応用耐量子セキュリティ

耐量子アルゴリズム及び量子鍵配送

日本語版の提供について

本書「応用耐量子セキュリティ」は、Cloud Security Alliance (CSA)が公開している「Applied Quantum-Safe Security –Quantum Resistant Algorithm and Quantum Key Distribution-」の日本語訳です。本書は、一般社団法人日本クラウドセキュリティアライアンス（CSA ジャパン）が、CSA の許可を得て翻訳し、公開するものです。
本書は、原文をそのまま翻訳したものです。また、本書内で参照されている URL 等は、すべて英語版へのリンクとなっております。原文と日本語版の内容に相違があった場合には、原文が優先されます。

翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性及び原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
翻訳に際して原文の誤りと推測されるものは著作者に確認の上、最小限の修正を行った上で翻訳しています。また、翻訳に際して行った判断については、脚注部に「訳注」として示しました。

この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。
変更履歴

日付	バージョン	変更内容
2017 年 9 月 5 日	日本語バージョン 1.0	

クラウドセキュリティアライアンスの耐量子安全性セキュリティワーキンググループの常置アドレスは、https://cloudsecurityalliance.org/group/quantum-safe-security/です。

謝辞

クラウドセキュリティアライアンス

Frank Guanco
Ryan Bergsma
Victor Chin
Stephen Lumpe

耐量子セキュリティワーキンググループ

Bruno Huttner, 共同リーダー
Jane Melia, 共同リーダー
Ludovic Perret
Lee Wilson

以下の方々に謝意を表します。

Sauvik Bhattacharya
Tom Brennan
Roberta Faux
Dan Hiestand
Jens Jensen
Xu Lei
Xinhua Ling
Larry Ramos
Rino Sanchez
耐量子セキュリティワーキンググループのメンバー達

1. はじめに：耐量子セキュリティワーキンググループ

耐量子セキュリティワーキンググループ(QSS-WG)は、クラウドセキュリティアライアンスによって設立された産業フォーラムで、その目標は*耐量子セキュリティ*[1]：すなわち、現代暗号によるセキュリティへの攻撃が可能である、耐量子コンピュータに対する保護を強化することによって、デジタル及び物理的データセキュリティの理解と実装を推進することである。

QSS-WG は、耐量子セキュリティという共通の目標に向かって、様々な異なるアプローチを取っているコミュニティがまとまって集合体となった、ユニークなフォーラムで、実質のある、かつ有意義な対話を可能にする。このグループは、セキュリティ業界の様々な分野から来た参加メンバーとフォロワーによって構成される。最も活発なメンバーは、一般企業及び学術研究機関から参加している、*耐量子アルゴリズム*によるソリューションを研究開発する人達、及び、物理学による、*量子技術*に依拠した代替策に取り組む人達である。

[1] イタリック体の用語については第 11 節の「用語の解説」に定義を掲載している。

このホワイトペーパーの目的は、セキュリティ産業及び関連する分野に身を置く人々に対して、量子コンピュータとそのサイバーセキュリティに対する影響に関する関連知識を提供することである。クラウドセキュリティアライアンスはこれらの情報が、我々全員が量子コンピュータ時代に備えるに当って、関心を持っているそのような人々が自分達の個別の問題や課題に対して最も適切なソリューションを見出す一助になることを願っている。

2. 耐量子セキュリティの必要性

昨年頃から、広範に普及している現代暗号標準への*量子コンピュータ*の脅威に対する認識は劇的に高まっている。合衆国政府の国家安全保障局(NSA)や英国政府の政府通信本部(Government Communications Headquarters, GCHQ)内のグループである通信機器セキュリティグループ(Communications-Electronics Security Group , CESG)などのセキュリティ機関が耐量子暗号スキームへの移行を求めていた。欧州電気通信標準化機構(European Telecommunications Standards Institute, ETSI)やアメリカ国立標準技術研究所(National Institute for Standards and Technology, NIST)や国際標準化機構(International Organization for Standardization, ISO)などの標準化組織は新しい国際標準に対するニーズの調査を開始している [CJLMPPS16]。これらのエンティティはみな同じ結論に達しており、合意は明らかである：今日のサイバーセキュリティソリューションが拠り所としている暗号基盤を直ちに再整備する必要があり、また耐量子セキュリティへの移行は今始めなければならない。

実用可能な量子コンピュータの実現が何時になるかはまだ議論の分かれるところではあるが、専門家は、現在の公開鍵暗号を破れるような量子コンピュータが 5 年から 15 年以内に現われるだろうと考えている。このことから、かなりの準備期間が与えられているかのように思えるかもしれないが、当てにしている助走期間は二つの要素によって短縮される。

- 第一に、耐量子セキュリティへの移行によって我々の情報セキュリティの生態系は著しく変化することとなり、これは一朝一夕に終えられるものではない。それらのシステムを新しいセキュリティアルゴリズムやプロトコルに適合させるには 5 年から 10 年を要するだろうというのが一致した見解である。
- 第二に、暗号化されたデータの殆どには長い秘匿期間があり、通常数年から数十年、またはそれ以上の期間秘匿を守らなければならない。データストレージ技術の現在の進歩からすると、通信されているほぼ無限量のデータを捕捉し将来解読すべく保存することができる。これは一般には「今落として後で解読」または「ハーベスト型」攻撃という名で知られている。ETSI のホワイトペーパー**Quantum Safe Cryptography and Security**, [CCDDFGZ15] に書かれているように、「耐量子暗号がなければ、ネットワーク上で既に通信されたかまたは今後通信される全てが盗聴され公に開示される危険がある」のだ。量子コンピュータは—原理的には—安全でない方法で暗号化されていた全ての機密情報を解読することができる。故に、我々のサイバーセキュリティシステムの機密性が崩壊するのを防ぐためには、行動すべき時は今なのである。量子によるアタックからも保護が可能な新しいソリューションを発見することは、サイバーセキュリティ産業に身を置く全ての人々にとってホットなテーマとなるべきである。

3. リスクマネジメントの実施

セキュリティは絶対的なものではない。あり得る全ての脅威に対して完璧なセキュリティを与えるような普遍的ソリューションは存在しない。セキュリティを提供することは常に、あるレベルの保護を—決められたコストで—そして然るべき期間、保証しようとする行為である。しかしながら、一つだけで全てを満足できるわけではない。幾つか例を示す：

- もしあなた方(の組織)がオンラインでアプリを提供しているソフトウェア会社ならば、最も大きな関心事は認証と自社のソリューションの完全性である。あなた方のお客様に対して、自分が機器に正しいアプリケーションをダウンロードしインストールしていると確信できるようにしなければならない。

- もしあなた方が任務実行中の警察組織ならば、あなた方の通信で第一の関心事は可用性で、次いで機密性になる。
- もしあなた方が病院で、遠方に患者の医療記録を送ろうとしているならば、長期的プライバシーが主要な要求事項になる。
- もしあなた方が、毎日様々な企業から送られて来るテラバイト単位のデータのバックアップを 2 つの場所で取るような大規模なデータセンターを運営しているならば、あなたのセキュリティ要件は、新しいアプライアンスを買おうとしてネットサーフィンしているスミス氏のそれと同じではない。
- もしあなた方が「完全な」セキュリティを必要とする政府機関ならば、ワンタイムパッド(OTP)を使うかもしれないが、その安全性は証明されている。しかしながら、セキュリティは完全に、キーのランダム性と鍵配送のセキュリティにかかっており、これらを問題にしなければならない。

結論：暗号ツールはデータの特定の型式に適合するように作らなければならない。量子コンピュータの脅威に対応するために開発される新しいツールはいずれも、特定の用途に合うように作られなければならない。

