量子コンピュータ開発の進展と次世代暗号

宇根正志（うねまさし）／菅　和聖（かんかずとし）

要　旨

大規模な量子コンピュータが実用化されると、金融分野をはじめとして、現在広く利用されている公開鍵暗号（RSA 暗号や楕円曲線暗号）の安全性が損なわれることが知られている。現状では、こうしたリスクが近い将来顕現化する可能性は小さいが、米国立標準技術研究所は、大規模な量子コンピュータが仮に登場した場合でも安全性を確保できる次世代暗号（耐量子計算機暗号）の標準化を進めており、現在 15 件（最終候補 7 件、代替候補 8 件）の方式の技術検証を行っている。標準化が完了すれば、米国政府のみならず、さまざまな分野において暗号方式の移行に向けた動きが加速する公算が高い。本稿では、量子コンピュータの研究開発の現状や、現行の公開鍵暗号の安全性低下のリスクについて説明した後、暗号の早期移行の必要性について考察する。次に、米国政府による標準化の動向や、これを受けた産業界および本邦における暗号移行に向けた動向を整理する。最後に、次世代暗号への移行にかかる課題について考察する。

キーワード：公開鍵暗号、耐量子計算機暗号、楕円曲線暗号、量子コンピュータ、RSA 暗号

本稿は、2021 年 1 月 8 日時点の情報に基づいて執筆したものである。本稿の作成に当たっては、安田雅哉准教授（立教大学）、田渕豊ユニットリーダー（理化学研究所）から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

宇根正志　日本銀行金融研究所企画役（E-mail: masashi.une@boj.or.jp）
菅　和聖　日本銀行金融研究所企画役（E-mail: kazutoshi.kan@boj.or.jp）

無断での転載・複製はご遠慮下さい。

1. はじめに

近年、世界中で量子コンピュータの研究開発が活発化している。取り扱うデータ量や演算回数に制限があるなど機能面では不完全なものの、International Business Machines Corporation（IBM）や Google LLC、Rigetti & Co, Inc. 等が開発しているものをはじめ、一部で利用可能な実機が提供され始めている。仮に、量子コンピュータ関連の技術が今後成熟し、大規模な量子コンピュータが実現すれば、社会インフラとして広く利用されている公開鍵暗号（RSA 暗号や楕円曲線暗号）の安全性が低下（危殆化）するとみられ、その社会的な影響は甚大となりうる。本稿執筆時点では、量子コンピュータは公開鍵暗号にとって脅威ではないが、大規模な量子コンピュータの実現に結び付く技術革新が今後生じる可能性があり、その時期は予測できない。また、暗号方式の移行には 10 年以上の長い期間を要するケースもありうる。このため、大規模な量子コンピュータの実現の見通しが立つ前に、量子コンピュータに対して安全な次世代暗号（耐量子計算機暗号）の研究開発や移行に向けた準備が進められている[1]。

米国立標準技術研究所（National Institute of Standards and Technology: NIST）は、次世代暗号の標準化に向けた取組みを進めている（4 節を参照）。2016 年に次世代暗号への移行計画を公表したあと、次世代暗号方式を公募した。1 回目の選考過程（第 1 ラウンド）では、応募された 69 件の候補方式が 26 件に絞り込まれた。2020 年 7 月までに行われた 2 回目の選考過程（第 2 ラウンド）では、候補方式が 15 件（最終候補〈finalists〉7 件、代替候補〈alternate candidates〉8 件）に絞り込まれた。今後、各方式の最終的な技術検証（第 3 ラウンド）が行われる予定である。NIST は、その後、2022～24 年頃に標準案を策定したのち、政府機関の情報システムにおいて暗号を順次移行する方針を表明している。NIST の標準化が完了すれば、多くのベンダーがその製品化に向けた動きを加速させ、米国政府のみならず、さまざまな分野において暗号の移行が急速に進む公算が高い。

わが国政府では、CRYPTREC（Cryptography Research and Evaluation Committees）[2]

1 公開鍵暗号の安全性低下のリスクに対して、量子通信路における量子鍵配送（Quantum Key Distribution: QKD）も対策となりうる。QKD は、量子力学の性質を利用した通信により、通信路での第三者による盗聴を検出できる。また、無限の計算能力をもつ攻撃者でも解読できない情報理論的に安全な暗号技術と組み合わせて利用するため、安全性も高い。もっとも、ネットワーク上の通信機器を入れ替えて通信網を新たに整備する必要があるなど、従来型の（古典）通信路をそのまま利用する次世代暗号とは、今後のインフラとしての普及に向けた課題が大きく異なっており、本稿では割愛する。

2 CRYPTREC は電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）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である（https://www.cryptrec.go.jp）。暗号技術検討会（事務局：総務省・経済産業省。座長：横浜国立大学・松本勉教授）およびその下に設置された暗号技術評価委員会（委員長：東京大学・高木剛教授）と暗

において、量子コンピュータが既存の暗号に与える影響の評価、次世代暗号の今後の取扱いに関する検討を進めている（暗号技術検討会［2020］）。特に、2019 年度には、「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下、量子コンピュータ TF）を設置し、量子コンピュータに関連する動向の調査や対応のあり方について議論が行われている（5 節を参照）。

産業界においては、NIST による標準化を後押しする取組みが活発化している。例えば、インターネット技術の標準化を担う IETF（Internet Engineering Task Force）[3] では、標準化候補の次世代暗号を現行の暗号と併存させながらウェブ上で利用できるように技術仕様の拡張が検討されている。また、Amazon.com, Inc.、Microsoft Corporation、Cisco Systems, Inc. 等の IT ベンダーと欧米の複数の大学が連携し、候補方式を実装した暗号製品のプロトタイプ開発や性能評価を目標とするプロジェクト「Open Quantum Safe」（6 節（2）を参照）が進められている。

こうした米国政府や主要ベンダーの取組み等を踏まえると、大規模な量子コンピュータの実現いかんによらず、2020 年代後半以降、次世代暗号への移行に向けた取組みが加速する可能性が高いといえる。金融分野においても、顧客の端末のブラウザ等において暗号移行が進むとすれば、金融機関や決済事業者は、次世代暗号による暗号化や認証に対応できるようにシステム更改等を迫られることになる。今後、次世代暗号への移行に向けた準備をどう進めていくかについて検討が求められよう。

本稿では、まず、2 節で量子コンピュータ開発の進展を概観し、次世代暗号への移行の必要性について考察する。3 節では、次世代暗号とその安全性証明の方法について解説する。4 節では、NIST による標準化の動向を概説し、5、6 節では、これを受けたわが国および産業界の動向をそれぞれ解説する。

2. 量子コンピュータ開発の進展と次世代暗号への早期移行の必要性

暗号との関連では、「量子ゲート型」[4、5] と呼ばれる量子コンピュータの動向が注目されている（以下では、量子ゲート型コンピュータを単に「量子コンピュータ」

号技術活用委員会（委員長：横浜国立大学・松本勉教授）によって構成されている。

3 IETF は、インターネット上で使用される情報通信技術の仕様策定や標準化を主たる目的とする技術者団体であり、標準化された技術仕様は「RFC（Request for Comments）」と呼ばれて付番されている。

4 量子ゲート型は、既存の古典コンピュータの演算回路を量子回路で実現するもので、さまざまなアルゴリズムを実行できる。計算モデル上は、既存のコンピュータの計算をすべて実行できること等から、「汎用機」と呼ばれることがある。もっとも、未知の量子ビット（量子コンピュータにおける演算単位。詳細は後述）は原理的に複製できないといった独特の制約（複製不可能定理〈no cloning

と呼ぶ。量子コンピュータの基礎理論については、Nielsen and Chuang [2010] を参照)。仮に、理想的な量子コンピュータが実現すれば、現在主流の公開鍵暗号の安全性が低下するとみられる（高木［2019］)。そこで、本節では、まず、量子コンピュータによる高速計算の原理と能力、特に公開鍵暗号の危殆化リスクとの関係を解説する。次に、近年の量子コンピュータの研究開発動向と同分野への積極投資の背景を概観する。それらを踏まえつつ、次世代暗号への早期移行の必要性について考察する。

(1) 量子コンピュータによる高速計算の原理

量子コンピュータによる高速計算は、概していえば、量子ビットを使って並列計算を行い、量子ビットの状態を観測することによって解を得るという流れとなる。その際、重ね合わせ状態（superposition)、量子もつれ（entanglement)、波の干渉（interference）という 3 つの量子力学的性質を利用する。

イ. 量子ビットを用いた並列計算

スーパーコンピュータを含む古典コンピュータでは、情報の基本単位であるビットは 0 または 1 を表す 2 つの状態のうちいずれか一方をとる。n 個の古典ビットは、とりうる 2^n 通りの状態のうちいずれか 1 通りを表現できる。このような確定的な状態を「古典状態」と呼ぶ。

一方、1 つの量子ビットは、0 または 1 を表す状態がそれぞれ観測される確率に関する重みで混ぜ合わされた状態を有する。これが重ね合わせ状態である[6]。重ね合わせ状態によって、量子ビットは複数の古典状態を同時に表現することが可能であり、このような確率的なゆらぎを伴う状態を「量子状態」と呼ぶ。例えば、n 個

theorem〉）等から、ソフトウェアの構成法が古典コンピュータと異なるほか、計算に要する（量子）ビット数等の面で計算効率が必ずしも古典コンピュータを上回るとは限らない。このため、量子コンピュータは単純な古典コンピュータの上位互換機とは言い難く、強みを発揮できる限られた領域でのみ古典コンピュータを代替する部分的な計算の加速装置との見方もある。

5 量子ゲート型のほかに、「量子アニーリング型」と呼ばれる、組合せ最適化問題の解を探索する専用マシンがある。量子力学的現象を計算に利用しているという点で、量子ゲート型と共通しているものの、計算の原理は異なる。量子アニーリング型は実機の開発・利用面で先行しており、D-Wave Systems Inc. が 5,640 量子ビットの商用機を 2020 年に発売している。暗号解読との関係では、D-Wave Systems Inc. のマシンや、量子アニーリング型コンピュータを古典コンピュータによってシミュレートした計算機によって、RSA 暗号を解読するアルゴリズムの研究も報告されている。ただし、暗号の安全性低下のリスクは、本稿執筆時点では、主に「量子ゲート型」によるものと考えられているため、本稿では量子アニーリング型については割愛する。

6 重ね合わせ状態は、「量子ビットが 0 または 1 のいずれかの状態であり、人間がいずれの状態にあるかを知らない」（古典状態の混合）というものではない。0 と 1 の両方の状態の情報を 1 つの量子ビットが同時に保持している。これはさまざまな実験結果から導かれている事実である。

の量子ビットは、2^n 通りの古典状態を（これらの量子もつれ状態〈説明は後述〉も含めて）同時に表現できる。

量子コンピュータでは、量子ビットに対して、古典コンピュータと同様の演算処理を行うことができる[7]。n 個の（重ね合わせ状態の）量子ビットを有する量子コンピュータの場合、1 回の演算処理は、2^n 通りの古典状態すべてを並列処理することに相当する。

ロ．観測における計算結果の効率的な抽出

重ね合わせ状態での並列計算の結果を知る際に、「観測」と呼ばれる行為を行い、重ね合わせ状態を解消する[8]。n 個の量子ビットを有する量子コンピュータのケースでは、1 回の観測で得られる情報は 2^n 通りのうち 1 通りのみであり、この情報量自体は古典コンピュータと変わらない。また、どの古典状態が観測で得られるかは確率的に決まる（観測者が自由に選ぶことができない）。仮に、2^n 通りのうち正解が 1 通りだけであって、すべての古典状態が等しい確率で観測されるならば、1 回の演算処理と観測によって正解が得られる確率が $1/2^n$ となることから、量子コンピュータは高速化に寄与しないことになる。このように、重ね合わせ状態のみを利用した並列計算は、直ちに量子コンピュータによる計算の高速化につながるというわけではない。

高速計算は、問題の解に相当する情報を量子ビットから効率的に抽出することによって実現される。このような効率的な抽出は、任意の（入力された）量子状態に対して所望の情報に対応する状態が観測される確率を巧みに増幅あるいは減衰させるアルゴリズムを実行することによって行われる。この確率の操作は、並列計算の際に、各量子ビット間に「量子もつれ」[9] と呼ばれる相関関係をもたせると同時に、量子状態が有する波の性質を巧みに利用して複数の量子状態の間で干渉を生じさせることによって行われる。

---

7 量子コンピュータの通常の演算は、ユニタリ変換と呼ばれる可逆変換で表される。これらを組み合わせると、古典コンピュータと同様の操作も原理的には実現できる。

8 これは、計算基底と呼ばれる軸によって観測を行った場合である。観測の方法によっては重ね合わせ状態が観測後に解消されない場合もあるが、ここでは計算基底によって観測を行った場合を念頭に記述する。

9 量子もつれは、量子ビットの観測値が互いに独立でない状態を表す。最も簡単な量子もつれの関係は、2 つの量子ビットのうち、一方を観測した結果が 0 であれば他方も必ず 0 となり、一方の観測した結果が 1 であれば他方も必ず 1 になるような完全な相関をもつものである（ベル状態〈Bell state〉と呼ばれる）。量子もつれの程度は、「エンタングルメント・エントロピー（entanglement entropy）」と呼ばれる量で表され、ベル状態のように完全な相関をもつ場合に最大となる。また、n 個の量子ビットが量子もつれの関係にある場合には、一部の量子ビットに対する演算や観測は、他のすべての量子ビットにも影響を及ぼし、量子ビットたちの一部を全体から切り離して独立に扱うことができない。

