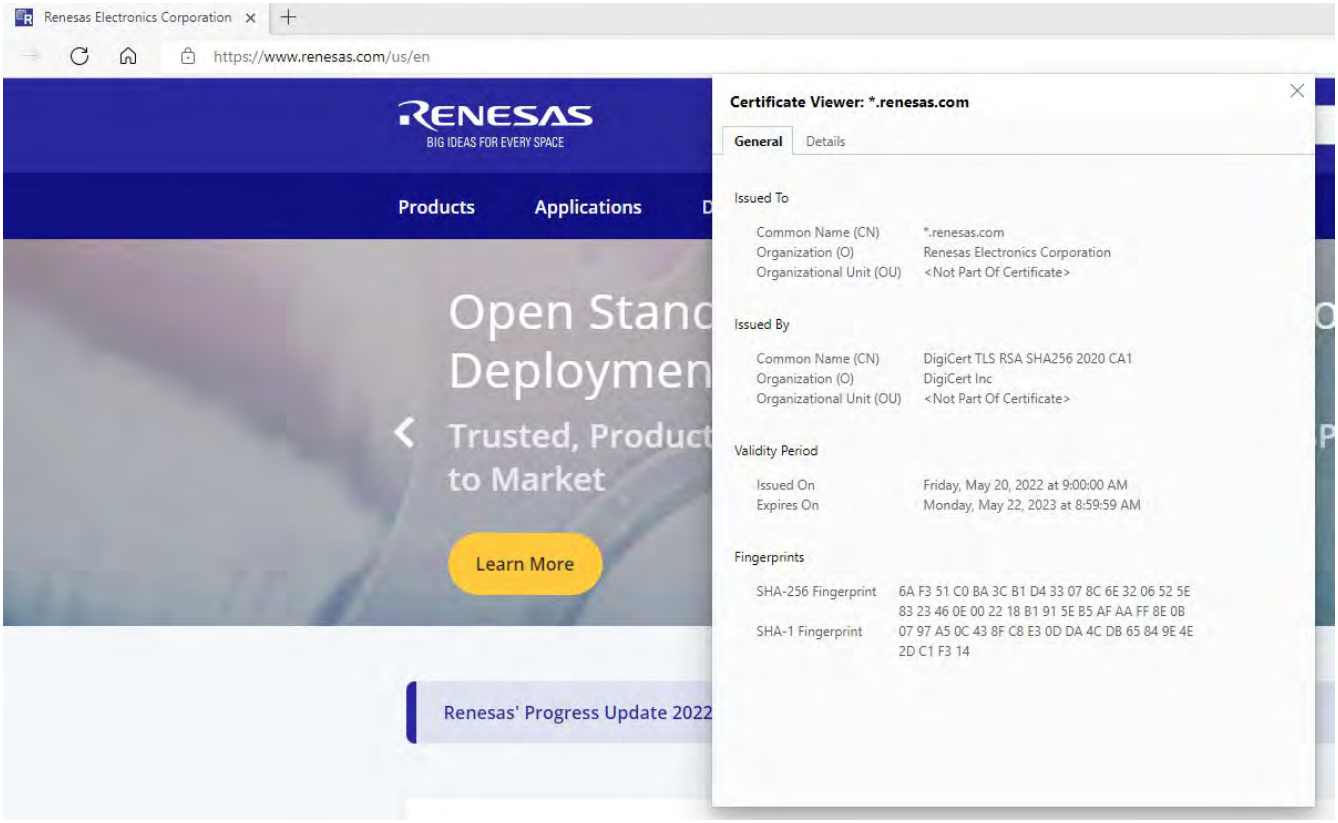

図 1. Renesas Electronics Web ページに対する証明書

現在の公開鍵暗号の安全性

電子署名方式や鍵交換プロトコルといった現在広く利用されている公開鍵暗号は、一般的なコンピュータを用いても解くことが難しい数学的問題を安全性の根拠としている。素因数分解問題はそのうちの有名なものの一