4. デジタル及び物理的セキュリティ

公開鍵暗号が約 40 年前に発見されて以来、コンピュータセキュリティに対する一般の理解は主に、認証やオンライン通信の暗号化を実現するアルゴリズムのようなデジタルセキュリティの手法に向かっていた。暗号スキームのセキュリティは数学と、巨大な計算能力に対する耐性に基づいている。このフレームワークでは、暗号鍵は 0 と 1 からなる抽象的なビット列と捉えられている。このスキームのセキュリティを確実なものとするには、この列は真にランダム(そして勿論、秘密)でなければならない。

しかし、データの物理的セキュリティもまた重要である。例えば、政府や大組織を揺るがすようなセキュリティ違反は、外部者に許されていないような物理的アクセスのできる内部者が関与している場合が多い。このような違反は、デジタルの通路が遮断されていたとしても、強力なセキュリティプロトコルが使用されていたとしても発生しうる。暗号鍵は難解なランダム列ばかりでなく、セキュリティの確保された物理的装置に保存すべき物理的物体の場合もある。セキュリティを真剣に扱っている認証局は、インターネットで使われる殆どの証明書に使うルート鍵を保護するのに、事前対策及び遡及的策を取るばかりでなく、連邦情報処理標準(Federal Information Processing Standards, FIPS)140-2 のレベル 3 または 4 の認定を受けたハードウェアセキュリティモジュール(HSM)を使っている。このような包括的アプローチにより、物理的セキュリティのレベルはフォート・ノックス(訳注：装甲部隊本部と合衆国金銀塊保管所のある軍保有地)並みになっている。

面白いことに、ストレージアプリケーションについては物理的物体としての鍵についての理解は広く受け入れられているが、鍵配送についてはそこまで達しておらず、今なおデジタルな抽象化のレベルに留まっている。これは特に、第 8 節で解説する*量子鍵配送*(quantum key distribution, QKD)についてそうである。量子鍵配送は HSM(セキュリティソリューションの別の要素の中で、物理鍵を保存する)とよく似たやり方で、セキュリティソリューション全体の中の要素として使うことのできる物理的システムの一例である。量子コンピュータ自身は、データが単なるビット列ではなく、別の姿を取ることも可能で、予期せぬ結果をもたらすこともあるということの証明である。

新しいツールには、あらゆる物理的及び数学的セキュリティシステムを含むべきであり、各々固有の実践対象の分野がある。

5. クラウドコンピューティングが耐量子セキュリティ戦略に及ぼす影響

全ての IT ニーズがクラウドへ向かうという現在進行中の動向によって、データネットワークへの依存度は大いに高まった。データは巨大なデータセンターに保存され、それらの間を伝送されており、その速度は益々増大している。クラウドモデルによって—及び、それと関連したストレージとネットワーク要件によって—より強固かつ信頼性の高い IT インフラが可能になる。この、密にネットワーク化されたモデルでは、量子時代の新たな脅威ベクターが現れる。そのような脅威ベクターの中で最も深刻なものは「データボールティング(data vaulting)」即ち、今まさに存在するアタッカーが、後の実用に使える量子コンピュータが利用可能となった時に解読できるようにクライアントとクラウドの間の通信を保存しておくというタイプのハーベスト型アタックである。クラウド以前の時代は、そのようなデータは、アタッカーのアクセスできないプライベートなイントラネットを通してやり取りされていた。今日では、そのようなデータの多くが公衆の情報通信ネットワーク上を物理的に伝送されている。機密性と信頼は、暗号方式に基づく仮想専用網(VPN)を使うことによって取り戻すことができる。

昨今では、組織が公衆ネットワーク通信のトラフィック上でボールティングアタックを編成しているとニュースで報じられている。同時にまた、政府や金融機関やヘルスケア組織、あるいはその他のエンティティが記録を何十年も秘密のまま保存しておくことが求められている。驚くべきことに、データボールティングアタックを受けて積み上げられて今日送られている情報は、将来の量子コンピュータによって危険にさらされているかも知れない(もしもデータが監視され保存されていれば)のである。実際、汎用量子コンピュータはこれらの情報の機密指定が解かれる前に現われるかもしれない。

また、もしネットワークが量子コンピュータに耐えるように造り直されていなければ、ネットワークインフラ自体が、量子コンピュータによる夥しい攻撃活動によって深刻なリスクにさらされるだろう。量子コンピュータ時代には、*耐量子*に造り直されていないネットワークではサービス拒否攻撃(denial of service, DoS)が可能に—または普通にさえ—なり得る。巨大なクラウドのデータセンター上に「停まって」いるデータもまた、危険にさらされている。そのデータを保護している鍵の強度が量子コンピュータによって元の半分に落とされてしまうからである。また、量子コンピュータ時代のアタックベクターはそのデータのセキュリティを守るための鍵を生成、配送、保護する鍵管理システムを危険にさらすであろう。

何故、我々は、アタッカーが今から将来までという長い時間をかけてまでも、クラウドコンピューティングに対してアタックをしようとすると、予想するのか？このことは類推から説明できる: 1930 年代の高名なアメリカの銀行強盗ウィリー・サットンは記者に何故銀行を襲うのかと質問された。彼はこう答えたとされる:「なぜならそこに金があるからだ。」通信でつながった現代世界では、データは新しい資産である。ハッカーは自らの努力を最も沢山のデータの集まっている所、即ち前世紀の銀行に当たるものへ集中させる。実際、今日流通する通貨の殆どは紙幣として刷られてもおらずコインに鋳造されてもいない。それはデータ—1 と 0 の集合—で、データネットワーク上を安全に伝送されており、その最大に集中するところはクラウドのデータセンターである。これらの大規模なデータセンターの間のいかなる接続もリンクも可能な限り最高のレベルで保護されなければならない。クラウドベースの IT 環境には、*耐量子*サイバーセキュリティへのニーズが色濃く織り込まれている。

6. 現在の暗号ツール

6.1 ツール

我々にとって最も重要な通信プロトコルと鍵管理システムは主に、コアとなる 3 つの暗号機能に依存している:

- デジタル署名
- データの暗号化
- 鍵交換

これらの機能を実現するため、私達は幾つかの種類のツールを使うことができる。具体的には以下である:

- ハッシュ関数
- 対称暗号
- 非対称暗号
- 量子鍵配送(QKD)

これらのツールと機能の間の関係を表 1 に示す。

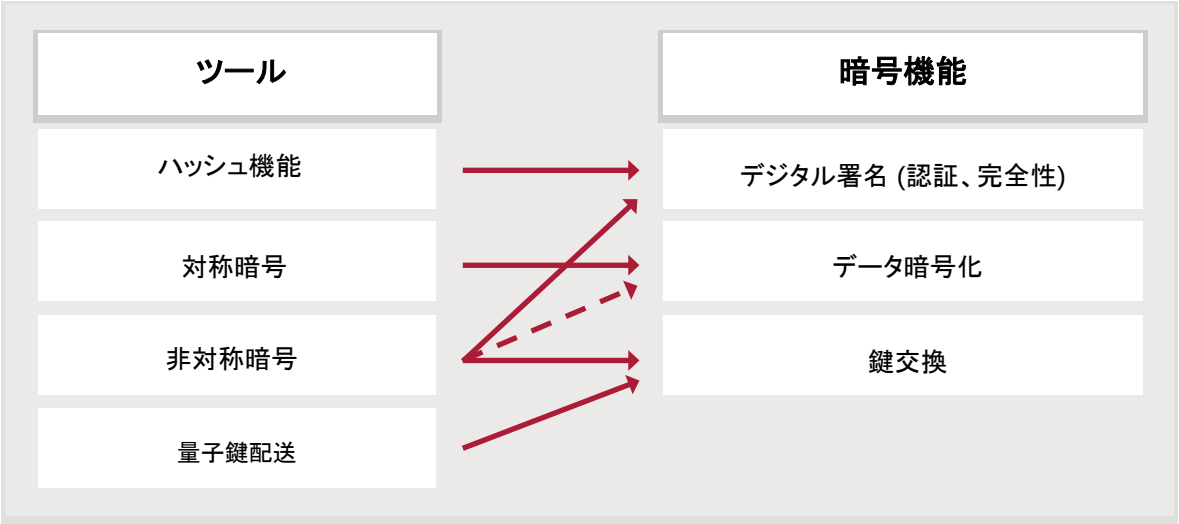

表 1: ツールと暗号機能の関係

ツールとその主要機能として適用される機能の間は赤の実線で結んである; 二次的に適用される機能との間は赤の点線で結んだ(詳細は本文を参照)