(2) 量子コンピュータの能力と暗号の危殆化リスク

量子コンピュータが、一般論として、どのような問題に対してどの程度の高速化（計算量の削減）を可能にするかについては、理論的に明らかではない[10]。量子コンピュータの計算法の特性からは、重ね合わせ状態を活かして、多数の場合分けに対応した並列計算を有効に利用できるタイプの問題に対して高速化が期待できる。もっとも、古典コンピュータ上で動作するアルゴリズムは、単純に並列化できるわけでないため、量子コンピュータによる高速化の余地は自明ではない。現状では、高速に求解できる問題やそれに対するアルゴリズムの個別的な探索が行われている[11]。一部の問題に対しては、量子コンピュータは、古典コンピュータを利用した最速のアルゴリズムを効率面で上回ることが知られている。例えば、n 個のデータの中からある条件を満たすデータを探索する問題の計算量は、グローバーのアルゴリズム（Grover [1996]）によって計算量を 1/2 乗に削減（2 乗の高速化）できる。また、離散的な値をとる関数の周期を求める問題に対しては、サイモンのアルゴリズム（Simon [1994]）によって計算量を指数関数的に削減できる[12]。

指数関数的な高速化が可能な問題の中に、公開鍵暗号の安全性の根拠である素因数分解問題や楕円曲線上の離散対数問題が（偶然にも）含まれている[13]。1994 年に提案されたショアのアルゴリズムは、素因数分解問題や離散対数問題を解くための計算量を指数関数的に削減できることを示した（Shor [1994, 1997]）[14]。このアルゴリズムが理想的な量子コンピュータ上で理論通りに動作することとなれば、現在普

10 量子コンピュータによって 3 分の 2 以上の確率で高速に（多項式時間で）解ける判定問題の集合（bounded-error quantum polynomial time: BQP）は、古典コンピュータによって高速に解ける判定問題の集合を含むが、古典コンピュータによる高速な求解が困難であると予想される判定問題（NP〈nondeterministic polynomial time〉完全）を含むか否かはわかっていない。ここで、判定問題とは、Yes か No かを答える形式の問題を指し、計算量に関する理論でよく利用される。後述する素因数分解問題（から自然に導かれる判定問題）は、量子コンピュータにより多項式時間で解けるため、BQP に含まれるが、NP 完全であるか否かはわかっていない。

11 Quantum Algorithm Zoo（https://quantumalgorithmzoo.org）では、現在知られている古典コンピュータを利用したアルゴリズムよりも高速に動作する量子コンピュータのアルゴリズムが収集されており、本稿執筆時点で約 70 個掲載されている。

12 より実用的な問題に対しては、上記のような典型的な問題を解く際に利用されるアルゴリズムのうち汎用性の高い部分をサブルーチンとして利用する。代表例を挙げると、量子化学計算では位相推定（phase estimation）、量子機械学習では振幅増幅（amplitude amplification）、HHL（Harrow–Hassidim–Lloyd）アルゴリズム等が頻繁に利用される。これらを利用して、指数関数的な高速化が可能な問題もあるが、そうした問題は限られている。

13 共通鍵暗号への量子コンピュータによる影響は、公開鍵暗号に比べて限られているとみられるが、注意を払うべき点もある。詳しくは、補論 1 を参照されたい。

14 ショアのアルゴリズムは、因数分解の対象の自然数（2 進数表示の桁数 k）に対して、多項式時間 $O(k^3)$ の計算量で高速に解ける。これに対して、古典コンピュータ上で動作する数体ふるい法を用いた最速のアルゴリズムでは、準指数時間の計算量が必要であるため、指数関数的な高速化が得られている。

及している主な暗号方式（RSA 暗号、ECDSA、ECDH 等）の安全性が損なわれると懸念されている[15]。これが公開鍵暗号の危殆化リスクである。

(3) 理想的な量子コンピュータの実現見通しと課題

本稿執筆時点では、現代暗号の解読に利用できるほどの理想的な量子コンピュータについて、実現の目途は立っていない。理想的な量子コンピュータとは、計算途中で量子ビットに生じるノイズ[16]の影響を除去する「誤り訂正（error correction）」機能[17]を備え、かつ多数の量子ビットを備えた大規模なマシンを指す[18]。これに対して、本稿執筆時点で実用化されているマシンは、誤り訂正ができないため、暗号解読等、量子ビットに対して繰り返し演算を行う必要がある場合には、ノイズの影響から信頼できる計算結果が得られない。また、100 量子ビットを下回る中小規模なものにとどまり、一度に処理できるデータ量が小さい。さらに、量子ビットやこれらの量子もつれを維持できる時間も、方式によってばらつきがあるが、例えば超伝導回路方式では、本稿執筆時点で 100 マイクロ秒程度であるため、数時間を要する暗号解読の計算には耐えられない。

15 これまでに、任意の自然数に対して有効な汎用性のある量子回路のかたちで、ショアのアルゴリズムを実装して暗号解読を行ったとの報告はなされていない。先行研究では、解となる素因数の性質を先験的に利用した量子回路を利用しており、任意の自然数に対して有効な手法とはいえない（暗号技術調査ワーキング・グループ［2019］）。

16 ノイズの発生源は装置によって異なる。現在主流の超伝導量子ビットの場合には、精度に限りのある量子ゲート演算、装置の熱輻射のほかに、影響度は必ずしも大きくないが宇宙から降り注ぐ放射線（Vepsäläinen *et al.* [2020]）等の環境要因もある。

17 古典コンピュータでの誤り訂正は、複数のビットによって冗長性をもたせることで実現される。例えば、「0」を表すビットを「000」と 3 つのビットで表した場合、中央のビットが反転して「010」となったとしても、残り 2 つのビットを観測すれば「000」と訂正できる。このとき、誤りが生じたビットの値を直接的に読み出せることや、誤りが生じていないビットの値を複製できることが暗黙の前提となっている。

一方、量子コンピュータでは上記の前提が成り立たないため、古典コンピュータの誤り訂正を単純に量子コンピュータに適用することはできない。まず、量子ビットは観測で破壊されるため、量子ビットの誤りの有無を直接的な観測で確かめられない。また、誤りのない量子ビットを、訂正を行うために複製することができない（複製不可能定理）。もっとも、こうした制約のもとでも、量子誤り訂正が理論的には可能であることが示されている（脚注 23 を参照）。

18 現代暗号の解読に利用できる量子コンピュータのスペックは、一定の想定のもとで、誤り耐性があり（fault-tolerant）、かつ数百万量子ビットを備えたもので、数時間から数十時間程度の一連の計算を実行できるものと推定される（National Academies of Sciences, Engineering, and Medicine [2019]）。こうした量子ビット数の試算では、ノイズの影響を全く受けない理想的な量子ビット（論理量子ビット）を 1 つ実現するために、数千個のノイズの影響を受ける量子ビット（物理量子ビット）を使う必要があるといった、量子誤り訂正に関する前提の影響が大きい点に留意する必要がある。例えば、2,048 ビットの鍵長の RSA 暗号の解読には 4,098 個の論理量子ビットを要するとされるが、必要な物理量子ビットは 800 万個となる。計算時間の試算についても、量子ゲート演算の動作速度の前提（上記試算では 5 MHz）に大きく依存する。

CRYPTREC の量子コンピュータ TF における議論では、量子コンピュータによる暗号解読に関して、「現状の（量子コンピュータの計算過程で生じる大きな）ノイズは暗号解読のための素因数分解に活用できる水準ではない」、「暗号解読ができるような（理想的な）量子コンピュータの実現時期は見えていない」といった見方が示されている（暗号技術検討会［2019］）。

理想的な量子コンピュータの開発に向けた主な課題は、大規模な量子もつれを実現し、これを維持できる時間を延長することである。これが達成されたもとで量子誤り訂正を実装すれば、一度に処理できるデータの量と演算可能回数を同時に増やすこと[19]ができる。この実現困難度は極めて高く、一部には、理想的な量子コンピュータが永遠に「理論上のもの」にとどまるのではないかとの見方もある[20]。

こうした状況を踏まえると、理想的な量子コンピュータが今後登場すると仮定したとしても、それは、現在の主流の技術の延長線上にあるマシンではなく、技術革新によって著しく頑健性を高めた新しい技術に基づくマシンである可能性が高いと考えられる。

(4) 量子コンピュータへの積極投資とその背景

本節（3）で述べた技術革新について予測することはできないが、近年、量子コンピュータへの研究開発投資が積極的に行われており、予想外のイノベーションが起きる可能性は無視できない。現在主流の超伝導回路方式のほかにも、量子コンピュータの物理的な実現方法は多数提案されており、基礎研究は活発に行われている[21]。産業応用のアプリケーションを含むソフトウェアの研究も同時進行して

19 現在、実機の開発・利用が先行している超伝導回路方式は、個々の量子ビットを制御するために敷設する配線の複雑さ等のハードウェア制約から 1,000 量子ビット以上への規模拡大が難しいとみられている（National Academies of Sciences, Engineering, and Medicine [2019]）。また、こうした見方を払拭し、量子コンピュータの大規模化・高性能化を達成する道筋（スケーリング則）も示されていない（田渕［2020］）。

20 廣田［2020］は、誤り耐性のある量子コンピュータの実現可能性の基礎となる理論（閾値定理〈threshold theorem〉。脚注 23 を参照）が、量子ビットに生じるノイズに関する楽観的な前提に基づくとの見解について考察している。特に、ノイズの発生確率が量子ビット数に依存して上昇する非線型タイプのノイズに対して、現在の量子誤り訂正は有効ではなく、閾値定理が成立しないと指摘している。これは、ノイズの性質によっては大規模量子コンピュータが現在の理論では実現不可能であることを示唆するため、ノイズの性質の正確な理解が重要であると論じた。

21 例えば、光方式（XANADU、PsiQuantum, Corp.）、イオントラップ方式（IonQ, Inc.）、ダイヤモンド NV センター方式、半導体量子ドット方式（Intel Corporation）、固体核磁気共鳴（NMR）方式（大阪大学北川研究室）、トポロジカル量子計算に基づく方式（Microsoft Corporation）等がある。超伝導回路方式は、Alibaba、D-Wave Systems Inc.、Google LLC、IBM、Intel Corporation、Rigetti & Co, Inc. 等、多くの企業が研究開発を手掛けている。企業のほか大学でも研究が進められている。これらの方式は長所短所がそれぞれで異なるため、次世代標準としての有望さを比較することが難しい。

おり、エコシステムが形成されている（National Academies of Sciences, Engineering, and Medicine [2019]）[22]。

こうした積極投資の背景にはいくつかの要因が存在する。第 1 に、理論面において、かつて実現困難と考えられていた量子ビットの誤り訂正の手法が考案され、理想的な量子コンピュータの実現が原理的には可能であるとの見方が拡がった[23]。第 2 に、実証面では、「量子超越性（quantum supremacy）」が 2019 年に実験的に確かめられ、量子力学的性質を利用した計算の高速化が理論通りに働くことが現象面でも確認された（Arute *et al.* [2019]）[24]。量子超越性とは、スーパーコンピュータを含む古典コンピュータでは達成できない高速化を量子コンピュータが実現することを指す。第 3 に、産業応用面では、一部に実機が提供されている誤り訂正できない中小規模のマシン（noisy intermediate-scale quantum technology: NISQ）について、古典コンピュータと組み合わせて利用するハイブリッド・アルゴリズムにより、化学や金融、機械学習等で有望な応用があると見込まれるため、短中期的な目線での投資でも果実を得られる可能性がある。第 4 に、アクセス面では、NISQ をクラウド経由で操作するインタフェースが提供されたことにより、量子コンピュータ利用の参入障壁が劇的に下がった。第 5 に、量子コンピュータがもたらす消費エネルギーの節減効果[25] の重要度が高まった。大規模な機械学習モデルの訓練に投入する莫大

22 JST 研究開発戦略センターの量子イノベーション戦略第 1 回有識者会議資料「量子技術分野の研究動向について」（https://www.kantei.go.jp/jp/singi/ryoshigijutsu_innovation/dai1/siryou3.pdf）を参照されたい。

23 量子ビットの情報を直接的に読み出すことなく、ビット誤りの有無を間接的に検知することによって誤り訂正を行うショアの符号（Shor [1995]）やスタビライザー符号（stabilizer code、Gottesman [1997]）等が考案されている。さらに、ノイズに関して一定の前提を置くもとで、量子ビットに 1 回の演算で生じる誤りを一定の確率以下まで低減させることができれば、前述の誤り訂正により、任意の精度にまで誤りを抑制することが可能となり、誤り耐性のある量子コンピュータを実現できることが知られている（閾値定理）。ただし、閾値定理では、量子ビットに生じるノイズに関して一定の仮定が置かれているため、今後実証的にノイズの性質を確かめることが重要である（脚注 20 も参照のこと）。なお、脚注 21 で言及したトポロジカル量子計算では、代数的な結び目理論を用いて誤り耐性が高い方式の実現を目指す研究も行われている（https://cloudblogs.microsoft.com/quantum/2018/09/06/developing-a-topological-qubit/）。

24 2020 年 12 月には、中国の研究チームにより、76 個の光子（76 量子ビット）を利用して光方式でも初めて量子超越性が示された（Zhong *et al.* [2020]）。採用された方式自体は、ボソン・サンプリングという量子超越性を示すために選ばれた計算困難な問題以外への適用は難しいとみられる。もっとも、光子で大規模な量子もつれを作成し、光方式による大規模計算の可能性を実証したことや、現在主流の方式以外にも有望な方式を模索することの有用性を示した意義は大きい。

25 量子コンピュータの演算はすべて可逆であるため、（最後に行う量子ビットの観測を除いて）演算そのものに要するエネルギー消費量の理論的な下限はゼロである。熱力学と計算の関係に関する理論によると、コンピュータが情報を消去する際に必ず熱が発生してエネルギーを消費する（ランダウアーの原理〈Landauer's principle〉）。量子コンピュータの演算は、ユニタリ変換と呼ばれる可逆操作のみで構成されるため、出力から入力を逆算できる。計算過程で情報は失われないため、装置の駆動に要するエネルギーを除けば、演算は必ずしもエネルギーを消費しない。これに対して、古典コンピュータは不可逆演算がほとんどであるため、原理的に計算過程でエネルギーを必ず消費する。

なエネルギー消費の増加は持続可能でなく、エネルギー制約が機械学習の将来的な発展を抑制する懸念がある（Thompson *et al.* [2020]）。量子コンピュータはそのエネルギー制約を緩和できる可能性がある。