つで、$N \coloneqq p \times q$から(p, q)の素数の組を計算するのは難しいという問題である。例えば21を3×7と因数分解するのは容易だが、データ長を非常に長くすると一般的なコンピュータを用いたとしても効率的に解くことができなくなる。この数学的問題をベースとして RSA 暗号が作られている。またそれ以外では、有限体上や楕円曲線上の離散対数問題が広く知られている数学的問題である。これらについてもデータ長が長くなれば長くなるほど問題を解く難易度は上がっていく。DSA や ECDSA はこれらの問題に基づく良く知られた電子署名方式である。

数学的問題に対しての安全性の強度は、AND・OR や XOR といったコンピュータによる 1 回の処理を 1 ステップとして何回計算が必要かを指標として考えられている。研究者が考案した最良の解読アルゴリズムを用いたとしても2^{128}回以上の計算の手間がかかる場合、その問題は指定されたビット長において 128-bit security を満たすという。素因数分解問題をベースとした RSA 暗号の場合、Nが 3,072-bit で(p, q)が 1,536-bit 設定の時に 128-bit security を満たすと現在では評価されている。いくつかの代表的なアルゴリズムとパラメータ例を表 1 に示す。

表 1. 典型的な既存アルゴリズムと一般的なコンピュータに対してのセキュリティ

	Encryption	Signature		Key exchange	
Algorithm	RSA	DSA	ECDSA	DH	ECDH
112-bit security	2,048-bit	2,048-bit	224-bit	2,048-bit	224-bit
128-bit security	3,072-bit	3,072-bit	256-bit	3,072-bit	256-bit
192-bit security	7,680-bit	7,680-bit	384-bit	7,680-bit	384-bit
256-bit security	15,360-bit	15,360-bit	512-bit	15,360-bit	512-bit

数学的問題を一つ破る実現性を図るため、1 億台のコンピュータを 24 時間 365 日稼働させ、4GHz 動作の CPU が 1 クロックに 1 回の頻度で解読に成功しているかどうかのテストを実行できると想定することにする。このとき 1 年間で行うことができる計算量の合計は$10^7 \times 60 \times 60 \times 24 \times 365 \times 4 \times 10^9 \approx 2^{80}$であり、仮に 1000 年稼働させたとしてもおおよそ2^{90}回の計算量であり、これだけの時間とリソースを消費して初めて 90-bit security の数学的問題を破ることに成功する。

このような推定に対して十分な余裕を持ち安全性を保ちつつ、利用する上で十分効率的なだけ小さいビット長のアルゴリズムを選ぶことが望ましい。CPU の処理性能は半導体技術の発展により徐々に高まっているため、現実的なレベルでセキュリティを維持するために必要なビット長も徐々に高まってきている。10 年前は 112-bit security は十分なセキュリティを保つものとして推奨に含まれていたが、NIST（アメリカ国立標準技術研究所）は 112-bit security が現実的に耐えられる期限は 2030 年までとし、現在は 128-bit security への移行を推奨している[8]。また、128-bit security は現在のコンピュータに対しての安全性であれば 2050 年までは許容されるであろうという見解が日本の政府系プロジェクト CRYPTREC によって示されている [9]。

量子コンピュータの登場と発展

上で説明した暗号の安全性は、私達が使っている PC・クラウドサーバ、マイクロコントローラといった古典的なコンピュータを基準に評価している。一方、近年多くの業界から着目を浴びている量子コンピュータは、量

子力学をベースとした物理現象である重ね合わせ状態や量子もつれ状態といったものを利用して計算を行う。量子コンピュータは単純に既存のコンピュータより多少計算速度が速いというだけではない。量子コンピュータ内ではこれまでのコンピュータにおける『ビット』の概念に相当する『量子ビット』が存在し、この量子ビットは 0 と 1 といったデジタルな状態ではなく両方の状態を同時に満たす。そのため、古典コンピュータにおける2^N-bit の状態をN個の量子ビットで表現することができる。この性質を利用することで、RSA 暗号や楕円曲線上の演算などのいくつかの数学的問題を破るのに必要な時間が非常に少なくなる。