表 1 から解るように、非対称鍵暗号アルゴリズムは全ての機能で使うことができる [2]。しかしながら、これはデータの暗号化には通常使われることはない。これはそのスピードのためである。そのスピードのため、特に、あるハードウェア実装では、対称アルゴリズム(AES (米国政府の次世代標準暗号方式)など)がこの目的のために使われる。

[2] 但し、あらゆる非対称アルゴリズムが全ての機能に使用可能ではないことに注意されたい。

6. 2 ランダム性の必要性

上記の全ての機能がその実装のためにランダム性を必要としていることに注目することが重要である。QSS-WG[MHMW15] から出た最近のホワイトペーパーでこの必要性を説明し、量子乱数生成器(quantum random number generator, QRNG)を使うことを提案している。良い、信頼性のある乱数発生器はあらゆる暗号アプリケーションにとって必須である。

6.3 耐量子の現状

現在使われている標準非対称暗号アルゴリズムは Diffie-Hellman(DH)鍵交換、RSA 及び楕円曲線暗号(elliptic curve cryptography, ECC)である。これらのアルゴリズムは、その安全性を以下の数学上の困難問題に依拠している: 整数の素因数分解問題、離散対数問題、及び楕円曲線離散対数問題である。これらの問題は全て、十分な量子ビット数のある汎用量子コンピュータ上で動く Shor のアルゴリズム[Shor97]によって容易に解くことができる。例えば、4,000 量子ビットの量子コンピュータは 2048 ビットの RSA 暗号と DH 鍵交換を破ることが可能で、僅か 2,300 量子ビットの量子コンピュータが既に 384 ビットの ECC 暗号を破れるとされる。従って、上記のアルゴリズムのどれも量子コンピュータの出現には耐えられない。耐量子暗号アルゴリズムの鍵は、それらを古典的コンピュータでも量子コンピュータでも解くことのできない数学上の難問に基づいたものにすることである。

対称鍵暗号(AES、トリプル DES(Data Encryption Standard), 等)、及びハッシュ関数(SHA(Secure Hash Algorithm)-2、及びそれ以上、等)はそれほど容易には量子コンピュータに屈するものではない。「Grover の検索アルゴリズム」[Grover96]と呼ばれる量子コンピュータのアルゴリズムを使ってこれらにアタックすることができる。このアルゴリズムにできることは、古典的コンピュータでの検索アルゴリズムに対して最大でも二乗のオーダーでの高速化までである。また、検索アルゴリズムについて指数関数的高速化は不可能であることが示されている; これらのことから、対称鍵暗号アルゴリズムとハッシュ関数は量子コンピュータ時代にも使用可能と思われる。対称鍵暗号アルゴリズムにおいて Grover のアルゴリズムを相殺するための単純なアプローチは、対称鍵長とハッシュ関数長を二倍にすることであろう。

NIST の新しい文書 [CJLMPPS16] には、ハッシュ・対称暗号・非対称暗号に関する、現在の状況と量子コンピュータ時代への予測をまとめた表を掲載している。表と報告書から導かれる結論は二つある。以下は報告書それ自体からの引用である:

1. 「対称アルゴリズムとハッシュ関数は量子コンピュータ時代にも使用可能である…」
2. 「古典的コンピュータと量子コンピュータの両方のアタックに耐えると考えられるアルゴリズムの探索は、公開鍵アルゴリズムに注力されている….」

NIST はまた、耐量子の現状を(安全と考えられている)ハッシュ関数及び対称暗号と、有力候補ではあるが更なる吟味の必要な、新しい非対称暗号アルゴリズム(以下に詳しく述べる)をはっきりと分けて書いている。

量子コンピュータによるアタックへの耐性に関しては、QKD は別のクラスに属する。これは数学上の困難問題に基づいておらず、量子コンピュータがそのセキュリティに影響を与えないからである。

7. 耐量子アルゴリズムの候補

7.1 定義

量子コンピュータ時代に使用すべきアルゴリズムの用語はなお不確定である。現在、二つの(概ね)同等の用語がセキュリティ産業で使われている。耐量子アルゴリズム(post-quantum algorithm, PQA)と呼ぶ者もあれば、抗量子アルゴリズム(quantum-resistant algorithm, QRA)と呼ぶ方を好む者もある。ここで筆者らは、新しいアルゴリズムは量子コンピュータの力に対抗できなければならないという事実を伝える後者の用語を使うことにする。NIST の報告書[CJLMPPS16]によれば、現下の全ての暗号アプリケーションに使用可能な、十分な QRA 候補があり、以下で評価する。QSS-WG はこの問題について短いホワイトペーパー[CHH15]を発行しており、ETSI もまた詳細な文書を作成している[CHH15]。

7.2 対称暗号

ブロック暗号(AES が典型例である)やハッシュ関数(例: SHA2 または SHA3)などの基本的対称暗号は QRA である。実際、このような暗号に対して知られている量子アタックは Grover のアルゴリズム[Grover96]である。従って、量子コンピュータが出現した場合、鍵長を上げること(そしてビット数を倍にすること)が必要になる。現在推奨されている鍵長 256 ビットは、Grover のアルゴリズムに対しても安全と考えられている。

対称暗号はデータ暗号化に使われる。これは、ユーザー間で共有される秘密鍵の存在に依拠する。最も広範に使われるアルゴリズムである AES は QRA と広く信じられている。Grover のアルゴリズムにより、量子コンピュータが出現した場合、鍵長を上げること(ビット数を倍にすること)が必要になる。現在推奨されている鍵長 256 ビットは Grover のアルゴリズムに対しても安全と考えられる。

7.3 非対称鍵交換及び署名

セキュアな通信路を確立する過程で、公開鍵暗号は主に、認証及び秘密鍵の交換に使われ、秘密鍵はその後第 7.2 節にあるような対称スキームに適用される。筆者らは以下に最も有望なスキームを紹介する;しかしながら、この分野はなお目まぐるしく変化している。2016 年 2 月に始まった NIST のコンテストによって、これらの問題は一層進歩を促進されるだろう。

7.3.1 符号ベース暗号

McEliece 暗号[McE78]は 1978 年から知られており、まだ破られていない。これは最古の抗量子アルゴリズムである。誤り訂正符号に基づくその他の暗号も提案された。符号ベースの暗号は通常、非常に高速に暗号化と復号を行う。これらの符号ベースアルゴリズムは非常に大きな鍵長になる。最近になって、鍵長を短縮しようとして、新しい符号ベースの暗号アルゴリズム—符号に更に構造を加えたもの—が紹介された[MB09, MTSB13]。追加された構造は、提案されたこれらのものに対するアタックの成功につながり易い(例:[FOPT10], [FOPPT15]及び[JSG16])。符号ベース暗号は署名にも暗号化にも使うことができる[CFS01]。

7.3.2 格子(Lattice)ベース暗号

格子暗号は約 20 年前から存在して居り、非対称暗号及び署名を提供している。

提案されたオリジナルの格子暗号のうち、一つのスキーム—NTRU[HPS98]—はその期間、ずっと綿密に検討されてきた。その結果、NTRU は強化され、最終的に標準化された[9]。最近、「learning with errors」(LWE)[Reg05]や「ring learning with errors」(R-LWE) [RLWE13]などの新しい格子ベースアルゴリズムが提案され、現在、安全性評価を受けている。ごく最近、Google は同社がテストバージョンの Chrome で R-LWE をテストすると発表した[G16]。この、「New Hope」と呼ばれるアルゴリズムは Google の標準暗号方式と組み合わせて実装される(ハイブリッドシステムの説明については 9.3.1 節を参照)。2016 年 4 月、NIST の報告書[CJLMPPS16]では格子暗号の現状について以下のように要約を述べている:

> 「格子ベースの鍵確立アルゴリズムの殆どは比較的シンプルで効率的、かつ高度に並列処理可能である。また、一部の格子ベースシステムのセキュリティは、平均的ケースでなくワーストケースでの困難性の下で安全性が証明可能である。一方で、既知の解析技術によるその正確な安全性評価は、困難であることが明らかになっている。」

格子暗号はまた、署名や公開鍵/秘密鍵の暗号化以外に、準同型暗号[G09]やコード難読化のような他の重要な暗号分野にも拡げられている。

7.3.3 多変数暗号

多変数暗号は、有限体上の多項式による多変数連立方程式の求解が困難であることに基づいている。これは古くからの耐量子暗号候補—1980 年代後期から—であり、ETSI[CCDDFGZ15]や NIST [CJLMPPS16]からは十分に認識されている。C*という名で知られる最初の多変数スキームは、松本及び今井[MI88]によって提案された。C*は破られたが、松本－今井のスキームの一般原理は全世代の研究者を触発して、オリジナルの設計に基

づいた改良型の変形法が提案されるに至った([HFE96], [ETSI16]を参照)。多変数暗号では非常に沢山の方式設計と解析法が生み出されている([ETSI16], [DFSS], [FJ03], [BFP13]を参照)。全体として、状況は安定化して居り、最も強いスキームは時の試練に耐えてきた。多変数暗号は主に署名へのアプローチで成功している。多変数のスキームは抗量子アルゴリズムの中で最も短い署名を与えるからである。

7.3.4 ハッシュベース暗号

ハッシュベースの署名はハッシュ関数を使って構築されるデジタル署名である。その古典的コンピュータ及び量子コンピュータによるアタックに対するセキュリティは良く解明されている。しかしながら、現在あるハッシュベースの署名スキームは全て、非対称鍵ソリューションと比べて署名サイズが非常に大きい。一般に、ハッシュベースの署名では、秘密鍵は実際はサブ鍵の列から成っている。各署名は異なるサブ鍵によって行われる。もし同じサブ鍵が 2 回使われたら、公開鍵全体の安全性が危険にさらされる。従って、安全な署名を行うには、以下の 2 つの動作のうち一つが行われなければならない：署名者が使われたことのある全てのサブ鍵の記録を保持する(ステートフル署名)；または、鍵に十分多くのサブ鍵が—その結果大きな秘密鍵が—あるようにして、無作為に鍵を選ぶとき同じ鍵が二度選択される可能性がなくなるようにする(ステートレス署名)。XMSS[XMSS]は、署名サイズが大きくなるステートフルなハッシュベース署名スキームで、現在標準化が進められている[6]。SPHINX[SPHINX15]はステートレスな、鍵サイズが大きく署名サイズも非常に大きいハッシュベース署名スキームである。そして、Leighton-Micali 署名スキーム(LMSS)は Merkle 木ベースのアプローチを Lamport-Diffie-Winternitz-Merkle のワンタイム署名スキームでインスタンス化したものである。インターネット技術タスクフォース(IETF)はこの技術の、David McGrew の書いたドラフトを評価しているところである。盗聴者がデータを後の使用のために保存しておくハーベストアタックは(第 2 節及び 5 節で述べたように)署名方式には当てはまらない。署名は伝送直後に検証される。

8. 量子鍵配送の現状

8.1 原理

量子鍵配送 (QKD) [GRTZ02]は二人のユーザーの間で秘密鍵を共有する方法を提供する。これは透過的なチャネル上で物理的な粒子、通常は光子を搬送することに基づいている。基本的発想は、伝送チャネル上で盗聴を試みるいかなる動きを行っても、それは粒子の測定となるため、その状態が変わってしまう。この変化は正当なユーザーに発見され、交換(した鍵)を破棄することができる。QKD についての簡単な入門は QSS-WG の過去のホワイトペーパー[MHHWK15]に掲載されている。その機密性は数学的前提や結果に基づくものではなく、量子力学原理から理論的に証明済みである。このカギは後に如何なる暗号化目的にでも使うことができる。今のところ、主要な応用は暗号化で、特に対称鍵暗号と組み合わせて使われる。情報理論的にセキュアな暗号もまた QKD とワンタイムパッドによって実現できる。QKD は計算に基づいていないので、本質的に量子コンピュータに対して安全である：量子コンピュータはその安全性に何らの影響も及ぼさない。

8.2 物理的リンクの必要性

上記で説明したように、QKD には物理的粒子をいわゆる量子チャネル上で搬送することが必要である。チャネルでの損失が不可避なので、QKD リンクの長さに限界が生じる。QKD の商用での実装には広く利用可能な、通信で使う光ファイバーインフラが使われる。QKD チャネルの通常の長さは数 10 キロメートル程度である(最大は約 100 キロメートル)。しかしながら、学問的原理証明系では 300 キロメートルまでが達成されている。自由空間(free space)の実装ができればソリューションのコストを下げて最大長を上げることができるが、この技術はまだ研究段階である。QKD ネットワークの長さは、複数の QKD リンクが安全な場所(通信交換機など)で接続される信頼ノードインフラを使って伸ばすことができる。例えば、北京と上海をつなぐ QKD バックボーンは現在建設中である。技術の改良によって、世界的な QKD ネットワークも視野に入れることができる(第 8.6 節を参照)。

8.3 リアルタイムの盗聴

QKD に物理リンクがなければならないという事実は、障壁と見なされているが、これは間違いではない。しかしながら、見方によっては、優位点でもある。アルゴリズムベースの鍵配送と QKD のはっきりした違いは、後者では盗聴者が伝送の際にしか鍵の発見を試みることができない。伝送の完了時、正当なユーザーはその鍵が安全かを知ることができる。QKD が使われるときも、この基本的図式は変わらない：盗聴者はこれらの瞬間に鍵を傍受するか、そうでなければ知らないままでいるしかない。

全てを考えに入れると、QKD の優位点は、この技術が既存の技術にのみ対抗すれば良いということである。もしも既存の技術で鍵を傍受することができなければ、将来のより優れた技術でそれ以上の情報を得ることもできない。それと比べて、アルゴリズムによるシステムは既存と将来の両方の脅威に対して考慮するという、ずっと困難な課題に取り組まなければならない。まさしく、第 2 節及び 5 節で述べたハーベストアタックはデータだけでなく鍵に対しても行うことができる。20 年 30 年先に、技術及び数学にどのような進歩があるだろうかとは誰もが考えるだろう。しかしながら、ある事例が訓話として役に立つだろう：1977 年、RSA アルゴリズムが初めて導入されたときに、サイエンティフィック・アメリカンのある記事では、その時代使われていた鍵長で暗号化されたメッセージを解読するには 4 京(4×10^{16})年かかるとしていた。実際にはその鍵は 20 年以内に解析された。

8.4 認証と署名

QKD は、セキュリティの課題の広い範囲の中で、ある特定の問題にのみ対処するものである: 具体的には、鍵配送である。完全なソリューションを与えるには、既存の暗号ツールを追加しなければならない。特に、耐量子認証及び署名—及び耐量子暗号—が必要である。幸い、第 7.3.3 節に述べた QRA が必要なツールを提供できる。

8.5 量子ハッキング及び認証

QKD の大きな優位点は、理論的にセキュアであることが証明されていることである。やり取りの中から情報を取り出そうとするいかなる盗聴者の試みも見つけ出すことができる。しかしながら、これは実装での欠陥も起らないようになっているということではない。安全性証明は、盗聴者が伝送チャネルにしかアクセスできない場合に当てはまる。より進化した戦略では、盗聴者がユーザーに対して、所謂「サイドチャネルアタック」によってアクセスを得る仕組みの設計[BP12]も成功した。これは量子ハッキングの領域である。