以上から、当面は、現代暗号にとって脅威とはならない NISQ の開発が目指されるとみられるが、積極的な研究開発と短中期的な投資の果実との好循環が投資資金を惹きつけ続ければ、理想的な量子コンピュータを実現するイノベーションが将来起きる可能性は無視できない。

(5) 次世代暗号への早期移行の必要性

現状では、量子コンピュータは現行の暗号技術にとって脅威ではなく、近い将来にもそうした脅威が差し迫ったものとなる懸念も乏しい。もっとも、以下の 4 つの理由から次世代暗号への移行準備を早期に進めることが望ましい。

第 1 に、暗号方式の移行には 10 年以上の期間を要するケースもあるとみられるため、大規模な量子コンピュータの実現の目途が立ってからの移行対応では遅い。金融や決済の分野を含む情報インフラの根幹に浸透した暗号方式の移行は、とりわけ、大規模なシステム更改やハードウェア機器の入替えが伴うケースや、関係者が多岐にわたるケースにおいては、長期的かつ大規模なプロジェクトとして計画的に取り組む必要がある（伊藤・宇根・清藤［2019］）。さらに、国防やそれに類する情報インフラの場合には、暗号方式の移行に 20〜30 年を要する場合があるとの見方もある（National Security Agency [2016]）。

第 2 に、オープンなネットワーク上で通信された暗号化データを収集・保管しておき、その暗号の安全性が低下したタイミングで暗号化データを解読するという「ハーベスト攻撃」が想定される。ハーベスト攻撃の脅威に備えるためには、データを秘匿しておくべき期間の分だけ移行を前倒しする必要がある。例えば、10 年間よりも長くデータを秘匿したい場合、理想的な量子コンピュータの出現の 10 年以上前から次世代暗号に移行しておく必要がある。もっとも、理想的な量子コンピュータの出現時期を予見することは不確実性が高いため、できるだけ早期の移行が望ましい。

第 3 に、本節（4）で述べたとおり、情報技術の発展のスピードは速いため、予想外のイノベーションが生じる可能性を無視できない。2014 年には 5 量子ビットのマシンしか実現していなかったが、2019 年 9 月には 53 量子ビットのマシンを利用して量子超越性も実験で確かめられた。現在の実機の規模は、約 70 量子ビットまで拡大している[26]。近年の量子分野での積極的な研究開発投資にも支えられて、直

26 本稿執筆時点では、IBM が 65 量子ビットのマシンを開発しているほか（https://www.ibm.com/blogs/

近 5 年間の技術進歩の速度は著しいものとなっている。

第 4 に、次世代暗号が社会基盤としての信頼を得るためには、暗号技術の実装を洗練したうえで広く利用し、安全性を確かめながら実績を積み重ねるプロセスを経ることが望ましい。3 節で述べるように、暗号方式の安全性について理論的に完全な証明を与えることは難しい。また、暗号化・復号処理を行うハードウェア機器の挙動から秘匿された情報を得ようとするサイドチャネル攻撃への耐性や、利用できる計算資源の乏しい IoT（Internet-of-Things）機器に搭載した場合の性能等について、暗号学的な検証だけでは十分確認できるとは言い難い。このため、新しいサービスや情報システムに次世代暗号を先行的に組み込み、本格的に普及させるに当たっての課題の洗出しと対処を繰り返すなかで、徐々に社会インフラとしての信頼を得ながら利用範囲を拡大していくというアプローチが有益であると考える。

3. 次世代暗号の特徴と安全性評価の動向

次世代暗号には多様な方式が提案されており、並行して安全性や処理性能の検証が進められている。次世代暗号の多くは研究の歴史が浅く、安全性評価が十分に安定しているとはいえないものもあるほか、技術検証の進捗度合いもばらつきがある。本節では、暗号方式の安全性評価の方法論を説明したうえで、安全性の根拠となる数学的問題に応じて次世代暗号を紹介する[27]。

(1) 計算量的安全性に基づく暗号方式の評価

次世代暗号や現在主流の（公開鍵）暗号方式の安全性は、「計算量的安全性」という概念に基づいて評価される[28]。計算量的に安全であるとは、（無限ではなく）有限の計算能力を有する攻撃者を想定したとき、現実的な範囲の時間では暗号が解読されることがないという特性を意味する。

計算量的安全性は、保証される安全性のレベルに応じて、OW-CPA（選択平文攻

research/2020/09/ibm-quantum-roadmap/）、Google LLC は 72 量子ビットのマシンを開発している（https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html）。

27 次世代暗号のより詳しい解説としては、四方［2019］、縫田［2020］、暗号技術調査ワーキング・グループ［2019］を参照されたい。

28 暗号方式には、計算量的安全性に基づくものと、情報理論的安全性に基づくものに大別される。情報理論的安全性に基づく暗号方式は、完全な秘匿が可能である一方、データと同じ長さの暗号鍵（乱数）を事前に配送する必要があり実用性に乏しい。計算量的安全性は、より実用に適した安全性基準である。

撃〈chosen plaintext attack〉に対する一方向性〈one-wayness〉）、IND-CPA（選択平文攻撃に対する識別不可能性〈indistinguishability〉）、IND-CCA（選択暗号文攻撃〈chosen ciphertext attack〉に対する識別不可能性）等に分類され、後者ほど強い安全性要件といえる。OW-CPA とは、攻撃者が「自由に選択した平文（解読したい平文を除く）に対する暗号文を入手できる」という状況において、解読対象の平文を完全には解読できないことを意味する。この要件は、部分的な暗号解読は許容するため、相対的に弱い安全性要件である。一方、IND-CPA とは、OW-CPA と同じ状況において、解読対象の平文を部分的にも解読できないことを意味する。また、IND-CCA は、攻撃者が「自由に選択した暗号文（解読したい暗号文を除く）に対する平文を入手できる」という状況において、解読対象の暗号文は部分的にも解読できないことを意味する。これは、公開鍵暗号で保証できる最高レベルの安全性要件である[29]。なお、IND-CPA を満たす方式を、IND-CCA を満たす方式に変換する「藤崎・岡本変換」[30]（Fujisaki and Okamoto [1999]）と呼ばれる手法が知られている。広く実用されている公開鍵暗号の多くは、IND-CCA を満たしている。

計算量的安全性に基づく暗号方式では、解を得るために莫大な計算量が必要であると信じられている計算問題を利用する。実際の利用を想定した安全性評価では、計算困難性に高い信頼が得られている典型的な問題を利用することが多い。現代暗号では、素因数分解問題と楕円曲線上の離散対数問題、次世代暗号では、最短ベクトル問題や符号訂正問題、多変数多項式問題が該当する。個々の暗号方式の安全性（IND-CCA 等）は、こうした典型的な問題が計算困難であるとの仮定のもとで数学的に証明される。

安全性評価では、これらの典型的な計算問題がどの程度難しいかを判定する問題が残される。現時点では、理論的な証明が不可能なため、実験的な評価が行われている。例えば、暗号解読コンテスト[31]を開催し、「研究者らを精一杯頑張らせる」ことによって、より厳しい目線での評価が実施されている。こうした取組みの中でも

29 IND-CCA のうち、攻撃者に適応的選択暗号文攻撃（adaptive chosen ciphertext attack）を許容するものを「IND-CCA2」と呼び、これを許容しない「IND-CCA1」と区別する場合がある。一般に、IND-CCA は、①攻撃者が平文 $\{m_0, m_1\}$ を選ぶ、②挑戦者が対応する暗号文 $\{c_0, c_1\}$ を作成し、いずれか一方 $c_* \in \{c_0, c_1\}$ を攻撃者に返す、③攻撃者が $c_* = c_0$ か $c_* = c_1$ を区別するという対話ゲームにおいて③が不可能であることと定義される。攻撃者が、③において、$\{c_0, c_1\}$ 以外の暗号文に加えて、$\{c_0, c_1\}$ のうち正解以外の暗号文（例えば、$c_* = c_0$ の場合は c_1）を復号することができる場合の攻撃を適応的選択暗号文攻撃という。

30 藤崎・岡本変換は、（IND-CCA を満たさない）弱い公開鍵暗号から、ハッシュ関数や共通鍵暗号と組み合わせることにより、（IND-CCA を満たす）強い公開鍵暗号を構成する手法である。

31 暗号の安全性の根拠となる計算問題を解くコンテスト。素因数分解問題を対象とした「RSA Factoring Challenge」（RSA Security LLC が主催。1991～2007 年）が有名であるほか、後述する次世代暗号の 1 つである格子暗号に関する「格子チャレンジ（Lattice Challenge）」（独ダルムシュタット工科大学が主催。2008 年開始。https://www.latticechallenge.org/）、多変数多項式暗号に関する「福岡 MQ チャレンジ（Fukuoka Multivariate Quadratic Challenge）」（九州大学等が主催。2015 年開始。https://www.mqchallenge.org/）が実施されている。

解けない問題は、現実的な時間では解けない数学的問題であると信じられることになる。また、実験的な評価は、実際の利用で安全なセキュリティ・パラメータ（暗号の鍵のサイズ等）を割り出す意味でも重要である。

(2) 次世代暗号の種類

次世代暗号は、安全性の根拠になる数学的な問題に応じて、①格子暗号、②符号暗号、③多変数多項式暗号、④同種写像暗号[32] 等に分類される。後述する NIST による標準化の最終候補は、①～③のいずれかに含まれているため、これらの概要を説明する。

イ. 格子暗号

格子暗号とは、高次元空間の中で規則的に並んだ点集合（格子）の性質を利用した公開鍵暗号の総称である。ほとんどの格子暗号は、与えられた格子の中から、最も原点に近い点を探す問題（最短ベクトル問題〈shortest vector problem: SVP〉）の困難性を利用した暗号方式である。格子の空間の次元が非常に大きい場合には、求解が困難であることが知られている。SVP に関しては、さまざまな解法[33] が提案されているが、本稿執筆時点では、著しく効率的な解法（多項式時間の解法）は見つかっていない。もっとも、SVP の求解コンテストである「格子チャレンジ」（脚注 31 を参照）において、より難度の高い問題の解が発見される事例が続いている。SVP がどの程度困難な問題といえるかについては評価が定まっていない。

SVP のほかに、次世代暗号では、格子を用いたさまざまな数学的問題の困難性が利用されている。代表的なものとしては、離散的な値をとる変数に関する連立線型方程式にノイズを加えて求解困難にした LWE（learning with errors）問題（Regev [2004]）[34] や NTRU（エヌトゥルー）問題（Hoffstein, Pipher, and Silverman [1998]）、およびこれらの変種が利用される。これらの問題の計算困難性は、すべて格子問題

32 同種写像暗号は、2 つの超特異楕円曲線の間に定義される同種写像を探索する問題の困難性を安全性の根拠とする。ディフィー=ヘルマン鍵共有方式を一般化した SIDH（supersingular isogeny Diffie–Hellman）鍵共有方式（Jao and De Feo [2011]）が提案されており、4 節で述べる NIST による標準化の代替候補に挙げられている SIKE は SIDH 鍵共有方式の一種である。

33 SVP を効率的に解くアルゴリズムとして、格子を生成するベクトルの集合（基底）を、より短いベクトルからなる基底へと繰り返し変換していく手法（基底簡約）が知られている。このほか、最短ベクトルの候補を効率的に全探索する列挙法（enumeration）や、解が確実に見つかる保証はないが、格子点のリストからより短い格子点を生成してリストを更新していくふるい法（sieving）が提案されている。

34 LWE 問題は、整数剰余類環 Z/nZ 上で定義された秘密ベクトル $\boldsymbol{s}$ に対して $b_i = \langle \boldsymbol{s}, \boldsymbol{a}_i \rangle + e_i$ の連立方程式から秘密ベクトルを復元する問題である。ここで、$\langle \cdot, \cdot \rangle$ は、ベクトルの内積である。エラー e_i が存在しない場合には、この問題はガウスの消去法（掃出し法）で簡単に解けるが、エラーが存在する場合には計算困難であることが知られている。LWE 問題は、暗号では次のように利用される。平文

の計算困難性を根拠としている。LWE 問題を多項式版に拡張・一般化したものに、Ring-LWE 問題、Module-LWE 問題、Module-LWR（learning with rounding）問題等がある[35]。

ロ．符号暗号

符号暗号は、誤り訂正符号（error-correcting code）を利用した暗号方式である。誤り訂正符号は、ノイズのある通信路で通信を行う際に、送信するメッセージに冗長性をもたせることで、受信者によるノイズの除去を可能とする通信技術である。符号暗号は、マクリースが公開鍵暗号への応用を提案（McEliece [1978]）して以来、約 40 年間の研究の歴史がある。McEliece 暗号は、OW-CPA を満たすと予想されているが、IND-CPA を満たしていない。もっとも、さまざまな変換法を適切に組み合わせることによって、IND-CPA 等のより強い安全性を実現できると期待されている。その他の符号暗号としては、Niederreiter 暗号（Niederreiter [1986]）やこれをベースにした Classic McEliece 暗号が提案されている。

ハ．多変数多項式暗号

多変数多項式暗号は、変数が離散的な値をとるもとで多変数連立 2 次方程式を解く問題（MQ〈multivariate quadratic〉問題）を利用した暗号方式である[36]。MQ 問題は、多変数多項式を互いに割り算することで簡素化する方法（グレブナー基底の計算）で解けるが、その計算は簡単ではない[37]。グレブナー基底を高速に求める手法の研究は概ね成熟しているが、暗号以外の基礎科学分野での関心も高いため、思わぬ技術革新により効率的な手法が提案される可能性もある。MQ 問題の解を求めるコンテストである「福岡 MQ チャレンジ」（脚注 31 を参照）では、これまでに解かれたものよりも高難度の問題の解が発見される事例が続いている。