一方で、量子ビットを数百ビット程度用意すれば現在の公開鍵暗号を容易に解くことができるというわけではない。量子コンピュータが直接扱う 1 つの量子は非常に不安定でノイズが乗るため、そのままでは AND や OR の計算に用いることはできない。この量子は物理量子ビットと呼ばれる。物理量子ビットを実際の論理演算に適応できるようにするには、十分なエラー訂正や論理演算を実行するだけの状態の維持が必要であり、1 つの論理量子ビットを安定的に利用するには 1,000 個程度の物理量子ビットが必要だとされている。2019 年には量子コンピュータを用いれば、2,048-bit の RSA 暗号を 8 時間で破ることができると試算された研究結果があるが、これは 2000 万個の物理量子ビットを扱うことができる量子コンピュータを作ることができた場合の予測である[10][11]。入力長nに対して、素因数分解問題を解くためにおおよそ$3n$個の論理量子ビットが必要であるとこの論文の著者らは推定している。また素体上の楕円曲線暗号に焦点を当てた場合は、離散対数問題を破るには$9n$個の論理量子ビットが必要であることが別の論文に示されている[12]。

2010 年頃から、いくつかの企業は実際に動作する量子コンピュータを発表するようになった。最新の成果としては、2019 年に Alphabet™ は 53-qubit（物理量子ビット）の量子コンピュータを発表し、IBM®は 2021 年には 127-qubit の量子コンピュータを、2022 年には 443-qubit の量子コンピュータを発表した[13][14][15](*1)(*2)。また、IBM®はロードマップとして 2023 年には 1121-qubit、2025 年には 4,158-qubit の量子コンピュータの開発を進めていることを発表している[16]。上記で記載した公開鍵暗号を破るための 2000 万 qubit の到達にはまだ時間がかかるが、量子コンピュータの研究・開発の進展は著しい。このような技術動向を受けて、ホワイトハウスは米国連邦機関に対し 2035 年までに量子コンピュータによる影響を低減する暗号アルゴリズムへの強化が必要であるという覚書を発行している [17]。ENISA (欧州ネットワーク情報セキュリティ機関) は、2021 年に公開しているレポートにおいて 10 年以上データの機密性を保持したいのであれば、一定の対策をとる必要があると述べている[18]。

(*1) Alphabet は Alphabet Inc.の商標です。
(*2) IBM は世界の多くの国で登録された International Business Machines Corp. の商標です。

耐量子計算機暗号の選定

2016 年に、NIST は量子コンピュータによる攻撃から守るため次世代の公開鍵暗号を選ぶための耐量子計算機暗号(PQC: Post Quantum Cryptography) 標準化を開始させた。NIST は世界中の研究者から現在使われている RSA 暗号や楕円曲線暗号に置き換わることができる暗号アルゴリズムを募集した。暗号化や電子署名などの暗号方式に対して合計で 69 件の投稿が行われた。NIST や研究者らが時間をかけて議論を交わし、2019 年にはその中から 26 個の方式が第 2 ラウンドに選ばれ、2020 年には 15 個の方式（うち最終候補 7 件、補欠候補 8 件）が第 3 ラウンドに進んだ。そして 2022 年 7 月に第 3 ラウンドに進んだ候補の中から標準化されるアルゴリズムとして公開鍵暗号方式に CRYSTALS-Kyber が、電子署名方式に CRYSTALS-Dilithium、FALCON、SPHINCS+の 3 つが選ばれた。

NIST は関連する FIPS ドキュメントを公開した時、CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+をそれぞれ ML-KEM, ML-DSA, FN-DSA, SLH-DSA という名称に変更した（FALCON は FN-DSA と呼ばれる予定である）。FN-DSA を除き、3 つのアルゴリズムについてはそれぞれ FIPS 203, FIPS 204, FIPS 205 として 2023 年 8 月に Draft 版が公開された後、2024 年 8 月に最終版が公開された[19][20][21]。この 2 年間、様々な研究者による細かい仕様変更の議論を行われた。