サイドチャネルアタックは QKD に限定されるものでも、物理ベースの暗号に限定されるものでもない。最終的には、どんな暗号実装も、数値を後から後から出してゆくコンピュータのような、何らかの物理システムに基づいたものである。実際、音響解析—暗号処理を行っているコンピュータから発せられるノイズを基にするサイドチャネルアタック—で RSA 暗号を破れることが示されている。その他のアタックは電磁波の放射を対象にしている。ひとたび攻撃法が知られたら、その対応策を実装するのは比較的容易である。しかしながら、このようなタイプのアタックが白日のもとに曝したのは、いかなる安全性証明も所与の前提の上に成り立っており、知恵のある盗聴者はそれを回避する方法を見つけられるということである。暗号スキームについて核心を得たければ、スキームの実装を徹底的に吟味し、様々な形式のアタックに晒さなければならない。その後、実装のガイドラインを然るべき認定団体が作ることができる。

従来型の暗号に対しては、量子ハッキングはサイドチャネルアタックと何ら異なるものではない。量子世界は暗号学者とハッカーの死闘に新しい側面を与えるだけである。従来型の暗号の既存の実装は、適切な認証があれば、様々なアタックが考慮されており、実装が一連のルールに従っている、ということが確認できる。QKD インフラを信頼あるものとするには、適切な認証の仕組みを開発することが絶対に必要である。

8.6 未来の世界的 QKD ネットワーク

広範に QKD が使われるようになるのに最も影響の大きい制約は、QKD リンクの距離である。しかしながら、それは根本的制約ではない。この先 10 年から 15 年の間に量子コンピュータの出現を先導するのと同じ技術が、また QKD の短所に対するソリューションをも生み出すだろう。世界的な QKD ネットワークは明らかに実現可能なものである。このシステムは、信頼できるノードとして衛星を使うことで、安全に秘密鍵を地上と交換し、安全に秘密鍵を保存し、別の場所へ鍵を運ぶことができるだろう。実際、最初の QKD 衛星が最近、中国科学院(Chinese Academy of Science)によって打ち上げられた[X16]。科学院の目的は、宇宙空間の QKD について原理証明を与えることである。この信頼できるノードは後に、量子リピーターの使用によって信頼されないノードに代替され、その結果量子リンクの距離の制約をなくすことができるだろう。量子メモリ—量子ビット(量子コンピュータにおいて通常のビットに当たるもの)を保存しておいて、後でコンピューティングに使うもの—があれば、鍵はあぶりだされることなく、使用の時まで量子状態に置いておくことができる。

これらの新しい構成要素—量子コンピュータのために構築されるもの—は、あらゆる所に秘密鍵を配送することのできる完全な QKD インフラを構築するのに使うことが可能である。この QKD ネットワークは高価なもので、低レベルの暗号化に使うことはできないだろう。しかし、それは、他の型式のデータのために必要なコンピューティング（従来型または量子型）の将来の進歩(またはそれができないこと)とは無関係に、真に長期間の機密とプライバシーの維持を可能にするだろう。

もし私達が自分らの水晶玉をもう少し深く覗きこんでみれば、完全量子のインターネットを見ることができるだろう。ひとたび私達が量子ビットを配送することも保存することも取り扱うことも可能になれば、私達は量子レベルの新しいレイヤを構築することもできる。この量子レイヤはインターネットの構造に組み込まれ、透過的になる。このシナリオはまさしく、私達が今日使っている光のレイヤをなぞるものである。インターネットは物理的物体、具体的には、別々の点の間で光パルスを伝送することに依存している。しかしながら、光レイヤは完全に組み込まれており、使う人達は下のレイヤに何があるのかを知ることさえない。

9. 耐量子への再作成

QSS-WG の目指す処の一つは、産業界に*耐量子(quantum-safe)*セキュリティを達成するための実践的な助言を提供することである。量子コンピュータの開発が提起した脅威—これは行動を取る必要性の根拠となるだけの確かさがあり、かつ実現は遠く、私達が対応をとるだけの時間が十分取れる—は、私達が自分らの暗号ツールボックスを開けて情報を保護する新しい方法を見つける良い機会だろう。第 6.1 節や第 9 節で定義した三つの主要な暗号機能を良く考えてみると、各機能のための現在及び将来の、直ちに実装することのできる耐量子セキュリティが見えてくるだろう。

9.1 耐量子署名及び認証

抗量子署名及び認証のスキームは第 7.3 節で紹介した。その中には、実践的で既に暗号のコミュニティの中で受け入れられているものもある。これらの分野でも非常に沢山の新しい成果が予想されるが、私達が量子コンピュータ時代の署名と認証への道のりへ歩を踏み出せるだけの効果的な耐量子署名アルゴリズムは現在既に存在する。署名と認証は絶対的に情報セキュリティの根本であることに注意されたい。インターネットは、プライバシーの低い商用ツールとして残るだろうが、認証と完全性が侵された場合には、量子コンピューティングの脅威に耐えることはできない。

9.2 耐量子データ暗号化

データ暗号化は、比較的「容易な」部分である。それは主に対称暗号に依拠しており、これらは量子コンピュータによって劇的に危険にさらされるわけではないからである。256 ビット鍵の AES は古典的コンピュータと量子コンピュータどちらのアタックに対しても安全と考えられている。もし新しい脅威が発生したら、鍵長は将来増やすことができるだろう。

9.3 耐量子鍵交換

9.3.1 ハイブリッドシステム

現在は、鍵交換及び非対称暗号化のための幾つかの抗量子公開鍵アルゴリズムが利用可能である。一部は綿密に点検されており、一つは標準化が行われている。標準化に加えて、実装者の多くは政府によって認可されたアルゴリズム(例：NIST SP800-131a、NSA スイート B、ISO 標準等)を使うことを好む—または要求される。しかしながら、政府はまだその認可アルゴリズムリストに抗量子アルゴリズムを含めていない。幸い、私達は現在の通信を耐量子(quantum-safe)とする取組みに足踏みする必要はない。解決策は存在し、これは「耐量子ハイブリッド技術(QSH)」と呼ばれていて、標準化され認可された方法と抗量子アルゴリズムを混合したものである。QSH は FIPS 140-2 準拠となるように実装することも可能で、特定の抗量子暗号アルゴリズムに特化したものでもない。これはインターネット技術タスクフォース(IETF)ドラフト[SWZ02]として発行され、現在は IETF の RFC 文書化が進められている。

ハイブリッドシステムの実践例として、QSH がどのように TLS(Transport Layer Security)で既存のアルゴリズムと抗量子アルゴリズムを一緒に使う方法、つまり TLS セッション対称鍵をネゴシエーションするときのやり取りを調べてみる。TLS セッション鍵は、非対称暗号アルゴリズムを使ってネゴシエーションされる共有対称鍵である。通信セッションをネゴシエーションする 2 者の間で*耐量子*コンポーネントを伝送するために、追加の耐量子アルゴリズムが使われる。以下は、QSH の主要部分である：

- 実装者は、TLS セッション鍵ネゴシエーションで、認可されたアルゴリズムを使い続けることが可能で、かつそれらを*耐量子*とすることができる。もし元の実装が FIPS 140-2 準拠であれば、*耐量子*のコンポーネントの追加を実装するときも FIPS 140-2 準拠性は保持される。
- 必要な耐量子コンポーネントが TLS 鍵生成関数に追加される。TLS 通信セッションの各パーティはその鍵導出関数(key derivation function, KDF)を使って、秘匿通信に必要な共有の対称セッション鍵を生成する。
- 今日では、現行の暗号アルゴリズムのみを TLS セッション鍵のネゴシエーションに使った場合、量子コンピュータはセッションの秘密鍵の平文を暴くことができる。抗量子暗号アルゴリズム及び*耐量子*コンポーネントを追加することで、TLS セッション鍵が量子コンピュータによって暴かれることは阻止することができる。今日のデータの機密性のハーベストアタック(第 2 節及び第 5 節を参照)に対する保護は量子コンピュータ時代になっても維持することができる。