---

m に対して、集合 $\{1, 2, \ldots, m\}$ の中からランダムに選んだ部分集合を S とする。暗号化では、平文のビットが 0 の暗号文を $(\sum_{i\in S} \boldsymbol{a}_i, \sum_{i\in S} b_i)$ とし、1 の暗号文を $(\sum_{i\in S} \boldsymbol{a}_i, \lfloor q/2 \rfloor + \sum_{i\in S} b_i)$ とする。復号は、暗号文 $(\boldsymbol{a}, \boldsymbol{b})$ に対して $\boldsymbol{b} - \langle \boldsymbol{s}, \boldsymbol{a} \rangle$ を計算し、$\lfloor q/2 \rfloor$ より 0 に近い場合は 0 とし、それ以外の場合は 1 を出力する。

35 これらの計算困難性の関係については、Peikert and Pepin [2019]、四方［2019］を参照。

36 ランダムに選ばれた多変数多項式の連立方程式 $F(x) = a$ を解く問題は、NP 困難である。暗号では、解きやすい連立方程式 $F(x) = a$ を秘密鍵としておき、これにランダムな変換（アフィン変換：S、T）を施した連立方程式 $T \circ F \circ S(x) = P(x) = b$ を公開鍵とする。公開された方程式系は、計算が困難になることが期待される。これを利用して、平文 m に対して、暗号文 $c \leftarrow P(m)$ で暗号化し、$m \leftarrow S^{-1} \circ F^{-1} \circ T^{-1}(c)$ で復号できる。

37 F_5 アルゴリズム（Faugère [2002]）等が考案されている。計算量は、入力である多変数多項式の集合から定まる「正則性の次数（degree of regularity）」と呼ばれる不変量で評価される（Bardet, Faugère, and Salvy [2004]）。

4. 米国政府による耐量子計算機暗号の標準化動向

NISTは2020年7月に次世代暗号の第2ラウンドの検証結果を公表した。第2ラウンドでは、26件の次世代暗号の候補のうち、15件（最終候補7件、代替候補8件）が審査を通過した。本節では、これまでの経緯を振り返るとともに、第2ラウンドの検証結果を解説する。

(1) これまでの経緯

米国政府は、政府機関の情報システムにおいて、RSA暗号やECDSAを主要な暗号方式として調達・使用してきたが、近年の量子コンピュータの研究開発の活発化とそれに伴う暗号解読のリスクの高まりを展望し、長期的な観点で、量子コンピュータに対して安全な次世代暗号を新たに調達標準とする方針を2016年に発表した（National Institute of Standards and Technology [2016a]）。同時に、稼働中の情報システムにおいて使用している暗号（RSA暗号等）についても、新たな調達標準を決定した後、次世代暗号に順次移行していく計画を明らかにした。

NISTや国家安全保障局（National Security Agency）は、政府機関で使用している大規模な情報システムにおいて、新しい暗号の実装（機器の入替え等）を完了するために20〜30年程度の時間が必要となるケースもあるとしている。そのうえで、NISTは、予想を上回るスピードで量子コンピュータの開発が進展した場合のリスクを考慮し、早めに暗号を移行したいとしている。

NISTは、標準化の候補となる暗号方式の応募要件や評価基準等を公表し、2017年11月末までに候補方式を募集した（National Institute of Standards and Technology [2016b]）。候補となる暗号方式には、公開鍵暗号および鍵共有[38]、または、デジタル署名のいずれかを提供することが求められた。その後、応募要件を満たした69件を受理した後、2019年1月までの第1ラウンドで26件に絞り込んだ（National Institute of Standards and Technology [2019]）。それに続く2020年7月までの第2ラウンドでは、候補方式を15件に絞り込んだ（図表1を参照。National Institute of

38 募集要項では、鍵共有を鍵カプセル化メカニズム（key encapsulation mechanism: KEM）と呼んでいる。KEMは、送信者から受信者に対する1回の通信により、送受信者間で一定以上の長さの乱数（共通鍵）を共有する仕組みである。KEMによって鍵共有が可能になれば、共通鍵暗号による高速な暗号通信を行うことができる。公開鍵暗号方式とKEMの違いは、暗号化の対象がそれぞれ任意のデータであるか、共通鍵のみであるかである。両者の暗号技術は相互利用ができるため、本質的な違いはない。詳しくは四方［2019］を参照されたい。

図表 1　耐量子計算機暗号の標準化の候補方式

（最終候補：7 件）

	方式名	依拠する数学問題	代表提案者の所属組織
公開鍵暗号（鍵共有）	CRYSTALS-KYBER	格子問題	Radboud University
	NTRU		University of Waterloo
	SABER		KU Leuven ほか
	Classic McEliece	符号問題	Eindhoven University of Technology ほか
デジタル署名	CRYSTALS-DILITHIUM	格子問題	IBM Research
	FALCON		Thales Communications & Security ほか
	Rainbow	多変数多項式問題	University of Cincinnati

（代替候補：8 件）

	方式名	依拠する数学問題	代表提案者の所属組織
公開鍵暗号（鍵共有）	FrodoKEM	格子問題	Microsoft Research
	NTRU Prime		Eindhoven University of Technology ほか
	BIKE	符号問題	Intel Corporation ほか
	HQC		University of Limoges ほか
	SIKE	同種写像探索問題	University of Waterloo
デジタル署名	GeMSS	多変数多項式問題	Sorbonne University ほか
	Picnic	共通鍵暗号の解読問題	Microsoft Research
	SPHINCS+	ハッシュ関数の衝突検索問題	Eindhoven University of Technology

Standards and Technology [2020]）[39]。

NIST は、2020 年から 2021 年にかけて候補方式のさらなる評価・選考を進め（第 3 ラウンド）、2022～24 年頃に標準案を策定する見通しを示している。しかし、「安全性を適切に評価するためにはもっと時間が必要である」との意見をもつ暗号研究者は少なくない[40]。この点、第 2 ラウンドの報告書では、次世代暗号は 1 つの方式に依拠するリスクを避けるために多様性をもつことが望ましいとしている。そのうえで、それぞれの方式の標準化を、広範な用途に供する準備が整い次第、優先順位をつけて順次行っていくことを示唆している。そして、第 3 ラウンドでは、まず最終候補 7 件から最終的な標準方式を選び、代替候補 8 件はその後に評価を行う可能

39 第 1 ラウンドでは、主に安全性の観点からの評価・選考が実施されたほか、第 2 ラウンドでは、主に処理性能（暗号化や復号にかかる処理時間等）に関して評価・選考が行われた。第 3 ラウンドでは、標準化に向けた最終段階として、実装を想定した安全性・性能の評価に重点が置かれる。NIST が示している評価基準（補論 2 を参照）には、安全性に関する詳細な基準が明記されておらず、各方式の提案者が独自に安全性の根拠を示すこととなっている。

40 NIST が 2019 年 8 月に開催した「Second PQC Standardization Conference」では、第 1 ラウンドを通過した 26 件の候補方式の評価・選考をどう進めるべきかが議論された。その際、複数の暗号研究者から、「26 件の候補方式を網羅的に評価するには多大な時間が必要となる」、「横並びでの安全性評価を適切に実施するためには、NIST は評価の基準をより精緻化することが求められる」といった意見が寄せられていた。

性が高いとされている。今後、NIST が、暗号方式の評価の信頼性と多様性とのバランスをとりながら、候補方式の絞込みを具体的にどのように進めるかに注目が集まっている。

(2) 第 2 ラウンドでの各方式の評価の概要

現在、最終候補となっている 7 方式のうち、格子暗号が 5 件と過半を占めている。内訳は、公開鍵暗号または鍵共有方式が 3 件（CRYSTALS-KYBER〈クリスタルス・ケイバー〉、NTRU、SABER〈セイバー〉）、デジタル署名が 2 件（CRYSTALS-DILITHIUM〈クリスタルス・ダイリチウム〉、FALCON〈ファルコン〉）である。格子暗号は、暗号化や復号の処理性能が高く、鍵のサイズも小さいことに加え、理論的な安全性証明を付与しやすいことから、次世代暗号の最有力候補とみられている。さらに、データを暗号化したまま四則演算が可能となる完全準同型暗号を構成できるという特長があり、機能面での拡張性も高い。今後、類似の数学的問題に依拠する候補方式については、1 つに集約されることが見込まれており、格子暗号の場合、公開鍵暗号または鍵共有方式として、CRYSTALS-KYBER、NTRU、SABER のいずれか 1 つが採用され、デジタル署名として、CRYSTALS-DILITHIUM あるいは FALCON が採用されるとみられる。

以下では、最終候補の各方式に関する特徴や評価について、NIST の第 2 ラウンドにおける報告書（National Institute of Standards and Technology [2020]）を参照して紹介する。

イ. 公開鍵暗号（鍵共有）

（イ） CRYSTALS-KYBER（格子暗号）

Module-LWE 問題の計算困難性を利用した鍵共有方式である。理論的な安全性評価では、古典コンピュータに対して、藤崎・岡本変換により、IND-CCA2 を達成している。量子コンピュータに対しては、量子ランダム・オラクル・モデル[41]のもとで安全性が証明されている。Module-LWE 問題は新しい問題であるため、LWE 問題への解法よりも効率のよい解法が知られていない。セキュリティ・パラメータを変更することにより、トレードオフのある安全性と処理性能を柔軟に調整できる。総合的に、安全性と処理性能の観点で優れたパフォーマンスを示している。本方式は、デジタル署名の CRYSTALS-DILITHIUM と理論的フレームワークを共有して

41 古典コンピュータの世界では、ランダム・オラクル・モデルは、ハッシュ関数の返り値が、与えられた定義と値域から完全にランダムに選ばれる仮想的な状況を想定する。量子ランダム・オラクル・モデルは、これを量子コンピュータの世界に拡張し、ハッシュ関数の入出力として重ね合わせ状態を許容する。

おり、最も有望な KEM 方式（脚注 38 を参照）の 1 つであると見込まれる。

（ロ） NTRU（格子暗号）

NTRU 問題の計算困難性を利用した鍵共有方式である。理論的な安全性評価では、量子ランダム・オラクル・モデルのもとで IND-CCA を達成している。この方式の性能は高いが、格子暗号の中で最良とはいえない。とりわけ、Ring-LWE 問題や Module-LWE 問題を利用した方式に比べて鍵生成が遅い。他の最終候補である CRYSTALS-KYBER や SABER に比べてわずかに処理性能が劣っているが、Ring-LWE 問題や Module-LWE 問題とは異なる仮定に基づくため、次世代暗号の選出に多様性をもたせる観点からは有望である。また、研究の歴史が長く、暗号方式に係る知的財産に関するリスクが小さいことも、第 3 ラウンドの候補に残された理由である。CRYSTALS-KYBER や SABER に安全性や知的財産に関する懸念が生じた場合には、NTRU がより有望な候補になると見込まれる。

（ハ） SABER（格子暗号）

Module-LWE 問題の変種である Module-LWR 問題の計算困難性を利用した鍵共有方式である。理論的な安全性証明では、藤崎・岡本変換により、IND-CCA が示されているが、SVP の計算困難性を仮定したもとでの数学的な安全性証明が完全でない点は若干の注意が必要である。もっとも、特定の数学的設定（2 のべき乗の法を利用するなど）により、浮動小数点数を整数に丸める操作（rounding）を効率化することが可能であり、多項式の乗算と剰余演算を高速に実行できる。総合的な処理性能は優れており、汎用の暗号方式として利用できると期待される。以上から、最も有望な KEM 方式の 1 つであると見込まれる。第 3 ラウンドでは、サイドチャネル攻撃への耐性を重視して評価が行われる見通しである。

（ニ） Classic McEliece（符号暗号）

Goppa 符号を利用した McEliece 暗号（McEliece [1978]）にさまざまな改良が加えられた符号暗号である。理論的な安全性では、IND-CCA を達成している。性能はやや変則的であり、公開鍵が非常に大きい一方で、暗号文が他の候補方式の中で最も短い。公開鍵が大きいためインターネット通信のプロトコルには向かず、汎用的ではないが、暗号文が小さいことは他の用途では魅力的である。本方式は、最初期のバージョンの提案から 40 年を超える研究の蓄積があり、一定の信頼を寄せることができる安定した暗号方式であるといえる。

ロ. デジタル署名

（イ） CRYSTALS-DILITHIUM（格子暗号）

Module-LWE 問題の計算困難性を安全性の根拠としており、鍵共有方式の

CRYSTALS-KYBER と数学的原理は共通している。すべてのセキュリティ・レベルのカテゴリーに対して、（多項式剰余類環や法等の）共通の数学的設定を利用するため、後述の競合方式である FALCON よりも簡潔かつ少ないリソースで実装が可能である。処理性能は非常に優れており、バランスもとれている。具体的には、鍵や署名のサイズは大きくなく、鍵生成や署名作成、署名検証のアルゴリズムは高速に動作するなど、優れた処理性能をもつことが実験的に示されている。

（ロ） FALCON（格子暗号）

NTRU 問題を安全性の根拠としており、量子ランダム・オラクル・モデルのもとで安全性が証明されている。競合方式である CRYSTALS-DILITHIUM に比べて、データ構造やアルゴリズムが複雑である。すなわち、木構造のデータ、拡張浮動小数点演算、離散ガウス分布からのランダム・サンプリング等を用いるほか、セキュリティ・レベルのカテゴリーに応じて（多項式剰余類環の選び方等の）数学的な設定が変化する。総合的な処理性能は優れている。すなわち、公開鍵と署名のサイズは最小の部類であり、署名作成や署名検証を高速に実行できる一方、鍵生成は遅い。

（ハ） Rainbow（多変数多項式暗号）

多変数多項式暗号を利用した Unbalanced Oil-Vinegar 署名方式（Kipnis, Patarin, and Goubin [1999]）にさまざまな改良を施した方式であり、MQ 問題を安全性の根拠としている。この方式では、署名およびその検証は高速に実行可能であり、署名鍵（秘密鍵）が非常に短い一方で、検証鍵（公開鍵）が非常に大きい。次世代暗号の候補方式の多様性を確保するために最終候補に選定されたが、公開鍵の大きさから汎用向けの暗号方式としては適しているとは言い難い。実際に利用する場合には、頻繁に公開鍵を送信しない状況に限られる。理論的な計算量とパフォーマンスにも乖離があり、より精緻な分析が必要である。また、セキュリティ・レベルの目標を達成するために、セキュリティ・パラメータも調整する必要がある[42]。