NIST は PQC アルゴリズムの安全性のレベルについて Category 1 から Category 5 までの 5 つに分けている。これらはそれぞれ順に AES-128, SHA-256, AES-192, SHA-384, AES-256 と同等のセキュリティレベルを耐量子安全性と古典コンピュータに対しての安全性の両方で有するものとした指標となっている（正式な分類については NIST SP800-57 part 1 に記載される予定である）。古典コンピュータにおける 128-bit security が Category 1 および 2、192-bit security が Category 3 および 4、256-bit security が Category 5 であると捉えると簡単である。ML-KEM, ML-DSA, SLH-DSA に定義されているパラメータセットと安全性レベルをまとめたものが表 2 である。より高い安全性を選んだ場合に PC やサーバにかかる計算時間が増えることは自然であるため、ユーザは状況に応じて適切な安全性レベルを選択する必要がある。

表 2. 耐量子計算機暗号標準化選定アルゴリズム

PQC Security Category	ML-KEM (Key Encapsulation Mechanism)	ML-DSA (Signature Scheme)	SLH-DSA (Signature Scheme)
Category 1	ML-KEM-512	-	SLH-DSA-SHA2-128 SLH-DSA-SHAKE-128
Category 2	-	ML-DSA-44	-
Category 3	ML-KEM-768	ML-DSA-65	SLH-DSA-SHA2-192 SLH-DSA-SHAKE-192
Category 4	-	-	-
Category 5	ML-KEM-1024	ML-DSA-87	SLH-DSA-SHA2-256 SLH-DSA-SHAKE-256

耐量子計算機暗号アルゴリズムは、RSA 暗号が利用している素因数分解問題とは異なり、ベクトル空間上の原点から最も近い点を求める shortest vector problem と呼ばれるものや、ある点から最も近い格子点を求める closest vector problem といった別の数学的な問題に基づいて構成されている。その他にもいくつかの量子コンピュータに対して安全な数学的問題が存在するが、ML-KEM, ML-DSA, FN-DSA はこの格子問題を利用したアルゴリズムである。

NIST の推奨によれば、ML-KEM と ML-DSA が一般的にアプリケーションにおいてよく用いられることを想定している[22]。FN-DSA は ML-KEM よりも署名の長さが短いという利点があるため、用途によっては利用価値が高いとしている。SLH-DSA は他の 2 つの署名方式と異なり、安全性の根拠を数学的な問題ではなくハッシュ関数の安全性（衝突困難性）に基づいたものとなっていることを理由に挙げている。格子に基づく問題は比較的新しい研究分野であるため、NIST は優れた新しい解読アルゴリズムの発見によってブレイクスルーが起こることを懸念して複数のアルゴリズムを標準化することを望んでいる。

NIST は上記 4 つの最初のアルゴリズムを選定したことを公表すると同時に、第 4 ラウンドとして KEM アルゴリズムの評価を継続することを発表している。本ホワイトペーパーを執筆している時点では、BIKE、Classic McEliece、HQC の 3 つのアルゴリズムが調査対象になっている[23]。これらのアルゴリズムの安全性は、格子問題とは異なるものを利用している。また、NIST は署名方式についても格子問題に基づかないものを中心とした新しいアルゴリズムの募集を行い、現在選定作業を行っている。そのため、最終的に標準化されるアルゴリズムは現時点のものよりも増える可能性がある。

耐量子計算機アルゴリズムは多く存在するが、多くの人々にとって重要なのは安全なチャネルを通じてお互いが途切れなく通信できることを保証するために、標準化されたアルゴリズムの定義に沿ったものを広めることである。AES、SHA、ECDSA などと同様に、すべてのハードウェア/ソフトウェアの実装が機能的な面で同一であることが必要である。

