量子コンピュータが共通鍵暗号の安全性に与える影響

清藤武暢（せいとうたけのぶ）／四方順司（しかたじゅんじ）

要　旨

近年、量子コンピュータや、それに耐性を有する耐量子計算機暗号の研究開発が活発化している。量子コンピュータが実現すると、現在主流の公開鍵暗号（RSA 暗号等）はもはや安全ではなくなることが知られている。共通鍵暗号については、これまで量子コンピュータの影響を受けにくいと考えられてきたが、近年、一部の暗号利用モードに関して、量子コンピュータによって現実的な時間で解読する手法が提案されている。本稿では、量子コンピュータが共通鍵暗号の安全性に与える影響を、最新の研究動向に基づき整理する。そのうえで、共通鍵暗号の安全性低下に対して、金融機関がどう対応していくべきかについて考察する。

キーワード：暗号利用モード、共通鍵暗号、耐量子計算機暗号、量子コンピュータ

本稿の作成に当たっては、NTT セキュアプラットフォーム研究所主幹研究員の青木和麻呂氏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、日本銀行あるいは横浜国立大学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。

清藤武暢　日本銀行金融研究所主査（E-mail: takenobu.seitou@boj.or.jp）
四方順司　横浜国立大学大学院環境情報研究院（E-mail: shikata@ynu.ac.jp）

無断での転載・複製はご遠慮下さい。

1. はじめに

金融分野では、各種取引の安全性を確保するために暗号が広く利用されている。例えば、金融機関のホストコンピュータと ATM の間でやり取りされるデータ（暗証番号や口座番号等）の機密性と完全性の確保や、オンライン・バンキングにおける通信相手の認証等で活用されている。

今後、暗号の安全性に対して脅威となりうる技術として、量子力学の性質を演算処理に応用した量子コンピュータ（特に、量子ゲート型コンピュータ）がある[1,2]。近年、この実用化に向けた研究開発が活発化しており、処理性能が向上している。量子コンピュータの処理性能が一定のレベルに達すると、現在主流の公開鍵暗号（RSA 暗号や楕円曲線暗号）を現実的な時間で解読できることが知られている（Shor [1994, 1997]、Bennett *et al.* [1997]、Brassard, Høyer, and Tapp [1998]、四方・鈴木・今井［1999］等）。

こうした状況を踏まえ、量子コンピュータでも容易に解読できない公開鍵暗号（耐量子計算機暗号）に関する研究が盛んに行われている。米国連邦政府は、現在主流の RSA 暗号を数時間で解読する量子コンピュータが 2030 年頃までに実現する可能性があるとの見解を示したうえで、2022 年頃までに耐量子計算機暗号の政府調達基準を策定し、現在使用している公開鍵暗号を 2026 年頃までに耐量子計算機暗号へ移行する計画を示している。この計画の一環として、米国の国立標準技術研究所（National Institute of Standards and Technology）では、連邦政府で使用する耐量子計算機暗号の標準化活動が開始されている（National Institute of Standards and Technology [2016a, b]、Chen [2017]）。

一方、共通鍵暗号については、量子コンピュータによる影響が公開鍵暗号に比べて小さいと考えられてきた。具体的には、暗号鍵のサイズを 2〜3 倍程度伸長することにより、これまでと同程度の安全性を確保できるとの見方が大勢であった。しかし、最近、一部の共通鍵暗号について、そうした対応が量子コンピュータの脅威への有効な対策とならないことを示唆する研究成果が報告されており、暗号鍵のサイズ伸長以外の対策が必要となってきている。共通鍵暗号は、オンライン・バンキングや IC カード（クレジットカード等）を用いた金融取引等のさまざまな金融サービスの安全性を支える基礎技術として広く利用されている。そのため、共通鍵暗号の安全性低下は金融サービス全体に大きな影響を及ぼす。したがって、金融機

1 量子力学とは、物質の構成単位である原子の内部構造のような極めて微細な世界における物理現象を対象とする物理学の研究分野の 1 つである。

2 量子コンピュータには、量子ゲート型コンピュータと量子アニーリング型（量子イジングマシン型とも呼ばれる）コンピュータの 2 種類の実装方法が存在する（詳細については 3 節を参照）。

関は、中長期（例えば、2030年以降）に亘って共通鍵暗号を利用する場合、量子コンピュータによる影響を適切に把握して、対応方針を検討する必要がある。

耐量子計算機暗号に関しては、これまで多くの研究成果が発表されており、それらを整理した解説論文も公表されている（高木［2017］、清藤・青野・四方［2015］等）。もっとも、量子コンピュータが共通鍵暗号の安全性に与える影響に関して俯瞰的に整理した文献は、筆者らが知る限り皆無に近い[3]。

本稿では、量子コンピュータが共通鍵暗号の安全性に与える影響に注目し、これまでに提案されている攻撃手法を整理するとともに、金融機関における対応について検討する。2節では共通鍵暗号の概要、3節では量子コンピュータの仕組みについてそれぞれ説明する。4節において量子コンピュータを利用した共通鍵暗号への攻撃手法について説明したうえで、5節において金融機関が共通鍵暗号の安全性低下にどのように対応していくべきかについて考察する。