5. CRYPTREC 暗号リストにおける次世代暗号の位置づけ

2019 年に開催された量子コンピュータ TF では、量子コンピュータの動向、次世代暗号への移行のあり方、CRYPTREC 暗号リスト[43] における次世代暗号の取扱い

42 最近では、Rainbow と代替候補の GeMSS に対して、新しい攻撃手法が提案されており、多変数多項式暗号に基づくデジタル署名の安全性に懸念が生じている。これを受けて、NIST のフォーラム（https://csrc.nist.gov/Projects/post-quantum-cryptography/Email-List）において、今後の影響や対応が議論されている。

43 CRYPTREC 暗号リストは、使用が推奨された暗号のリスト（電子政府推奨暗号リスト）や、今後電

等について議論が行われた（暗号技術検討会［2019］）[44]。以下では、これらの議論の概要を紹介する。

(1) 次世代暗号への移行に関する見方

次世代暗号への移行について、量子コンピュータ TF の議論では、当面は現行の暗号を使い続けながらも、「大規模システムの更改には 10 年以上要することもあり、データのライフサイクルも踏まえ」つつ、「量子コンピュータに対しても準備しておくことが必要」との見解が示されており、移行に向けた取組みの重要性が指摘されている。

また、NIST が次世代暗号に一定の多様性を確保する方針を採るなかで、次世代暗号の利用形態は、「アプリケーションによって使用アルゴリズムを切り替えるようになる可能性」もあるとの見方が示されている。そのうえで、複数の方式が選択できる環境が整備されたとしても、「SHA-1 等の危殆化に備え SHA-3 が作られたがほとんど使われていない」ように、次世代暗号についても実際の普及の度合いも勘案しつつ、「どの暗号方式が残っていくかという点に留意が必要」との意見も示されている。これらは、今後も各種方式の評価を継続し、アプリケーションに応じた方式の選択を可能とする取組みも必要であるとの考え方に基づくものと捉えられる。

(2) CRYPTREC 暗号リストにおける取扱い

CRYPTREC 暗号リストにおける次世代暗号の取扱いについては、「CRYPTREC 暗号リストは、利用実績や普及見込みも考慮したものである」点を踏まえ、次世代暗号に関しては、「ガイドライン等の別文書にすることが適当」、「利用者視点としても、量子コンピュータに対する安全性を考えない従来のリストと、量子コン

子政府推奨暗号リストに掲載される可能性がある暗号のリスト（推奨候補暗号リスト）から構成されている。このうち、電子政府推奨暗号リストは、「政府機関の情報セキュリティ対策のための統一基準」（平成 30 年度版。サイバーセキュリティ戦略本部［2018］）において、政府機関において暗号を使用する際に参照することが推奨されている。金融分野では、金融情報システムセンターの「金融機関等コンピュータシステムの安全対策基準・解説書（第 9 版）」（金融情報システムセンター［2018］）において、データの漏洩防止策等として暗号の利用を検討する際に、同リストが参考として紹介されている。

44 このほか、暗号技術評価委員会は、量子超越性を実験的に確認したとする Arute *et al.* [2019] の論文公表に際して、主張の解釈や CRYPTREC 暗号リスト掲載の暗号への影響を説明するレポート（暗号技術評価委員会［2020］）を公表している。

ピュータ時代の安全性を考えた暗号に関する文書とを分けることは適当」といった意見が示されている。なお、2020 年 6 月に開催された暗号技術検討会では、次世代暗号に関する文書を CRYPTREC 暗号リストに含まずに別の文書とすることが決定されている（暗号技術検討会［2020］）。

この次世代暗号に関する文書に関しては、具体的な内容に踏み込んだ議論は行われておらず、今後の検討項目となっているようである。もっとも、量子コンピュータ TF の議論では、「NIST 等の他のアクティビティが実施している取組みも参考にしていくことが適当」、「公開鍵暗号方式だけでなく、共通鍵暗号方式に対する影響についても言及すべき」といった意見が示されており、NIST による技術検証等を踏まえた内容にするほか、共通鍵暗号に関してもスコープに含むといった考え方が紹介されている。

6. 次世代暗号の実装に向けた取組み

NIST による標準化の候補方式の実装に向けた取組みが産業界において活発化している（Sikeridis, Kampanakis, and Devetsikiotis [2020]、Schwabe, Stebila, and Wiggers [2020]）。IETF においては、暗号通信プロトコル TLS（Transport Layer Security）[45] に実装するための技術仕様を拡張する検討等が行われている[46]。また、候補方式を実装した暗号ライブラリのプロトタイプの開発や各種の暗号製品への組込み、それらの性能評価を目的とする Open Quantum Safe が実施されている。

（1） IETF における検討

IETF では、既存の暗号と次世代暗号の両方を TLS において実装できるように、既存の TLS 1.3 の仕様の拡張が検討されている。こうした異なる暗号学的仮定に基づく複数の方式を同時に実装する手法は「ハイブリッド方式」と呼ばれることが多

45 TLS は、インターネット・バンキングをはじめとする各種のオンラインによる金融取引において、通信データの秘匿や一貫性の確保、通信相手の相互認証を実現する手段として普及している。本稿執筆時点における最新バージョンは 1.3 であり（Rescorla [2018]）、その技術仕様は RFC 8446 と付番されている。TLS 1.3 における鍵共有およびサーバ認証の処理の流れについては、補論 3 を参照されたい。

46 このほか、インターネット上におけるリモート・ログインやリモート・ファイル・コピー等の通信サービスにおいて認証や暗号通信を行うプロトコルである SSH（Secure Shell Protocol。RFC 4251）においても、TLS と同様に、ハイブリッド方式の実装を企図した仕様拡張の検討が開始されている（Kampanakis *et al.* [2020]）。

い[47]。以下では、ハイブリッド方式の概要を説明したうえで、TLS の仕様拡張に関する検討について紹介する。

イ．ハイブリッド方式

あるエンティティが暗号通信を他のエンティティとの間で行う際には、通信当事者間で同じ暗号方式を使用することが前提となる。次世代暗号を新たに使用したい場合、通信相手に、自分と同じ暗号を使用できる環境を整えてもらう必要がある。もっとも、すべての当事者が同じタイミングで暗号の移行を実現することは実務的に困難であり、相互運用性を確保しつつ暗号移行を実現するための工夫が求められる。

その手段の 1 つがハイブリッド方式である。既存の方式と将来移行の対象となる新しい方式の両方を使用できるように情報システムを整え、既存の方式のみ使用可能な通信相手にはそれを使用し、新方式を使用可能な通信相手には新方式を使用する。こうした状況を一定期間継続し、ハイブリッド方式を利用可能な通信環境を徐々に拡大していく。その後、既存の方式の安全性低下が顕現化した際には、既存の方式の使用を直ちに停止して新方式に切り替える。

もっとも、ハイブリッド方式では、両方の暗号を動作させるための追加的なハードウェアやソフトウェアが必要であり、こうした改修に伴うコストが発生する。また、通信相手との間でどの方式を使用するかを決定するなどの処理も追加的に発生し、実行時の処理時間が増加する。したがって、ハイブリッド方式の検討に当たっては、性能面への影響も考慮し、既存の技術仕様を極力変更しないようにする、処理時間の増加をなるべく抑制するなどの工夫が求められる。

ロ．TLS における仕様拡張の検討

（イ） 目標

TLS において次世代暗号を適用する対象は、公開鍵暗号による鍵共有（セッション鍵の共有）とデジタル署名（サーバ証明書の検証によるサーバ認証）の部分である。これらのうち、ハイブリッド方式を採用する対象となるのは鍵共有の部分であり、そのための仕様案（Internet Draft）が検討されている[48]。本稿執筆時点で有効な最新の仕様案（Stebila, Fluhrer, and Gueron [2021]）では、以下の目標が掲げられて

47 TLS 1.3 の仕様拡張の文脈では、ハイブリッド方式における鍵共有（hybrid key exchange）は、「少なくとも 1 つの鍵共有アルゴリズムが安全な状態である間はセッション鍵が安全な状態を維持できるようにする目的で、異なる暗号学的仮定に基づく複数の鍵共有アルゴリズムを使用する方法」と定義されている（Stebila, Fluhrer, and Gueron [2021]）。

48 デジタル署名に関しても、次世代暗号を TLS 等に実装した場合の性能を評価する研究が行われている（例えば、Sikeridis, Kampanakis, and Devetsikiotis [2020]、Schwabe, Stebila, and Wiggers [2020]）。もっとも、TLS におけるデジタル署名方式は、サーバの認証に用いられ、そのセッションの際に安全に実行できればよい（後日、署名方式が危殆化したとしても〈過去の〉サーバ認証自体は影響を受けない）ことから、鍵共有のようなハイブリッド方式は必ずしも必要でないとの見方がある（Paquin,

いる。

- 安全性の向上：（暗号学的な安全性の性質が異なる）複数の方式を組み合わせて鍵を共有することによって、それらのうち、少なくとも 1 つの方式が安全である限り（他の方式が安全でなくなったとしても）、共有した鍵の安全性が保たれるようにする。
- 後方互換性（backwards compatibility）：既存の暗号方式（現在の TLS 1.3 において準備されている方式）のみを使用可能な通信相手であっても、鍵共有を実現可能とする。
- 高性能（high performance）：ハイブリッド方式の鍵共有によって必要となる計算量がなるべく増加しないようにする。
- 低遅延（low latency）：ハイブリッド方式の鍵共有によって発生する通信の遅延（レイテンシー）がなるべく小さくなるようにする。
- 追加的な通信の回避（no extra round trip）：仕様を拡張したとしても、鍵共有に必要なデータの送受信の回数が増加しないようにする。
- 鍵の重複保有の回避（minimal duplicate information）：通信のデータ量の増加を抑制するために、同一タイプ（既存の方式あるいは新方式）の複数の鍵を通信相手に送信しないようにする。

（ロ） 仕様拡張のアイデアと課題

上記のハイブリッド方式による鍵共有の仕様案では、主な特徴として次の 3 点を挙げることができる（図表 2 を参照）。

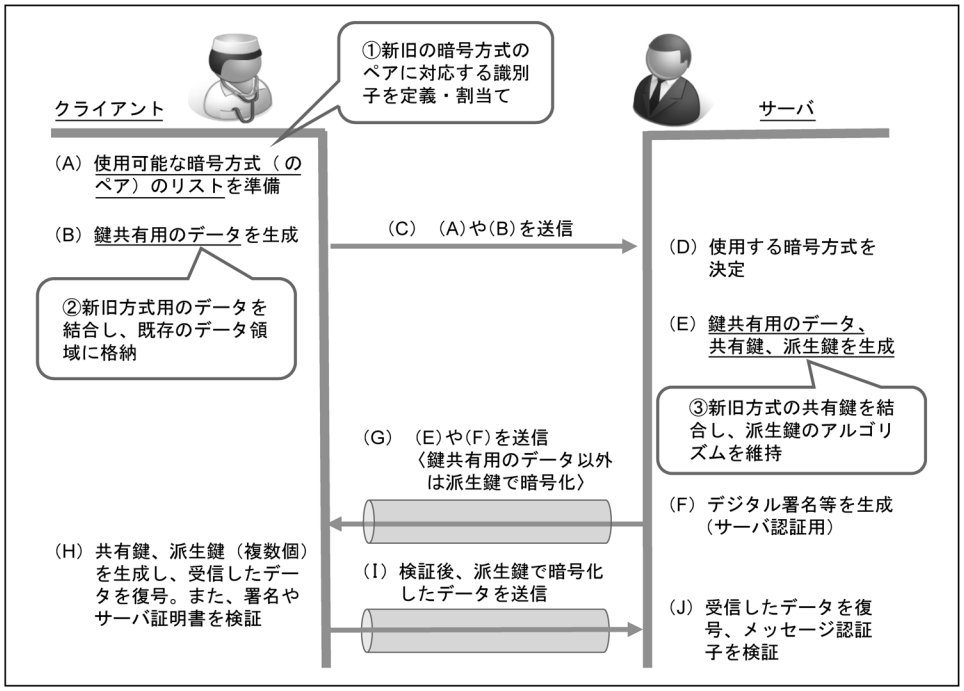
①ハイブリッド方式において使用する新旧の暗号方式（のペア）にそれぞれ識別子を定義し割り当てる。

—— TLS による通信では、クライアントとサーバは、鍵共有等に用いる方式を調整・決定する。最初に、クライアントが使用可能な方式の識別子（のリスト）とそれらの鍵共有用のデータをサーバに伝え、サーバは、それらの中から自分も使用可能な方式を選択し、その方式の識別子と（その方式に対応する）鍵共有用のデータをクライアントに返信する。ハイブリッド方式では、新旧の方式を組み合わせて新たに使用することとなるため、各ペアに対応する識別子を新たに定義・割り当てることとする。

②新旧の方式における鍵共有用のデータ（2 つ）を結合し、1 つのデータとして取り扱う。

Stebila, and Tamvada [2020]）。実際に、本稿執筆時点では、デジタル署名にかかるハイブリッド方式を目的とした仕様拡張案の提案には至っていないようである。

図表２　TLS 1.3 における鍵共有部分の仕様拡張のイメージ



―― ハイブリッド方式では、新方式における鍵共有用のデータが新たに発生するため、それを格納するためのデータ領域を新たに定義・追加する必要がある。データ領域の追加を回避するために、旧方式における鍵共有用のデータと結合し、結合後のデータを既存のデータ領域に格納する。

③新旧の方式によってそれぞれ生成される共有鍵（クライアントとサーバ間で共有される鍵）を結合し、それを用いて、通信データの一部を暗号化するための鍵（派生鍵）を生成する。

―― TLS 1.3 では、クライアントとサーバとの間の通信データの一部を共通鍵暗号によって暗号化する。この暗号化に用いられる派生鍵は、共有鍵をパラメータとして使用して生成される仕組みとなっている。ハイブリッド方式では、新方式における共有鍵が新たに発生するが、派生鍵の生成アルゴリズムの変更を回避するために、旧方式における共有鍵と結合して 1 つのデータとし、それを旧方式における共有鍵とみなして派生鍵を生成することとする。