共通鍵暗号の量子コンピュータに対する安全性

上記で述べたように、量子コンピュータは現在の公開鍵暗号を攻撃するには非常に効果的なツールである。一方、共通鍵暗号に対しての安全性としては、Grover のアルゴリズムという全数探索アルゴリズムが知られている。それは、全数探索を行う場合に通常のコンピュータで2^N回の計算が必要とされる演算の場合、量子コンピュータは$2^{N/2}$回の計算で済むというものである。例えば、AES において 128-bit/192-bit/256-bit 秘密鍵を用いる場合、古典的な安全性の強度は 128-bit/192-bit/256-bit security であるが、量子コンピュータにおけるセキュリティはこの時点では 64-bit/96-bit/128-bit security と評価される。この計算量の削減も一つの正しい測定指標である。ただし PQC アルゴリズムの安全性と対比される具体的な共通鍵暗号の量子コンピュータに対する安全性を厳密に研究者が評価する場合は、共通鍵暗号アルゴリズムの仕様に基づいた計算量あるいは回路規模も含めてカウントを行う。

従来、古典コンピュータを用いて AES に対して全数探索を行う場合、秘密鍵をインクリメントする単純な For 文によるループ処理を実行して正しい秘密鍵を見つけるプログラムを実行する。そのため、アルゴリズムを実装したソフトウェアのコード量やハードウェア実装される端末数が増えるわけではない。一方で、量子コンピュータを用いて Grover のアルゴリズムを実行するためには、共通鍵暗号アルゴリズムを直列的に実装する必要があり、ループ関数による単純な反復的な動作を用いることはできない。そのため、Grover のアルゴリズムを AES-128 に対して適応するということは、2^{64}個の AES 回路を実装する必要となる。そのため、AES を演算するために消費する量子コンピュータ上の資源も正確にカウントする必要がある。また、正確な計算を維持するために前の章で述べたようにすべての量子ビットに対するノイズを除去する必要もある。

NIST は量子コンピュータが一定時間内に直列で実行することができる計算量の上限を MAXDEPTH というパラメータで定めており、2^{40} (1 年)、2^{64} (10 年)、2^{96} (1000 年)としている。これらの条件を一通り加味した上での共通鍵暗号アルゴリズムの計算を含めた全数探索を実行するためのゲート数（計算量）が見積もられる。NIST は研究者によって分析された AES についての評価結果を採用している [24]。現時点ではハッシュ関数については NIST 文書では言及されていないが、いくつかの研究者は SHA2 および SHA3 についてのハッシュ関数の計算時間やデータ量を含めた安全性評価を行っている[25]。表 3 は NIST が公開している共通鍵暗号の演算処理を含めた全数探索全体の安全性評価 [24]に、文献[25]による最新のハッシュ関数に対する量子コンピュータ向け安全性を加えたものである。

表 3. 全数探索にかかるすべての処理を含めた共通鍵暗号の安全性

PQC Security Category	Symmetric Key Cryptography	Security with Quantum Gates (Quantum Computer)	Security with Classic Gates (Classic Computer)
Category 1	AES-128	2^{157}/MAXDEPTH	2^{143}
Category 2	SHA-256	2^{188}/MAXDEPTH [25]	-
	SHA3-256	2^{183}/MAXDEPTH [25]	2^{146}
Category 3	AES-192	2^{221}/MAXDEPTH	2^{207}
Category 4	SHA-384	2^{266}/MAXDEPTH) [25]	-
	SHA3-384	2^{260}/MAXDEPTH [25]	2^{210}
Category 5	AES-256	2^{285}/MAXDEPTH	2^{272}
-	SHA-512	2^{343}/MAXDEPTH [25]	-
	SHA3-512	2^{347}/MAXDEPTH [25]	2^{274}

耐量子計算機安全性は公開鍵と共通鍵で異なるが、ハッシュ関数は特に電子署名を実行する際にはメッセージを圧縮するために必要不可欠である。また、ML-KEM や ML-DSA はハッシュ関数 SHA3 を構成要素とし、アルゴリズム内で複数回ハッシュ計算が実行される。そのため、安全に暗号化や署名を実行するためにはハッシュ関数の安全性への考慮も必要になり、これらのアルゴリズムでは全体の安全性が保たれることを考慮して適切なハッシュ関数アルゴリズムを選定している。