2. 共通鍵暗号

(1) アルゴリズムと金融分野での用途

共通鍵暗号は、データ（平文）に対する暗号化や復号に同一の暗号鍵（共通鍵）を用いる暗号の総称である。共通鍵暗号により実現できる主な機能として秘匿とメッセージ認証が挙げられる。秘匿は、データをやり取りしている当事者（送信者と受信者）以外の第三者による覗き見を防止する機能である。メッセージ認証は、データが第三者に改ざんされていないこと（完全性）を検証する機能である。秘匿とメッセージ認証の機能を同時に実現する機能は認証付き秘匿と呼ばれる[4]。共通鍵暗号では、送信者と受信者の間で事前に共通鍵を共有する必要があるが、本稿ではどのように共有したかは問わないこととしたうえで、送信者と受信者が事前に共通鍵を共有していることを前提とする。

共通鍵暗号は、金融分野のいくつかの標準規格において規定されており、広く利用されている。共通鍵暗号が規定されている国際標準としては、ISO 9564-2とISO 16609が挙げられる。ISO 9564-2は、金融取引を行う際の本人確認で用いられる暗証番号（Personal Indentification Number: PIN）の安全性を確保する仕組みを規定し

3 欧州における情報技術・電気通信・放送にかかる標準化を推進する欧州電気通信標準化機構（European Telecommunications Standards Institute）は、量子コンピュータに対して安全性を確保するために必要な共通鍵サイズを見積った文献を公表している（European Telecommunications Standards Institute [2017b]）。ただし、当該文献は、一部の共通鍵暗号を検討対象外としている。

4 認証付き秘匿用の暗号は、認証暗号または認証付き暗号とも呼ばれる。

ており、ISO 16609 は、金融取引でやり取りされるデータにおける改ざんの有無を確認するための仕組みを規定している（International Organization for Standardization [2012, 2014]）。

また、オンライン・バンキングの安全性を確保するために利用される暗号通信プロトコル TLS（Transport Layer Security、Dierks and Rescorla [2008]）では、やり取りされるデータの安全性を確保するために共通鍵暗号が用いられている。また、クレジットカードおよびデビットカードの業界標準である EMV 仕様では、IC カードを用いた金融取引の安全性を確保するために共通鍵暗号の利用が推奨されている（EMVCo [2011]）[5]。

わが国においては、金融機関が情報システムのセキュリティ対策を行う際の指針となる金融機関等コンピュータシステムの安全対策基準・解説書において、利用する暗号を選定する際、CRYPTREC 暗号リストを参照することが推奨されている（金融情報システムセンター［2015］）。CRYPTREC 暗号リストには、総務省と経済産業省が事務局を担当する暗号技術検討会、およびその下に設置されている関連委員会（暗号技術評価委員会と暗号技術活用委員会。ともに情報処理推進機構と情報通信研究機構が事務局を担当）により安全性が確認された公開鍵暗号や共通鍵暗号等が掲載されている（総務省・経済産業省［2013］）。

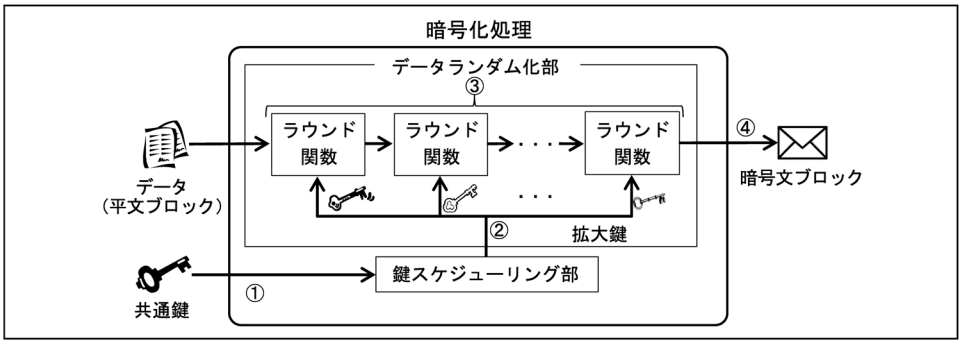
(2) ブロック暗号

金融分野で広く利用される共通鍵暗号では、ブロック暗号を構成要素としたうえで、それを一定のアルゴリズムに基づいて繰り返し使用して暗号化する仕組み（暗号利用モード）が採用されている[6]。ブロック暗号は、暗号化するデータを一定長のサイズのデータ（平文ブロック）に分割したうえで、各平文ブロックを共通鍵で