もっとも、これらの拡張を行ったとしても実装上の課題がいくつか残されている（Stebila, Fluhrer, and Gueron [2021]）。その 1 つが、公開鍵や暗号文のサイズの上

限に関する問題である。次世代暗号では、既存の方式に比べて、公開鍵や暗号文のサイズが大きくなる傾向にある。一部の暗号方式では、これらのサイズが、既存のTLS 1.3 において規定されているデータ領域のサイズの上限を超えてしまう[49]。これへの対応として、①公開鍵や暗号を格納するデータ領域のサイズの上限を見直す、②公開鍵等を格納するための拡張領域を追加する、③公開鍵を外部のサーバ等に格納しておき、その場所を示すデータ（例えばURL）を公開鍵の参照情報として提供するというアイデアが示されている。

（2） Open Quantum Safe

Open Quantum Safe は、NIST による標準化の候補方式を動作させる暗号ライブラリ「LIBOQS」を開発するとともに、それらを組み込んだ暗号製品やそのプロトタイプを開発することを主な目的とする産学連携のプロジェクトである[50]。以下では、LIBOQS の開発の状況と、それを組み込んだ暗号製品の性能評価に関する研究成果の概要を紹介する。

イ． LIBOQS

LIBOQS は、C 言語によって記述されたオープン・ソースの暗号ライブラリであり、随時アップデートされて GitHub において公開されている。本稿執筆時点における最新のバージョン（0.5.0。2021 年 3 月 10 日リリース）の LIBOQS は、NISTの標準化における最終候補 7 件と、代替候補 6 件（鍵共有 4 件〈BIKE、FrodoKEM、HQC、SIKE〉、デジタル署名 2 件〈Picnic、SPHINCS+〉）をサポートしている。

LIBOQS の暗号製品への組込みに関しては、本稿執筆時点において、TLS、SSH、S/MIME（Secure/Multipurpose Internet Mail Extension）といった暗号プロトコルを動作させる暗号製品への組込み事例が紹介されている[51]。例えば、TLS を動作させるソフトウェアについて、OpenSSL や BoringSSL に LIBOQS をそれぞれ組み込んだ

49 例えば、鍵共有方式の 1 つである Classic McEliece の場合、最も小さなサイズのパラメータ・セットにおける公開鍵のサイズが 261,120 バイトとなっている。一方、TLS 1.3 における公開鍵と暗号文を格納するデータ領域のサイズの上限は 65,535 バイト（$= 2^{16} - 1$ バイト）に設定されており、Classic McEliece の公開鍵を格納することができない。

50 Open Quantum Safe には、ウォータールー大学、ロンドン大学、デラウェア大学、ラートボート大学、ニューメキシコ大学等の研究者に加え、IBM、Amazon.com, Inc.、Microsoft Corporation、Cisco Systems, Inc. 等の技術者や研究者が参画している（https://openquantumsafe.org/）。

51 S/MIME は、電子メールのセキュリティを強化するためのプロトコルであり、メッセージの暗号化とデジタル署名によって、メッセージの秘匿、送信者の認証、メッセージの一貫性確認の機能を有している。S/MIME（バージョン 4）で用いられるメッセージ形式が 2019 年に RFC 5751（S/MIME Version 4.0 Message Specification）として標準化されている。また、LIBOQS の暗号製品への組込みの状況については、https://openquantumsafe.org/applications において紹介されている。

OQS-OpenSSL、OQS-BoringSSL が開発・発表されている[52]。これらは、TLS 1.3 における鍵共有にハイブリッド方式を採用しているほか、デジタル署名方式に次世代暗号を採用している[53]。また、仮想プライベート・ネットワーク[54] を実現する、オープン・ソースのソフトウェア OpenVPN についても、LIBOQS 等を組み込んだ PQCrypto-VPN が開発・公開されている。

上記のソフトウェアだけでなく、LIBOQS をハードウェア・セキュリティ・モジュール[55] に組み込んで動作させる試みも発表されている。ドイツの暗号装置のメーカーである Utimaco GmbH と、次世代暗号の実装や評価を行っているセキュリティ・ベンダーであるカナダの evolutionQ Inc. は、Utimaco GmbH のハードウェア・セキュリティ・モジュール「CryptoServe」において LIBOQS を実装・動作させることができた旨を 2019 年に発表している[56、57]。

ロ. 性能評価

LIBOQS を組み込んだ暗号製品の性能評価として、TLS 1.3 を動作させた際の処理時間（TLS 1.3 の動作が開始されてから、鍵共有やサーバ認証が完了するまでの時間）を測定・評価する試みが活発化している[58]。以下では、最近の OQS-OpenSSL に関する評価事例として、ハイブリッド方式による鍵共有を採用した場合の処理時間を評価した事例と、サーバ認証用の署名方式に次世代暗号を採用した場合の処理

52 OpenSSL と BoringSSL は、TLS やその前身の暗号通信プロトコル SSL（Secure Sockets Layer）を動作させる主要な暗号ライブラリであり、特に、BoringSSL は OpenSSL から派生して開発されている。いずれもオープン・ソースとして提供されている。

53 OQS-OpenSSL については、次世代暗号を使用して S/MIME を動作させることが可能となっているほか、その公開鍵に対する電子証明書（代表的な証明書フォーマットである X.509 準拠の証明書）を発行する機能もサポートしている。

54 仮想プライベート・ネットワーク（virtual private network: VPN）は、オープンなネットワーク上の特定の拠点間において暗号技術によって仮想的に実現される閉域網である。また、こうした閉域網を実現する技術を VPN と呼ぶこともある。

55 ハードウェア・セキュリティ・モジュール（hardware security module）は、暗号の鍵の生成・保存、暗号処理等を実行するハードウェアであり、非侵襲攻撃（動作時の消費電力パターンや漏洩電磁波から内部の鍵を推定するなどのサイドチャネル攻撃等）や侵襲攻撃（カバーを剥離して回路を露出させ、細い電力を用いて内部の状態を観察するなどのプローブ攻撃等）を検知あるいは防止する機能を有する。

56 プレスリリースの URL は https://hsm.utimaco.com/news/utimaco-evolutionq-set-standards-by-taking-post-quantum-crypto-open-source/ である。なお、LIBOQS が適切に動作したことの検証を evolutionQ Inc. が実施した旨も説明されている。

57 このほか、クラウドでの次世代暗号の活用を検討する動きもみられる。例えば、IBM は、2020 年 11 月、クラウドとの通信やクラウド上でのデータの処理・保存において量子コンピュータに耐性を有する暗号技術（quantum-safe cryptography）の研究開発を進める方針を発表している。このプレスリリースは、https://newsroom.ibm.com/2020-11-30-IBM-Cloud-Delivers-Quantum-Safe-Cryptography-and-Hyper-Protect-Crypto-Services-to-Help-Protect-Data-in-the-Hybrid-Era に掲載されている。研究対象となるオープン・ソースのツールに Open Quantum Safe のツールも含まれることも示されている。

58 Open Quantum Safe のサイトでは、TLS の性能に関する測定結果（1 秒当たりの動作回数）が掲載されている（https://openquantumsafe.org/benchmarking/visualization/handshakes_series.html）。

時間を評価した事例をそれぞれ紹介する。

（イ） ハイブリッド方式による鍵共有を採用した場合の処理時間

Paquin, Stebila, and Tamvada [2020] は、OQS-OpenSSL（バージョン 1.1.1）を対象に、ハイブリッド方式による鍵共有の処理時間を測定・評価している。ここでは、既存の TLS 1.3 における鍵共有方式（ECDH〈鍵長 256 ビット〉）と、NIST による標準化における 3 つの候補方式（最終候補：CRYSTALS-KYBER、代替候補：FrodoKEM、SIKE）を組み合わせる形態を採用している[59]。また、ECDH を単独で動作させた場合の処理時間も測定しており（4,500 回測定）、ハイブリッド方式での処理時間と中央値によって比較している。実験環境は、1 台のサーバ上でクライアントとサーバを仮想的に立ち上げ、両者の間で TLS 1.3 の通信を行うというものである。クライアント・サーバ間の通信時間等を制御することによって、通信距離を無視できるほど近接しているケースや、遠隔地にあるクラウド上のサーバと通信を行うケース（通信の往復時間〈round trip time〉が 200 ミリ秒程度）が準備された。このほか、インターネットの通信路における通信品質の変動も考慮するために、パケットが一定の確率（パケット損失率〈packet loss rate〉。0〜20％）で欠損する状況を再現した実験も行われた。

実験の結果、CRYSTALS-KYBER を用いたハイブリッド方式による TLS 1.3 の処理時間は、ECDH 単独の場合に比べて目立って増加しなかった。通信時間や通信路の品質が変化しても、同様の結果となった。FrodoKEM を用いたハイブリッド方式については、通信路の品質が比較的悪い状況（パケット損失率が 5％以上）において、処理時間が ECDH 単独の場合よりも大きく増加した。また、両者の処理時間の差がパケット損失率の増加とともに拡大する傾向が示された[60]。SIKE を用いたハイブリッド方式については、比較的近距離（通信の往復時間が約 30 ミリ秒以下）の場合を除き、ECDH 単独の場合と比べて、処理時間が目立って増加することはなかった。一方、近距離の場合には、ECDH の場合に比べ、処理時間が大きく増加した[61]。

59 この評価の対象となっている候補方式は、いずれも NIST による標準化の第 2 ラウンドに提出されたアルゴリズムである。また、候補方式のパラメータの設定については、NIST のセキュリティ・レベル①（補論 2（2）イ.（ニ）を参照）に対応したパラメータが選択されている。

60 パケット損失率が増加すると、通信データの一部が欠損するケースが増え、それを補うために通信データを何度も再送することが必要となる。実験で用いられた FrodeKEM のパラメータ設定では、公開鍵や暗号文のサイズが、それぞれ約 9,600 バイト、約 9,700 バイトと非常に大きく（ECDH の 150 倍以上）、パケットの欠損に伴ってこれらが完全に送信できないケースが他の方式に比べて多くなる。そのため、パケット損失率の増加に伴って、ECDH 単独の場合の処理時間との差も増加したとみられている。

61 近距離になると、通信時間が短くなり、処理時間に占める暗号処理の時間の割合が大きくなる。そうしたなか、SIKE の暗号・復号処理の時間は共に 23 ミリ秒程度と ECDH の場合（暗号・復号処理が共に 0.07 ミリ秒程度）に比べて非常に大きいことから、近距離における両者の処理時間の差が生じ

（ロ） サーバ認証用に耐量子計算機暗号を採用した場合の処理時間

Paquin, Stebila, and Tamvada [2020] は、本節（2）ロ.（イ）において紹介した実験環境において、TLS 1.3 におけるサーバ認証用に次世代暗号を採用した OQS-OpenSSL を動作させ、その処理時間を測定・評価した。この実験では、鍵共有には、ECDH と CRYSTALS-KYBER を組み合わせたハイブリッド方式が採用され、デジタル署名には、既存方式である ECDSA（鍵長 256 ビット）や、NIST による標準化の 2 つの候補方式[62]（最終候補：CRYSTALS-DILITHIUM、代替候補：Picnic）が採用された。

CRYSTALS-DILITHIUM を使用した場合、処理時間（6,000 回測定して中央値で比較）は ECDSA の場合に比べて大きく増加することはなかった。一方、Picnic を使用した場合には、処理時間は ECDSA の場合よりも大きく増加し、両者の処理時間の差はパケット損失率が大きくなるほど拡大する傾向が示された[63]。

Sikeridis, Kampanakis, and Devetsikiotis [2020] は、Paquin, Stebila, and Tamvada [2020] と同様に、サーバ認証用に次世代暗号を採用した OQS-OpenSSL を動作させ、TLS 1.3 における処理時間を測定・評価している。署名方式には、NIST の標準化の 5 つの候補方式[64]（3 つの最終候補：CRYSTALS-DILITHIUM、FALCON、Rainbow、2 つの代替候補：Picnic、SPHINCS+）や、既存の方式（RSA 暗号〈鍵長 3,072 ビット〉、ECDSA〈鍵長 384 ビット〉）が採用されている。鍵共有方式には ECDH（鍵長 256 ビット）が用いられている。クライアントとサーバは遠隔地に設置され、インターネットでの通信の往復時間が約 11 ミリ秒かかるケース（米国内の通信）や最大で約 230 ミリ秒かかるケース（米国・アジア間の通信）で実験が行われている。

実験の結果、クライアントとサーバが共に米国内に設置されるケースにおいて、CRYSTALS-DILITHIUM と FALCON を用いた場合の処理時間（1,000 回の平均値）は、共に、既存の方式の場合に比べて大きく増加することはなかった[65]。Rainbow を用いた場合は、鍵やサーバ証明書のサイズが既存の方式に比べて非常に大きいこ

たとみられている。

62 候補方式は NIST による標準化の第 2 ラウンドに提出されたアルゴリズムであるほか、パラメータの設定については、NIST のセキュリティ・レベル①に対応したものが採用されている。

63 FrodoKEM の場合と同様に、実験での Picnic のパラメータ設定では、署名データのサイズが約 34,000 バイトと非常に大きく（ECDSA の 530 倍以上）、パケットの欠損に伴ってこれらが完全に送信できないケースが他の方式に比べて多くなる。そのため、パケット損失率の増加とともに、ECDSA の場合との処理時間の差も増加したとみられている。

64 候補方式は NIST による標準化の第 2 ラウンドに提出されたアルゴリズムであるほか、パラメータの設定については、NIST のセキュリティ・レベル①に対応したものが採用されている。

65 この実験では、サーバ証明書の検証の際に、ルート鍵を用いた中間認証局証明書の検証と、中間認証局の公開鍵によるサーバ証明書の検証の 2 段階の処理が実行される設定となっている。なお、Paquin, Stebila, and Tamvada [2020] では、中間認証局証明書を用いない設定となっており、サーバ証明書の検証では、ルート鍵を用いたサーバ証明書の検証のみを実行する設定となっていた。