RSA や楕円曲線暗号のような既存の公開鍵暗号に比べ、量子コンピュータが共通鍵暗号に与える影響は限定的である。上記で述べたように、現在の公開鍵暗号アルゴリズムを破るのに必要な論理量子ビットの数は入力長に対して比例するだけである。一方、共通鍵暗号アルゴリズムを破るのには指数的に大きな計算量がいまだに必要である。そのため NIST は現状、公開鍵暗号アルゴリズムについての耐量子計算機暗号の標準化に焦点を当てている。

耐量子計算機暗号導入の世界的動向

今や世の中にはオープンソースプロジェクトによって様々なオープンソースのソフトウェアを商用製品に対して評価及び利用することができる。耐量子計算機暗号アルゴリズムを実装しているソフトウェアについてもいくつか存在し、NIST に投稿された資料の中に C 言語によるリファレンス実装を手に入れることができる。また、これらとは別により公平に評価し広範に使われることを目的としている PQClean Project について紹介しよう[26]。

PQClean Project は 2019 年に始動し NIST による標準化に選ばれた 4 つのアルゴリズムを含むいくつかの耐量子計算機暗号アルゴリズムのオープンソースソフトウェアを提供している。典型的なオープンソースプロジェクトと異なるのは、PQclean は主要な C 言語ツールチェーンでのコンパイル上でエラーもワーニングも出ないこと、静的・動的解析の実行、名前空間のルールなど、ソフトウェア品質改善を施していることを特徴としていることである。そのため、上位レイヤのシステムに安全に組み組むことができ、また標準化された複数のアルゴリズムのうちどのアルゴリズムがそのシステムにおいて適切かを評価することができる。PQClean Project

から生み出されたソースコードは、Open Quantum Safe Project という OpenSSL™ 等へのプロトタイプ実装のオープンソースプロジェクトに取り入れられている[27] (*3)。

また、ヨーロッパ連合が主導となり進められた PQCRYPTO プロジェクトでは、ARM® Cortex®-M4 を対象としたライブラリとして pqm4 が公開されている (*4)。pqm4 には、NIST に投稿されたリファレンス実装・最適化 C 言語実装・PQClean による実装・Cortex®-M4 の命令セットを用いたアセンブリ実装など複数の実装から選ぶことができ、IoT 製品向けのマイクロコントローラに対しての SW 実装評価において非常に役立つであろう。

現在、いくつかの IT 企業は主にベータ版として Transport Layer Security (TLS)に対して耐量子計算機暗号を有効にしたライブラリやソフトウェア・サーバサイドの設定を提供している[28][29][30][31]。それ以外の業種での導入事例はまだ把握できていないが、政府機関による注意喚起は最近多く聞かれるようになった。一つのシステムが数十年利用され続けることが想定される重要インフラに関しては、CISA（米国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁）は今後の技術動向に注意しながら、耐量子計算機暗号への移行を計画するよう注意喚起を促すガイドラインを発行している[32][33]。また、ENISA や BSI（ドイツ連邦政府情報セキュリティ庁）は既存のシステムとの共存や、耐量子計算機暗号側への重大な脆弱性の発見による影響を最小化するための安全性の確保のために、耐量子計算機暗号と既存の公開鍵暗号を併用して共有する鍵生成の導出や電子署名の生成を行う方法を提案している[34][35]。多くの業種において耐量子計算機アルゴリズムの移行には数年単位での時間が必要であると予想されるが、各国政府機関や民間企業が率先して長期的な目線で安全な社会を継続するためにより安全な技術の導入を推し進めていくことが重要である。

(*3) OpenSSL は OpenSSL Software Foundation の商標です。
(*4) ARM および Cortex は米国およびその他の国における ARM Ltd.の登録商標または商標です。