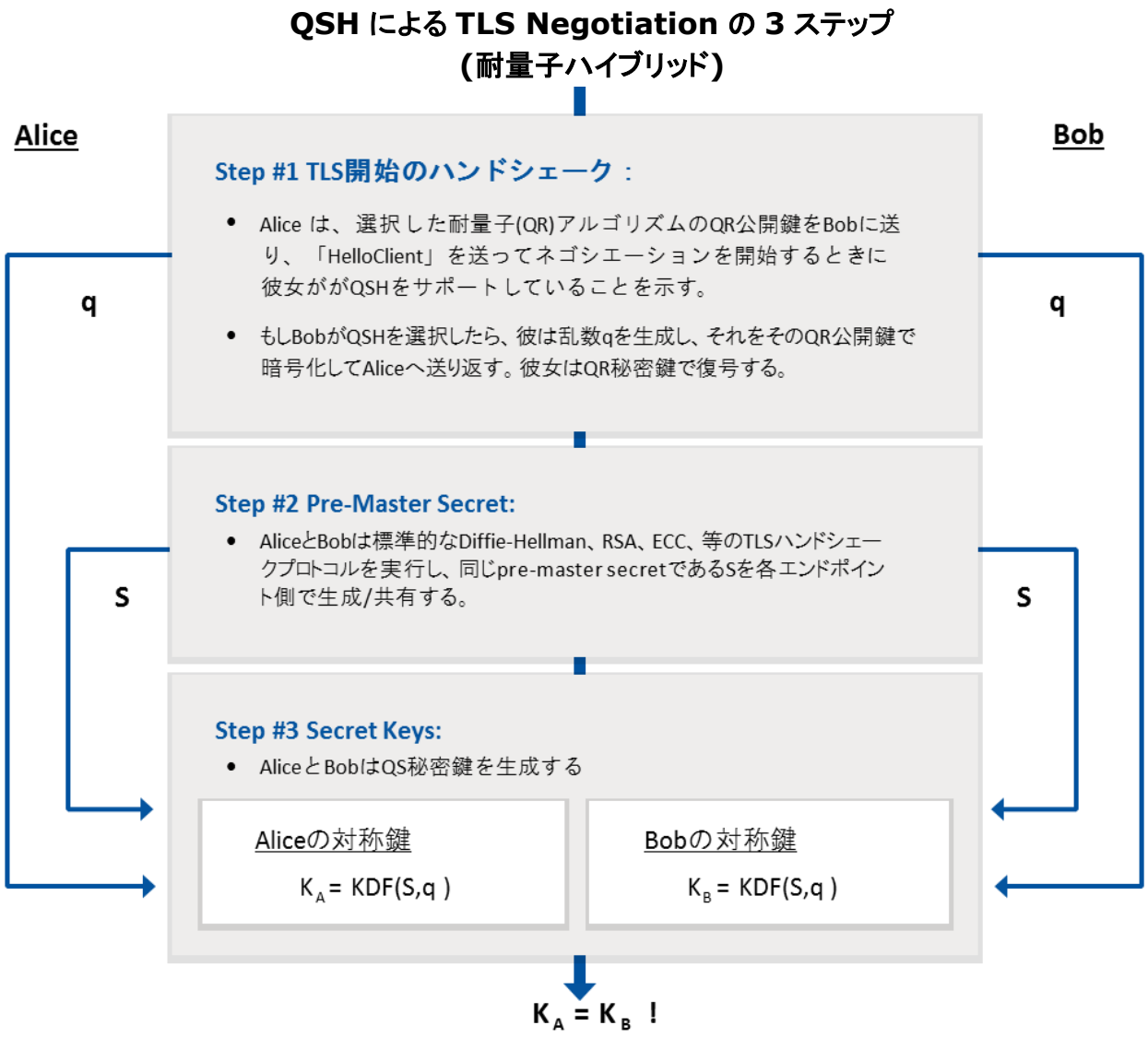

図 1: TLS プロトコルでの QSH ネゴシエーションのフロー
(KDF は Key Derivation Function(鍵導出関数)を表わす)

QSH 技術は TLS 以外にも様々な鍵確立/鍵交換の環境に拡げることができる。

9.3.2 高価値リンク用アドオンとしての QKD

第 8.3 節で論じたように、QKD の原理的優位性は、盗聴者が試みることができる唯一のアタックはリアルタイムでなければならない、ということである。もし盗聴者が鍵に関する情報を伝送の際に盗もうとしなかったら、正当なユーザー間の全てのトランザクションをダウンロードして保存していても何も得ることはできない。更にまた、QKD の性質によりそのような試みは正当なユーザーによって発見されてしまう。伝送の終了時に、ユーザーは鍵が安全であるか、あるいは破棄しなければならないかを知ることができる。従って、高価値のリンクでは、QKD の追加によって、安全性のもう一つのレイヤ(これは耐量子であることが知られている)が加えられる。新しいタイプのハイブリッドシステム—特に、QKD レイヤを加えながらいかなる非対称暗号システム(上記 QSH を含む)をも使えるもの—は最高のセキュリティレベルを、特に長期的セキュリティの求められるリンクに対して保証する。これは、第 7 節で述べた*耐量子*署名及び認証プロトコルと併せて使うべきである。このシステムは、耐量子コンピュータのような技術進歩や数学上の新しい進歩による脅威を受けない。しかし、その現在の長さに対する制約や高いコストゆえに、どこにでも適用できるものではない。これは特定のリンク(例えばデータセンタ