とから、処理時間が既存の方式の 3 倍以上となった。Picnic と SPHINCS+ を用いた場合についても、署名のサイズが既存の方式に比べて非常に大きくなることから、処理時間は Rainbow の場合と同様に既存の方式に比べて 3 倍以上となった。

7. 結びに代えて：今後の展望

(1) 将来の暗号方式の安全性について

将来における暗号の安全性は、現代暗号と次世代暗号の双方とも不確実である。RSA 暗号や楕円曲線暗号等の現代暗号は、理想的な量子コンピュータが永遠に実現しなければ、その間は、安全性が保たれる可能性が高い。これに対して、次世代暗号は、理想的な量子コンピュータに対して安全であると現時点では考えられているが、研究の歴史が浅いため、安全性評価は十分に安定していないものもある。今後、新しい暗号解読アルゴリズムやサイドチャネル攻撃手法の発見等、想定しえない弱点が露呈して、古典コンピュータに対する安全性すら確保できなくなるおそれもある。今後も、より厳しい目線での評価を通じて、安全性評価の確度を高めていくことが求められる。

次世代暗号は高度な数学に基づくものが多く、安全性評価に関する情報も一般には難解である。有識者からは、安全性の評価結果に関して、CRYPTREC の活動等を通じて、適時適切な情報が発信されることを期待したい。

次世代暗号のユーザとなる組織・企業側も、逐次的に更新される安全性評価の動向に注意を払うことが望ましい。本稿では触れなかったが、実際の利用に際しては、次世代暗号の安全性を決めるセキュリティ・パラメータが多変数であるものが多いため、これらの値の組合せが適切であるかにも注意を払う必要がある。

(2) 次世代暗号への移行に向けて

次世代暗号への移行では、研究の蓄積のある現代暗号を活かしつつ、将来の量子コンピュータの脅威への保険として次世代暗号も利用し、暗号方式に冗長性をもたせるアプローチが望ましい。また、NIST による標準化では、1 つの技術革新が暗号全体の安全性を損なうことがないよう、異なる数学的問題に基づく方式を候補としており、暗号方式の多様性が確保されるように意図されている。こうした考え方を踏まえると、新規サービスに次世代暗号を採用する際には、暗号方式の将来的な入

替えも視野に入れたシステム設計が望ましい。

次世代暗号への移行に向けた動きは、既に米国政府だけでなく、主要ベンダーや標準化機関にも広がってきている。特に、世界最大の暗号ユーザである米国政府が2020年代後半に次世代暗号の標準化を完了させる見通しであることから、理想的な量子コンピュータの実現いかんによらず、標準化された方式が急速に普及していく公算が高い。

そうした場合、ネットワークの相互接続性の観点から、日本銀行を含む金融機関や決済事業者は、次世代暗号による通信や認証を実現可能な環境の整備を余儀なくされるであろう。今後、情報システムを新規に構築・更改する際には、次世代暗号への移行を見据えた検討が求められるといえる。

具体的な検討項目の1つは、ハイブリッド方式の採用である。ハイブリッド方式については、主要な暗号通信プロトコルであるTLSにおいて新旧の暗号方式を同時に実装する試みが進められており、一部の候補方式は十分な実装性を有するとの結果も示されている。また、IETFにおいても、ハイブリッド方式の標準化が進められていることから、早晩、ハイブリッド方式を実現する暗号ライブラリ製品が提供されるようになる可能性が高い。今後も、関連する動向を注視していくことが重要である。

次世代暗号への移行過程では、次世代暗号に対応した（ハイブリッド方式の）新システムとそうでない旧システムが混在することになる。その際には、新システムに後方互換性をもたせて配備を進めつつ、旧システムを徐々に入れ替えていくことになる。デジタル署名についても、タイムスタンプ局を利用した署名の有効期限の延長措置を活用することも選択肢である。いずれにしても、複雑な工程を経ることになるため、少なくとも十分な準備期間を設けるべきであろう（伊藤・宇根・清藤［2019］）。

(3) 暗号通貨への影響について

近年、ビットコインやその他の暗号資産等に利用される、管理者が存在しないパブリック・ブロックチェーンの社会的な重要性も高まっている。こうした情報システムでも、サービスの安全性を継続的に確保するために、次世代暗号への移行を求められる可能性が高い。

例えば、ビットコインでは2つの暗号技術が利用される。1つ目は、複数の取引データを1個のブロック（マークル木）にまとめる際や、ブロック同士の連結性の正しさを保証するために行うプルーフ・オブ・ワーク（Proof of Work）において採用される、ハッシュ関数SHA-256である。SHA-256の衝突検索問題については、

量子コンピュータで得られる高速化は高々 3 乗であるため、共通鍵暗号の場合と同様に、ハッシュ長を伸ばすことにより、現行方式の枠組み内で対応できる。2 つ目は、取引に付すデジタル署名で採用される ECDSA であるが、これは、次世代暗号に切り替える必要がある。

上記の移行の際には、新しく採用する暗号方式や移行のタイミングに関して参加者間で予め合意を形成する必要があろう。また、デジタル署名やハッシュ値については、過去の取引やブロックについても改ざんされないよう適切な保護措置をとる必要がある。例えば、次世代暗号への移行時点で、それ以前のブロックチェーン全体の情報のハッシュ値を計算しておく方法が考えられる。

最近では、プライバシー保護と取引の改ざん耐性を両立する手法も提案されている。双方の性質にそれぞれ保証される安全性のレベルが異なる場合もあるため、例えば、プライバシー保護には量子コンピュータに対する安全性までは保証しない方式を採用するなどの判断を行う場合には、その社会的な影響も考慮することが必要となろう。

参考文献

暗号技術検討会、「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース（第 3 回）議事概要」、Cryptography Research and Evaluation Committees、2019 年（https://www.cryptrec.go.jp/report/cryptrec-mt-1430-2019.pdf、2021 年 1 月 7 日）

———、「暗号技術検討会 2019 年度報告書」、Cryptography Research and Evaluation Committees、2020 年（https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2019.pdf、2021 年 1 月 7 日）

暗号技術調査ワーキング・グループ、「耐量子計算機暗号の研究動向調査報告書」、Cryptography Research and Evaluation Committees、2019 年（https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2018.pdf、2021 年 1 月 7 日）

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」、Cryptography Research and Evaluation Committees、2020 年（https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html、2020 年 12 月 8 日）

伊藤忠彦・宇根正志・清藤武暢、「量子コンピュータによる脅威を見据えた暗号の移行対応」、金融研究所ディスカッション・ペーパー No. 2019-J-15、日本銀行金融研究所、2019 年

金融情報システムセンター、『金融機関等コンピュータシステムの安全対策基準・解説書第 9 版』、金融情報システムセンター、2018 年

サイバーセキュリティ戦略本部、「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」、内閣サイバーセキュリティセンター、2018 年（https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf、2020 年 12 月 7 日）

四方順司、「量子コンピュータに耐性のある暗号技術の標準化動向：米国政府標準暗号について」、金融研究所ディスカッション・ペーパー No. 2019-J-4、日本銀行金融研究所、2019 年

情報通信研究機構・情報処理推進機構、『CRYPTREC Report 2019』、情報通信研究機構・情報処理推進機構、2020 年

高木　剛、『暗号と量子コンピューター耐量子計算機暗号入門―』、オーム社、2019 年

田渕　豊、「量子コンピュータハードウェアアーキテクチャ（超伝導素子）の検討」、情報処理学会量子ソフトウェア研究会発足記念講演会、2020 年

縫田光司、『耐量子計算機暗号』、森北出版、2020 年

廣田　修、「ゲート型量子コンピュータの量子ノイズ解析～大規模量子多体系のエラーモデルと実例～」、信学技報、120(105)、電子情報通信学会、2020 年、37～42 頁

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」、Cryptography Research and Evaluation Committees、2020 年（https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf、2020 年 12 月 7 日）

Arute, Frank, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John M. Martinis, "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature*, 574, 2019, pp. 505–511 (available at https://www.nature.com/articles/s41586-019-1666-5.pdf、2020 年 12 月 8 日).

Bardet, Magali, Jean-Chales Faugère, and Bruno Salvy, "On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations," Proceedings of the International Conference on Polynomial System Solving, 2004 (available at http://magali.bardet.free.fr/Publis/ltx43BF.pdf、2021 年 3 月 9 日).

Faugère, Jean-Charles, "A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F_5)," Proceedings of the 2002 ACM International Symposium on Symbolic and Algebraic Computation, Association for Computing Machinery, 2002, pp. 75–83.

Fujisaki, Eiichiro, and Tatsuaki Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes," Proceedings of CRYPTO 1999, Lecture Notes in Computer Science, 1666, Springer, 1999, pp. 537–554.

Gottesman, Daniel, "Stabilizer Codes and Quantum Error Correction," arXiv:quant-ph/9705052, 1997.

Grover, Lov K., "A Fast Quantum Mechanical Algorithm for Database Search," Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Association for Computing Machinery, 1996, pp. 212–219.

Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," Proceedings of International Algorithmic Number Theory Symposium

1998, Lecture Notes in Computer Science, 1423, Springer, 1998, pp. 267–288.

Jao, David, and Luca De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," Proceedings of International Workshop on Post-Quantum Cryptography 2011, Lecture Notes in Computer Science, 7071, Springer, 2011, pp. 19–34.

Kampanakis, Panos, Douglas Stebila, Markus Friedl, Torben Hansen, and Dimitrios Sikeridis, "Post-Quantum Public Key Algorithms for the Secure Sell (SSH) Protocol, Draft-Kampanakis-Curdle-PQ-SSH-00," Internet-Draft, Internet Engineering Task Force, 2020 (available at https://tools.ietf.org/pdf/draft-kampanakis-curdle-pq-ssh-00.pdf、2021 年 3 月 8 日).

Kaplan, Marc, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia, "Breaking Symmetric Cryptosystems Using Quantum Period Finding," Proceedings of CRYPTO 2016, Lecture Notes in Computer Science, 9815, Springer, 2016, pp. 207–237.

Kipnis, Aviad, Jacques Patarin, and Louis Goubin, "Unbalanced Oil and Vinegar Signature Schemes," Proceedings of EUROCRYPT 1999, Lecture Notes in Computer Science, 1592, Springer, 1999, pp. 206–222.

McEliece, Robert J., "A Public-Key Cryptosystem Based on Algebraic Coding Theory," The Deep Space Network Progress Report, DSN PR 42-44, National Aeronautics and Space Administration, 1978, pp. 114–116 (available at https://tmo.jpl.nasa.gov/progress_report2/42-44/44N.PDF、2021 年 3 月 9 日).

National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*, The National Academies Press, 2019（西森秀稔訳『米国科学・工学・医学アカデミーによる量子コンピュータの進歩と展望』、共立出版、2020 年）.

National Institute of Standards and Technology, "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms," 81 *Federal Register* 92787, 2016a, pp. 92787–92788, (available at https://federalregister.gov/d/2016-30615、2020 年 12 月 16 日).

———, "Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process," National Institute of Standards and Technology, 2016b (available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf、2020 年 12 月 16 日).

———,"Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process," National Institute of Standards and Technology, 2019 (available at https://doi.org/10.6028/NIST.IR.8240、2020 年 12 月 16 日).

————,“Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process,” National Institute of Standards and Technology, 2020 (available at https://doi.org/10.6028/NIST.IR.8309、2020 年 12 月 16 日).

National Security Agency, “Commercial National Security Algorithm Suite,” MFQ-U-OO-815099-15, National Security Agency, 2016 (available at https://apps.nsa.gov/iad/programs/iad-initiatives/cnsa-suite.cfm、2021 年 3 月 9 日).

Niederreiter, Harald, “Knapsack-Type Cryptosystems and Algebraic Coding Theory,” *Problems of Control and Information Theory*, 15(2), Akadémiai Kiadó, 1986, pp. 157–166.

Nielsen, Michael A., and Isaac L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2010.

Paquin, Christian, Douglas Stebila, and Goutam Tamvada, “Benchmarking Post-Quantum Cryptography in TLS,” Proceedings of Conference on Post-Quantum Cryptography 2020, Lecture Notes in Computer Science, 12100, Springer, 2020, pp. 72–91.

Peikert, Chris, and Zachary Pepin, “Algebraically Structured LWE, Revisited,” Proceedings of Theory of Cryptography Conference 2019, Lecture Notes in Computer Science, 11891, Springer, 2019, pp. 1–23.

Regev, Oded, “New Lattice-Based Cryptographic Constructions,” *Journal of the ACM*, 51(6), Association for Computing Machinery, 2004, pp. 899–942.

Rescorla, Eric, “The Transport Layer Security (TLS) Protocol Version 1.3,” Request for Comments: 8446, Internet Engineering Task Force, 2018 (available at https://tools.ietf.org/pdf/rfc8446.pdf、2021 年 3 月 9 日).

Schwabe, Peter, Douglas Stebila, and Thom Wiggers, “Post-Quantum TLS without Handshake Signatures,” Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, 2020, pp. 1461–1480.

Shor, Peter W., “Algorithms for Quantum Computations: Discrete Logarithms and Factoring,” Proceedings of 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, pp. 124–134.

————, “Scheme for Reducing Decoherence in Quantum Computer Memory,” *Physical Review A*, 52(4), 1995, pp. 2493–2496.

————, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing*, 26(5), Society for Industrial and Applied Mathematics, 1997, pp. 1484–1509.

Sikeridis, Dimitrios, Panos Kampanakis, and Michael Devetsikiotis, “Post-Quantum Authentication in TLS 1.3: A Performance Study,” Proceedings of Network and Distributed System Security Symposium 2020, Internet Society, 2020 (available at https://www.

ndss-symposium.org/wp-content/uploads/2020/02/24203.pdf、2020 年 12 月 17 日).

Simon, Daniel R., "On the Power of Quantum Computation," Proceedings of 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, pp. 116–123.