まとめ

本ホワイトペーパーでは、量子コンピュータと耐量子計算機暗号の最新動向について取り上げた。現在利用されている公開鍵暗号は古典コンピュータに対しては十分安全であるが、量子コンピュータが登場した場合には安全性が非常に低下する。現在では NIST による耐量子計算機暗号の標準化プロジェクトにより 4 つのアルゴリズムの選定が完了し、これらのアルゴリズムが今後のデジタル社会のセキュリティを提供する上で非常に重要な役割を担うと予想される。技術移行には非常に長い時間がかかると思われるが、多くの機関が協力し消費者に対してどのようなデジタルサービスや製品についても安全な環境を提供できるようにすることが望まれる。特に長期間稼働することが見込まれる IoT や車載機器については、現在の公開鍵暗号の危殆化がその製品の寿命に影響を与えないように耐量子暗号が対応できるかも重要な要素の一つになると考えられる。特に、長期的に利用されることが想定される製品について耐量子計算機暗号をサポートすることによって影響を軽減することができる。Renesas は耐量子計算機暗号に関連する標準化動向や技術動向について今後も観測を継続していく予定である。NIST による標準化はまだ完全に完了したわけではないが、それぞれの PQC アルゴリズムにはハッシュ関数を含め様々な算術的・論理的な演算が行われており、自動車や IoT 製品において Microcontroller や System-on-Chip (SoC)は効率的にこれらの演算を実行できるようにするための重要な役割を担う。私達は、強力な量子コンピュータが登場したとしても私達の顧客が Security を維持したエコシステムを

実装することができるよう、近い将来において効率的な PQC のハードウェア・ソフトウェアを提供することができるよう検討を重ねています。

[参考資料]

[1] https://w3techs.com/technologies/history_overview/site_element/all/y

[2] https://www.renesas.com/us/en/products/microcontrollers-microprocessors/rx-32-bit-performance-efficiency-mcus/rx-partners/wolfssl-embedded-ssl-tls-library

[3] https://www.renesas.com/us/ja/blogs/realizing-secure-and-high-speed-communications-rx-mcu-and-wolfssls-tls-library ([2]の日本語版)

[4] https://www.renesas.com/us/en/blogs/introduction-about-secure-boot-automotive-mcu-rh850-and-soc-r-car-achieve-root-trust-1

[5] https://www.renesas.com/jp/ja/blogs/introduction-about-secure-boot-automotive-mcu-rh850-and-soc-r-car-achieve-root-trust-1 ([4]の日本語版)

[6] https://www.renesas.com/us/en/software-tool/flexible-software-package-fsp

[7] https://www.renesas.com/us/ja/software-tool/flexible-software-package-fsp ([5]の日本語版)

[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[9] https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2021.pdf (日本語のみ)

[10] https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/

[11] https://arxiv.org/abs/1905.09749

[12] https://link.springer.com/chapter/10.1007/978-3-319-70697-9_9

[13] https://www.nature.com/articles/s41586-019-1666-5

[14] https://research.ibm.com/blog/127-qubit-quantum-processor-eagle

[15] https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

[16] https://www.ibm.com/quantum/roadmap

[17] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[18] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

[19] https://doi.org/10.6028/NIST.FIPS.203

[20] https://doi.org/10.6028/NIST.FIPS.204

[21] https://doi.org/10.6028/NIST.FIPS.205

[22] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[23] https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

[24] https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf

[25] https://eprint.iacr.org/2024/513.pdf

[26] https://github.com/PQClean/PQClean

[27] https://openquantumsafe.org/

[28] https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world

[29] https://aws.amazon.com/blogs/security/how-to-tune-tls-for-hybrid-post-quantum-cryptography-with-kyber/

[30] https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

[31] https://blog.cloudflare.com/post-quantum-for-all/

[32] https://www.cisa.gov/uscert/ncas/current-activity/2022/08/24/preparing-critical-infrastructure-post-quantum-cryptography

[33] https://www.cisa.gov/news/2022/08/24/cisa-releases-new-insight-preparing-critical-infrastructure-transition-post-quantum

[34] https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

[35] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html

（Rev.1.1 Oct 2024）

本社所在地

〒 135-0061 東京都江東区豊洲 3-2-24（豊洲フォレシア）

https://www.renesas.com

お問合せ窓口

弊社の製品や技術、ドキュメントの最新情報、最寄りの営業お問合せ窓口に関する情報などは、弊社ウェブサイトをご覧ください。

http://www.renesas.com/contact/