一間)、及び長期的にプライバシー保護することが要求される全てのリンクに使用すべきである。

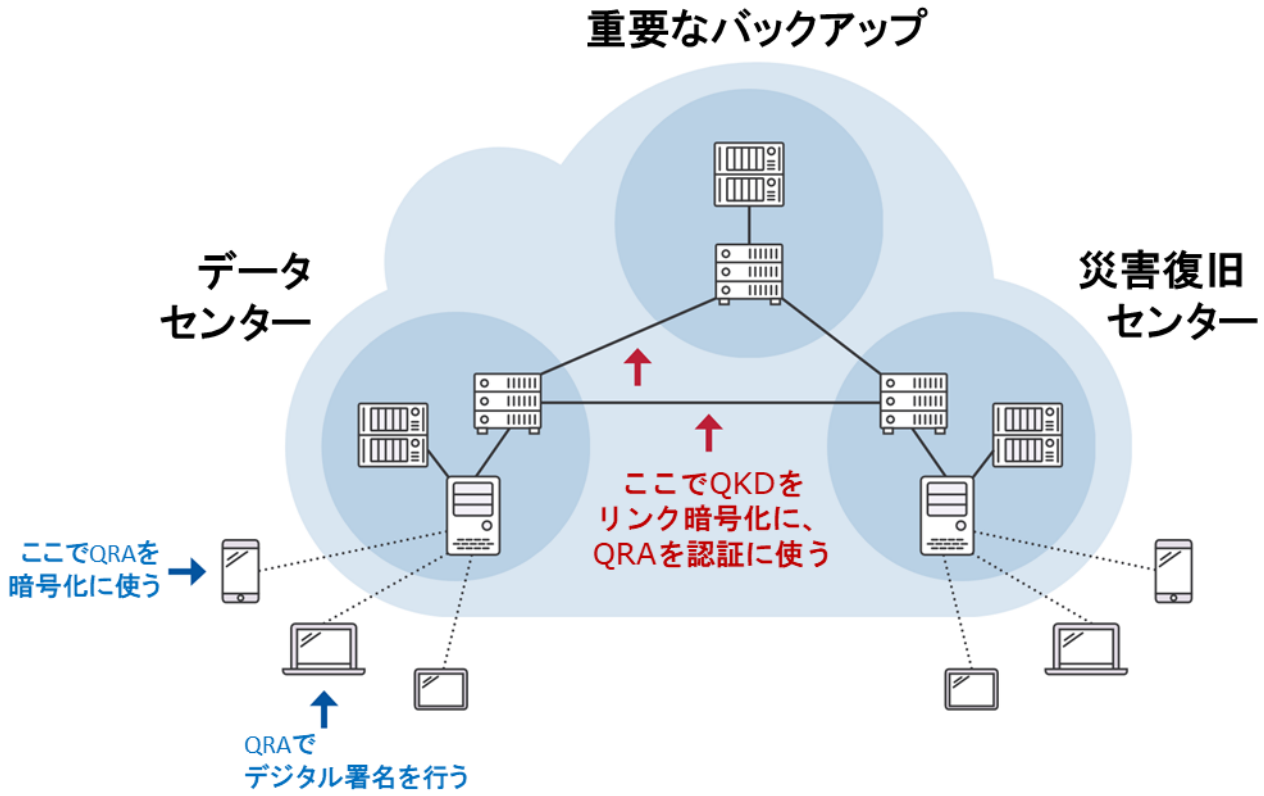

図 2: QRA 及び QKD のユースケース

データセンターとユーザーの間のリンクは、暗号化と署名のための QRA で保護される。

データセンターとバックアップまたは災害復旧センターの間の更に重要なリンクは QKD によって保護される。このことを図 2 に例示する。QKD と QRA のアプリケーションのユースケースを示している。高価値のリンクには長期間の保護が必要で、これは QKD によって実現される。遠からず量子技術が進歩することによって、距離の限界はなくなり、世界中に QKD ネットワークを広げることが可能になる。

10. 結論

「予測することは非常に難しい。特にそれが未来に関する場合には。」

—ニールス・ボーア

ニールス・ボーアからのこの有名な引用は、サイバーセキュリティに関する現状に良くあてはまると思われる。長期におけるサイバーセキュリティの方向を予測することは非常に難しい。しかしながら、確かだと思われるのは、我々の現在のツールキットを量子コンピュータの潜在的脅威に応じることができるように完全に改造しなければならない、ということである。1 年ほど前まで、量子コンピュータの実現可能性はなお答えの出ない問題だったが、NSA や NIST による最近の声明によってこの均衡は変わった。サイバーセキュリティのコミュニティ内では殆どの人が、暗号に関係する量子コンピュータが手に入ることは時間と投資の問題だけであると信じている。良いニュースは、私達は量子コンピュータ時代の脅威に対応するための予定を立てる助けになるような意義ある情報を持っている、ということである。第 2 節で、筆者達は暗号解読のできる汎用量子コンピュータ出現までのタイムラインを示した。その開発ができる確率は 2020 年代の初めから大きく上昇する。非常にセキュリティ要件の高い業種(ヘルスケアや金融セクター等)にとっては、準備は量子コンピュータが現実の脅威となる前に完了しなければならない。準備ができている、とは、それらのシステムが完全に耐量子に造り直されていなければならない、ということである。これは注目すべき大仕事である。もしも彼らが賭けに負けて量子コンピュータが彼らの予想よりも早く現れたら、結果は破滅的なものになる。今日インターネット上で伝送されるデータは既に危険にさらされている可能性がある。なぜならその多くは量子コンピュータの脅威が現れた後も機密であることが要求されているからである。

今日では、情報セキュリティに携わる人達のうちかなりの割合は耐量子暗号や QKD になじみがない。IT 産業が完全耐量子の情報セキュリティインフラへの整然とした移行を行うための「量子コンピュータリスクマネジメントプラン」(量子コンピューティング研究所による用語)を立てようとしている、ということは重要である。我々皆が、耐量子のサイバーセキュリティ対策と技術について理解し始める必要がある。本当は、量子コンピュータ時代の脅威のうち特定の重要ないくつかの点については、政府や標準化機関と共に行わなければならない仕事がまだ山ほど残っている。しかしながら、私達が耐量子サイバーセキュリティのために計画を立て始められる分野は沢山あり、あるものに対しては、今行動を起こす必要がある。

付属資料

11. 用語の解説

- **量子技術:** 量子力学の特定の方面、具体的にはコヒーレント重ね合わせ及びもつれに依拠する技術。QKD と量子コンピュータがこれらの技術でサイバーセキュリティに関係するものの例である。

- **耐量子暗号:** 広い意味の言葉で、通常、量子アルゴリズムを実行できるコンピュータに対抗できる暗号スキームを指す。これには、QKD のように量子技術に依拠した、物理学に基づいた暗号方式、及びアルゴリズム的暗号方式(候補として:格子ベース、多変数多項式ベース、ハッシュベース、及び同種(isogeny)ベースの暗号方式等)があげられる。

- **耐量子(quantum-safe):** この用語は、暗号スキーム及びセキュリティプロトコルについて、耐量子(post-quantum)と同義に使われる。量子コンピュータの実現及び量子アルゴリズムの実装がなされてもそれに耐えられるものを言う。この用語は ETSI 及び CSA 耐量子セキュリティワーキンググループで使われる。

- **抗量子アルゴリズム:** 現在のコンピュータエコシステムで耐量子セキュリティを実現する、アルゴリズムベースの暗号方式を言う。これは NSA がその「抗量子アルゴリズムへの移行への予備計画」に関する発表で一貫して使っていた用語である。抗量子という用語は、量子コンピュータによるアタックの影響を受けない暗号アルゴリズム、または抗量子アルゴリズムを使ったセキュリティプロトコルを実装したセキュリティソリューションを形容するのに使われる。

- **量子攻撃:** セキュリティシステムに対する攻撃で、そのセキュリティを破るのに量子コンピュータ上で実行される量子アルゴリズムに依拠するもの。

- **量子鍵配送(quantum key distribution, QKD):** 量子技術に依拠して耐量子セキュリティを提供する暗号プリミティブ。

- **暗号プリミティブ:** セキュリティプロトコルや暗号方式を構築するのに使うことのできる低レベルの暗号アルゴリズム。

- **実用的量子コンピュータ:** 従来型の公開鍵暗号を破るために 1 つ以上の Shor または Grover のアルゴリズムを実行できるコンピュータ; 暗号関連(cryptographically relevant)または汎用的量子コンピュータ(universal quantum computer)とも呼ばれる。

参考文献

[BFP13] Bettale, L., Faugère, J.-C.,& Perret, L. (2013). Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic. *Designs, Codes and Cryptography*, 69 (1), pp. 1–52

[SPHINCS15] Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., & Wilcox-O'Hearn, Z. (2015). SPHINCS: Practical Stateless Hash-Based Signatures. In:
Oswald, E. & Fischlin, M. (Eds.) *Advances in Cryptology—EUROCRYPT 2015* (pp. 368-397). Lecture Notes in Computer Science, Vol. 9056. Springer Berlin Heidelberg

[BP12] Braunstein, S. L., & Pirandola, S. (2012). Side-Channel-Free Quantum Key Distribution. *Physical Review Letters* 108 (13).

[BDH11, XMSS] Buchmann, J., Dahmen, E., & Hülsing, A. (2011). XMSS: A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In: Yang, B.-Y. (Ed.) *Post-Quantum Cryptography* (pp. 117-129) Lecture Notes in Computer Science, Vol. 7071. Springer Berlin Heidelberg

[CCDDFGZ15] Campagna, M., Chen, L., Dagdelen, Ö., Ding, J., Fernick, J.K., Gisin, N., … Zhang, Z. (2015). Quantum Safe Cryptography and Security. [White Paper]. No. 8, June 2015. European Telecommunications Standards Institute. Retrieved January 17, 2017, http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[CHH15] Carter, G., Hayford, D. & Huttner, B. (2015). What is Post-Quantum Cryptography? [White Paper]. Cloud Security Alliance.