Stebila, Douglas, Scott Fluhrer, and Shay Gueron, "Hybrid Key Exchange in TLS 1.3, Draft-Ietf-Tls-Hybrid-Design-02," Internet-Draft, Internet Engineering Task Force, 2021 (available at https://tools.ietf.org/pdf/draft-ietf-tls-hybrid-design-02.pdf、2021 年 5 月 6 日).

Thompson, Neil C., Kristjan Greenewald, Keeheon Lee, and Gabriel F. Manso, "The Computational Limits of Deep Learning," arXiv:2007.05558, 2020.

Vepsäläinen, Antti P., Amir H. Karamlou, John L. Orrell, Akshunna S. Dogra, Ben Loer, Francisca Vasconcelos, David K. Kim, Alexander J. Melville, Bethany M. Niedzielski, Jonilyn L. Yoder, Simon Gustavsson, Joseph A. Formaggio, Brent A. VanDevender, and William D. Oliver, "Impact of Ionizing Radiation on Superconducting Qubit Coherence," *Nature*, 584, 2020, pp. 551–556.

Zhong, Han-Sen, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, Peng Hu, Xiao-Yan Yang, Wei-Jun Zhang, Hao Li, Yuxuan Li, Xiao Jiang, Lin Gan, Guangwen Yang, Lixing You, Zhen Wang, Li Li, Nai-Le Liu, Chao-Yang Lu, and Jian-Wei Pan, "Quantum Computational Advantage Using Photons," *Science*, 370(6523), 2020, pp. 1460–1463.

補論 1.　量子コンピュータの共通鍵暗号等への影響

ノイズを訂正する機能を有する大規模な量子コンピュータが実現すれば、公開鍵暗号の安全性が低下するだけでなく、データ本体の暗号化を担う共通鍵暗号やハッシュ関数の安全性についても、公開鍵暗号ほどではないものの、影響を受けるとみられている。グローバーのアルゴリズムを利用すると、共通鍵暗号の鍵の全探索やハッシュ関数の原像探索は、2 乗の高速化が可能である。また、ハッシュ関数の衝突を探索する問題は、3 乗の高速化が可能である（BHT アルゴリズム）。こうした攻撃の高速化に対しては、既存の暗号技術のもとで、鍵長を長くすることで対応できる。もっとも、最近では、共通鍵暗号を解読するアルゴリズムの効率を改善する研究が発表されており、留意が必要である（Kaplan *et al.* [2016]）。

CRYPTREC の暗号技術評価委員会は、量子コンピュータが共通鍵暗号（電子政府推奨暗号リストに掲載されているもの）の安全性に及ぼす影響について、外部専門家による評価を実施し、その報告書（細山田［2020］）を公表した[66]。

この内容に基づき、暗号技術評価委員会は、共通鍵暗号等に関する評価結果を「暗号技術評価委員会報告」（2019 年度版。情報通信研究機構・情報処理推進機構［2020］）において公表している。すなわち、「外部評価報告書の評価結果は妥当である」としたうえで、「電子政府推奨暗号リストにある共通鍵暗号、暗号利用モード、ハッシュ関数に対する直近で現実的な脅威が生じる可能性は極めて低く、現状では CRYPTREC での具体的な対応は不要である」としている。もっとも、先行きについては、「攻撃手法および量子コンピュータの発展に関して継続的な監視・評価が必要である」と付言しており、今後の研究動向に注意を払う必要があるとの考え方を示している。

66 細山田［2020］では、共通鍵暗号に関する評価結果として、「電子政府推奨暗号リストにある共通鍵暗号系技術の安全性に量子コンピュータが直接与える影響は “グローバーのアルゴリズムを用いると k ビット鍵の全数探索が時間 $\widetilde{O}(2^{k/2})$ で実行できるため、長期的に保護したいデータには鍵長が 192 ビットや 256 ビットの暗号技術を使用した方が賢明である” という以上のものは現状では無いと考えられる」との見解が示されている。

補論 2.　NIST による次世代暗号の評価基準

(1)　方式提案にかかる最低限の要件

- 提案方式のアルゴリズムの詳細が公開されていること。
- 提案方式は、以下のいずれかを満たしていること。

①公開鍵暗号方式については、鍵生成、暗号化、復号のアルゴリズムを有し、少なくとも 256 ビットの共通鍵暗号の鍵を暗号化・復号できること。
②KEM については、鍵生成、鍵カプセル化、鍵抽出のアルゴリズムを有しており、少なくとも 256 ビットの鍵共有が可能であること。
③デジタル署名方式については、鍵生成、署名生成、署名検証のアルゴリズムを有しており、2 の 63 乗ビットを上限とするメッセージの署名の生成・検証が可能であること。

(2)　評価基準

イ．セキュリティ

（イ）　公開鍵暗号系のアプリケーションの要件

- 米国政府機関が使用している暗号アプリケーション（例えば、TLS、SSH 等）で安全に実装することが可能であること。

（ロ）　暗号化と鍵共有のセキュリティの要件

- 攻撃者が任意に選んだ暗号文に対する平文を入手できるという環境のもとで、暗号文の情報が漏れないというレベルのセキュリティを達成していること。
- 上記のセキュリティを達成していることを数学的に証明することが望ましいが、必須ではない。

（ハ）　デジタル署名のセキュリティの要件

- 攻撃者が任意に選んだメッセージに対する署名（メッセージ数の上限は 2 の 64 乗未満）を入手できるという環境のもとで、ある特定のメッセージに対する署名の偽造が不可能というレベルのセキュリティを達成していること。
- 上記のセキュリティを達成していることを数学的に証明することが望ましいが、必須ではない。

（ニ）　セキュリティ・レベルの分類

- 提案方式のセキュリティを以下の 6 つのカテゴリーに分けて評価する。

①128 ビット鍵長のブロック暗号における鍵の全数探索と同程度のリソースが攻撃に必要なレベル（計算量：2 の 143 乗程度）
②256 ビットのハッシュサイズのハッシュ関数における衝突探索と同程度のリソースが攻撃に必要なレベル（計算量：2 の 146 乗程度）
③192 ビット鍵長のブロック暗号における鍵の全数探索と同程度のリソースが攻撃に必要なレベル（計算量：2 の 207 乗程度）
④384 ビットのハッシュサイズのハッシュ関数における衝突探索と同程度のリソースが攻撃に必要なレベル（計算量：2 の 210 乗程度）
⑤256 ビット鍵長のブロック暗号における鍵の全数探索と同程度のリソースが攻撃に必要なレベル（計算量：2 の 272 乗程度）
⑥512 ビットのハッシュサイズのハッシュ関数における衝突探索と同程度のリソースが攻撃に必要なレベル（計算量：2 の 274 乗程度）

—— 量子コンピュータ（超伝導回路方式）による攻撃のリソースの上限として、回路深度を設定する。回路深度は、量子コンピュータのゲート（回路素子）数で表現され、2 の 40 乗ゲート（1 年間量子コンピュータを動作しつづけたときに処理可能とみられる素子数）とする。

- 提案方式が対応するカテゴリーを明記するとともに、そのカテゴリーにおけるアルゴリズムのパラメータを明確にすること。

（ホ）　その他のセキュリティに関する特性

- 追加的な望ましい特性として、①完全前方セキュリティ（あるタイミングで鍵が漏えいしたとしても、それよりも過去の暗号文等が解読されないこと）、②サイドチャネル攻撃への耐性、③マルチ鍵攻撃（一度に複数の鍵の推定を試みる攻撃）への耐性、④アルゴリズムの誤った使用への耐性が挙げられる。これらに関して、提案方式の特性を明記することが望ましい。

（ヘ）　その他の考慮点

- その他の評価上の考慮点として、①アルゴリズムの数学的な構造（シンプルな構造が理解しやすく望ましい）、②提案方式のドキュメントの記述の明確さ、③分析の品質、④より多くの専門家による評価が挙げられる。これらに関して、提案方式の特性を明記することが望ましい。

ロ．コスト

- コストの観点では、①公開鍵、暗号文、署名のそれぞれのサイズ、②公開鍵・秘密鍵の処理にかかる性能（処理性能）、③鍵生成の処理性能、④復号の失敗の影響が挙げられる。これらの特性を明記することが望ましい。

ハ．その他の特性

（イ）柔軟性

- 例えば、①機能の追加の容易性、②パラメータの変更の容易性、③さまざまなプラットフォームにおける安全かつ効率的な実装の可能性、④高速処理を実現するための並列実装の可能性、⑤既存のプロトコルやアプリケーションへの組込み可能性が該当する。これらの特性を明記することが望ましい。

（ロ）アルゴリズムの簡便性

- アルゴリズムの構造がなるべく簡便であることが望ましい。

（ハ）使用可能性

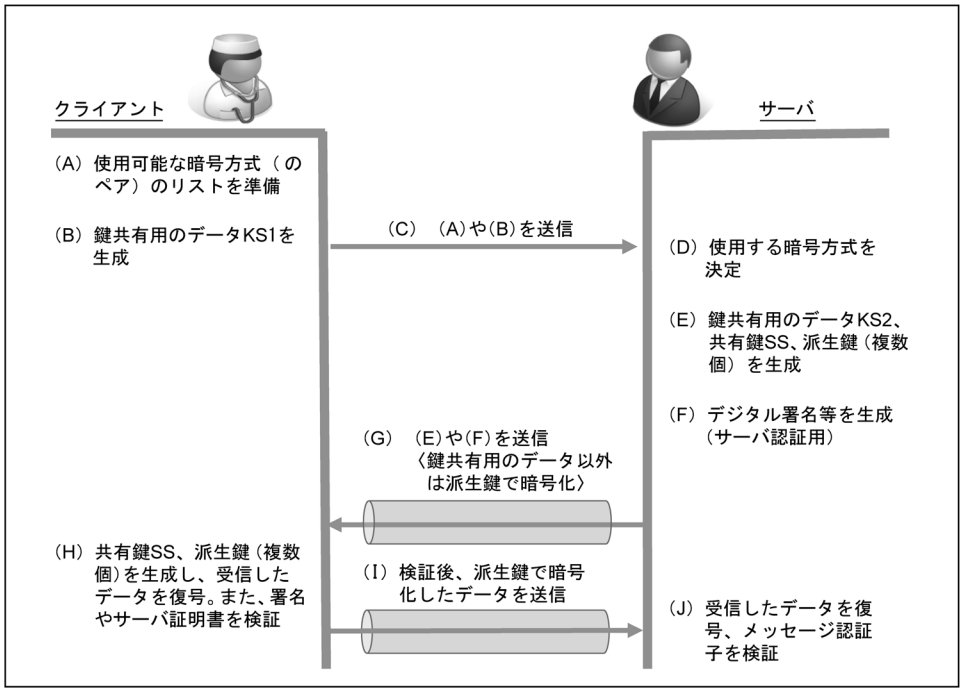
- 特許等の知的財産権の有無、使用に際してのライセンスの必要性に関して、明記することが必要である。

補論 3.　TLS 1.3 における鍵共有等の概要

TLS 1.3 においては、クライアントとサーバによる鍵共有とサーバ認証の手順がいくつか規定されている。ここでは、代表的なものの 1 つとして、クライアントとサーバが 1 往復の通信（1 round trip time）によってこれらを実行する場合を取り上げて紹介する。主な処理の概要は以下のとおりである（図表 A-1 を参照）。

（A）　クライアントは、鍵共有、サーバ認証（デジタル署名）、通信データの暗号化（共通鍵暗号、ハッシュ関数、メッセージ認証）に用いることが可能な暗号方式（のペア）の識別子のリストを生成する[67]。
（B）　クライアントは、鍵共有用のデータ KS1（両者で共有する鍵〈共有鍵〉を生成するために必要となるデータ。「key share」と呼ばれる）を生成する。こ

図表 A-1　TLS 1.3 における鍵共有の動作のイメージ



67 鍵共有方式としては、ディフィー=ヘルマン鍵共有方式（有限体上の方式〈DHE〉と楕円曲線上の方式〈ECDHE〉）、デジタル署名としては RSA 暗号（PKCS#1 あるいは PSS）または ECDSA が使用される。また、共通鍵暗号方式としては AES（暗号利用モードは GCM あるいは CCM）あるいは ChaCha20-Poly1305（メッセージ認証子による認証機能付き）、ハッシュ関数としては SHA-2 が使用される。

のとき、(A) においてリストアップした鍵共有方式が複数存在する場合、それらに対応する KS1 をそれぞれ生成する。

(C) クライアントは、(A) における識別子のリストと、(B) の鍵共有用のデータ KS1（複数の場合がある）を、サーバに送信する。

(D) サーバは、自分が使用可能な暗号方式のペアを考慮し、(A) におけるリストの中から、実際に使用する暗号方式のペアを決定する。

(E) サーバは、自身も鍵共有用のデータ KS2 を生成した後、(B) において得た KS1（(D) で決定した鍵共有の方式に対応するもの）と KS2 を用いて共有鍵 SS を生成・取得する。さらに、SS を用いて、後述の (G) の通信データの暗号化等に用いる鍵（派生鍵）を複数生成する。

(F) サーバは、サーバ認証のために、デジタル署名を生成する。

(G) サーバは、KS2、(F) における署名、(その署名を検証するための) サーバ証明書等をクライアントに送信する。このとき、KS2 以外は、(E) で生成した派生鍵によって暗号化（共通鍵暗号。メッセージ認証子も含まれる）して送信する。

(H) クライアントは、(G) で得た KS2 と KS1 から共有鍵 SS を生成した後、それを用いて派生鍵を複数生成する。これらの派生鍵を用いて、(G) における暗号文を復号し、その復号されたデータに含まれるサーバ証明書と署名を検証する。さらに、メッセージ認証子が含まれている場合にはその検証も行う。

(I) クライアントは、(H) における検証が成功したら、その結果を示すデータ等に対するメッセージ認証子を派生鍵によって生成するとともに、これらのデータを別の派生鍵によって暗号化してサーバに送信する。

(J) サーバは、(I) におけるデータの復号やメッセージ認証子の検証を行う（以降は、クライアントとサーバが、それぞれ派生鍵によってアプリケーションのデータを暗号化して相互に通信）。