[CJLMPPS16] Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). NISTIR 8105
DRAFT: Report on Post-Quantum Cryptography. N*ational Institute of Standards and Technology Internal Report 8105* (February 2016). Gaithersburg, MD: U.S. Department of Commerce. Retrieved January 17, 2017, from http://csrc. nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf

[CFS01] Courtois, N.T., Finiasz, M., & Sendrier, N. (2001). How to Achieve a McEliece-Based Digital Signature Scheme. In: Boyd, C. (Ed.), *Advances in Cryptology—ASIACRYPT 2001* (pp. 157-174). Lecture Notes in Computer Science, Vol. 2248. Springer Berlin Heidelberg

[DFSS] Dubois, V., Fouque, P-A., Shamir, A., & Stern, J. (2007). Practical Cryptanalysis of SFLASH. In: Menezes, A. (Ed.),
Advances in Cryptology—CRYPTO 2007 (pp. 1-12). Lecture Notes in Computer Science, Vol. 4622. Springer Berlin Heidelberg

[ETSI16] ETSI Industry Specification Group (ISG) Quantum-Safe Cryptography (QSC). (July 2016) Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. [Group Report]. Retrieved from ETSI http://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf

[FJ03] Faugère, J-C., & Joux, A. (2003). Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In: Boneh, D. (Ed.), *Advances in Cryptology*—CRYPTO 2003 (pp. 44-60). Lecture Notes in Computer Science, Vol. 2729. Springer Berlin Heidelberg

[FOPT10] Faugère, J-C., Otmani, A., Perret, L. & Tillich, J-P. (2010). Algebraic Cryptanalysis of McEliece Variants with Compact Keys. In: Gilbert, H. (Ed.), Advances in Cryptology—*EUROCRYPT 2010* (pp. 279-298). Lecture Notes in Computer Science, Vol. 6110. Springer Berlin Heidelberg

[FOPPT15] Faugère, J.-C., Otmani, A., Perret, L., Portzamparc, F., & Tillich, J-P. (2016). Structural cryptanalysis of McEliece schemes with compact keys. *Designs, Codes and Cryptography*, 79 (1), pp. 87-112

[G09] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *STOC '09 Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178). New York, NY: ACM Publications.

[GRTZ02] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002) Quantum Cryptraphy. *Reviews of Modern Physics*, 74 (1), pp. 145-195. Retrieved January 17, 2017, from https://d22izw7byeupn1.cloudfront.net/files/RevModPhys.74.145.pdf

[Grover96] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *STOC '96 Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp 212-219). New York, NY: ACM Publications.

[G16] Greenberg, A. (2016, July 7) Google Tests New Crypto in Chrome to Fend Off Quantum Attacks. *Wired*. Retrieved January 17, 2017, from https://www.wired.com/2016/07/google-tests-new-crypto-chrome-fend-offquantum-attacks

[JSG16] Guo, Q., Johansson, T., & Stankovski, P. (2016). A Key Recovery Attack on MDPC with CCA Security Using

Decoding Errors. In: Cheon, J.H. & Takagi, T. (Eds.), *Advances in Cryptology—ASIACRYPT 2016* (pp. 789-815). Lecture

Notes in Computer Science, Vol. 10031. Springer Berlin Heidelberg

[HPS98] Hoffstein, J., Pipher, J., & Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (Ed.), *Algorithmic Number Theory* (pp. 267-288). Lecture Notes in Computer Science, Vol. 1423. Springer Berlin Heidelberg

[K14] Klarreich, E. (2014, February 3) Cryptography Breakthrough Could Make Software Unhackable. *Quanta Magazine*. Retrieved January 17, 2017, from https://www.wired.com/2014/02/cryptography-breakthrough

[KPG99] Kipnis, A., Patarin, J., & Goubin, L. (1999). Unbalanced Oil and Vinegar Signature Schemes. In: Stern, J. (Ed.), *Advances in Cryptology—EUROCRYPT '99* (pp. 206-222). Lecture Notes in Computer Science, Vol. 1592.
Springer Berlin Heidelberg

[RLWE13] Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On Ideal Lattices and Learning with Errors over Rings. *Journal of the ACM (JACM)*, 60 (6), Article No. 43

[MHHWK15] Melia, J., Huttner, B., Hayford, D., Walenta, N., & Kerling, F. (2015). What is Quantum Key Distribution? [White Paper]. Cloud Security Alliance.

[MHMW15] Melia, J., Huttner, B., Moulds, R., Walenta, N., & Fuller, A. (2016). Quantum-Safe Security Working Group: Quantum Random Number Generators. [White Paper]. Cloud Security Alliance.

[MB09] Misoczki, R., & Barreto, P.S.L.M. (2009). Compact McEliece Keys from Goppa Codes. In: Jacobson, M. J.,

Riimen, V., & Safavi-Naini, R. (Eds.), *Selected Areas in Cryptology* (pp. 376-392). Lecture Notes in Computer Science, Vol. 5867. Springer Berlin Heidelberg

[MTSB13] Misoczki, R., Tillich, J.-P., Sendrier, N., & Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. *2013 IEEE International Symposium on Information Theory* (pp 2069-2073). Istanbul, Turkey: IEEE

[McE78] R.-J. McEliece (1978). A Public-Key Cryptosystem Based on Algebraic Coding Theory. T*he Deep Space Network Progress Report* (No. 42-44, pp 114-116). Pasadena, CA: National Aeronautics and Space Administration.

[NTRU09] NTRU Cryptosystems, Inc. (2009, February 18) *NTRU Announces That IEEE Has Approved the Standardization of NTRUEncrypt* [Press Release]. Acton, Mass.: BusinessWire.

[NTRU11] NTRU Cryptosystems, Inc. (2011, April 11) Security Innovation's NTRUEncrypt Adopted as X9 Standard for Data Protection [Press Release]. Wilmington, Mass.: BusinessWire.

[Reg05] Regev, O. (2005). On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *STOC '05 Proceedings of the thirty-seventh annual ACM symposium on Theory of computing* (pp 84-93). New York, NY: ACM Publications.

[MI88] Matsumoto, T. & Imai, H. (1998). Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: Barstow, D., Brauer, W., Hansen, P.B., Gries, D., Luckham, D., Moler, C., Pnueli, A., Seegmüller, G., Stoer, J., Wirth, N, & Günther, C.G.(Eds.), *Advances in Cryptology—EUROCRYPT '88* (pp. 419-453).
Lecture Notes in Computer Science, Vol. 330. Springer Berlin Heidelberg

[M2016] Moody, D. (2016, February). Post-Quantum Cryptography: NIST's Plan for the Future. Presented at The Seventh International Conference on Post-Quantum Cryptography, Fukuoka, Japan. Retrieved January 17, 2017, from http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf

[HFE96] Patarin, J. (1996). Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U. (Ed.), *Advances in Cryptology—EUROCRYPT '96* (pp. 33-48). Lecture Notes in Computer Science, Vol. 1070. Springer Berlin Heidelberg

[Shor97] Shor, P.W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*., 26 (5), pp. 1484–1509

[SWZ02] Schanck, J.M., Whyte, W., Zhang, Z. (2015). *Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.3.(Internet Engineering Task Force Draft)*. Retrieved January 17, 2017, from https://datatracker. ietf.org/doc/draft-whyte-qsh-tls13/.https://datatracker.ietf.org/doc/draft-whyte-qsh-tls13/

[X16] Xinhua (2016, August 16) China Launches First-Ever Quantum Communication Satellite. *Xinhua*. Retrieved January 17, 2017, from http://news.xinhuanet.com/english/2016-08/16/c_135601026.htm