5 EMV 仕様（EMV specifications）とは、金融分野における IC カードを用いた取引に関する、IC カード内での暗号処理などを含めた仕様を定めたもの。

6 共通鍵暗号には、ブロック暗号を用いて実現するもののほかに、ストリーム暗号を用いて実現するものがある。ストリーム暗号は、現時点では、安全性の評価基準が必ずしも十分に確立されていない。そのため、金融分野では、安全性への信頼確保の観点からブロック暗号を用いて実現する共通鍵暗号が広く利用されている（International Organization for Standardization [2010]）。なお、ストリーム暗号は、主に秘匿の機能を実現する共通鍵暗号であり、例えば、携帯電話における通話内容の暗号化等の用途で利用されている（3rd Generation Partnership Project [2010] 等）。具体的には、暗号化するデータと同じサイズの共通鍵を生成し、両者の排他的論理和を計算することにより暗号文を生成する方式である。排他的論理和は、1 桁のビット同士で行う演算の 1 つであり、直感的には桁上りを無視した加算と解釈できる。すなわち、ビット同士の演算において、1 と 1 を単純に加算すると、通常の論理和では桁上りが発生して計算結果は 10 となる。一方、排他的論理和の演算においては、2 桁目は無視して計算結果を 0 とする。複数桁のビット同士で排他的論理和の演算を行う場合には、各ビット同士で上記の演算を行い、その結果を計算結果とする。

図表 1　ブロック暗号の典型的な暗号化処理



暗号化する方式である。本節（1）で紹介した標準規格に規定されている代表的なブロック暗号として、AES（Advanced Encryption Standard）が挙げられる。

一般に、ブロック暗号の暗号化処理は、鍵スケジューリング部とデータランダム化部によって行われる（図表 1 を参照）。①平文ブロックと共通鍵が入力として与えられ、②鍵スケジューリング部において共通鍵から複数の拡大鍵を生成する。そのうえで、③各拡大鍵をパラメータとして利用して平文ブロックを変換する。こうした変換に用いられる関数はラウンド関数と呼ばれる[7]。④上記③の処理結果を、平文ブロックに対応する暗号文のブロック（暗号文ブロック）として出力する。暗号文ブロックの復号処理は、ラウンド関数の処理内容により、暗号化処理と同じ場合と異なる場合がある。

ブロック暗号では、複数の平文ブロックと暗号文ブロックの組を入手できる攻撃者を想定したうえで、それらの情報をもとに送信者と受信者が共有している共通鍵を推測できないこと（安全性要件 1 と呼ぶ）が安全性要件として求められる。これは、共通鍵を知らない第三者が暗号文ブロックを入手したとしても、正しい平文ブロックを入手できないことを保証するためである[8]。後述する暗号利用モードは、安全性要件 1 を満たすブロック暗号を利用することを前提条件に設計されている。

(3)　暗号利用モード

ブロック暗号のみを用いて、各平文ブロックを単純に暗号化すると、同じ平文ブ

7 ラウンド関数は、排他的論理和や四則演算等を組み合わせた演算処理を行う関数であり、その処理は入力される拡大鍵に基づいて行われる。

8 ここでは、ブロック暗号が最低限満たすべき安全性要件について整理しているが、用途や安全性のレベル等によっては他の安全性要件が必要となる場合もある（後述する暗号利用モードの安全性要件についても同様）。共通鍵暗号の安全性要件の詳細については Rogaway [2011] 等を参照されたい。

ロックから同一の暗号文ブロックが生成される。この場合、ブロック暗号が安全性要件 1 を満たしていたとしても、暗号文ブロックの系列から平文ブロックに関する一部の情報（同じ平文ブロックが含まれていることなど）が漏洩するという問題がある。

そこで、ブロック暗号を構成要素とし、同じ平文ブロックを同一の共通鍵で暗号化したとしても、異なる暗号文ブロックが生成される仕組みを実現するためのアルゴリズム（暗号利用モード）が提案されている。具体的には、各平文ブロックの暗号化処理に関連性を持たせたり、初期値と呼ばれる値を暗号化処理に利用したりする仕組みが知られている。ここでは、秘匿、メッセージ認証、認証付き秘匿のための主要な暗号利用モードについて説明する。

イ．秘匿用の暗号利用モード

ISO 9596-2、TLS、EMV 仕様、CRYPTREC 暗号リストに規定されている秘匿用の暗号利用モードとして、CBC（Cipher Block Chaining Mode）、CFB（Cipher Feedback Mode）、CTR（Counter Mode）、OFB（Output Feedback Mode）が挙げられる（図表 2 を参照）。ここでは、データを n 個の平文ブロックに分割したうえで暗号化処理を行う状況を想定する。

各方式の安全性については、構成要素として用いるブロック暗号が安全性要件 1 を満たすことに加えて、任意に選択した（攻撃対象外の）データと初期値に対する暗号文を入手できたとしても、攻撃対象となる暗号文からデータの内容が漏洩しないこと（安全性要件 2 と呼ぶ）も必要となる[9]。一般に、安全性要件 1 を満たすとともに、初期値（乱数）が適切に選択されている場合には、その暗号利用モードは安全性要件 2 を満たすことが知られている[10、11]。

ロ．メッセージ認証用の暗号利用モード

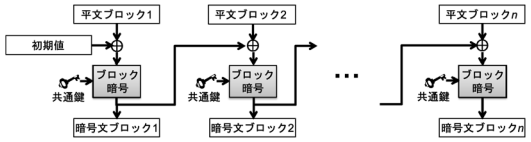
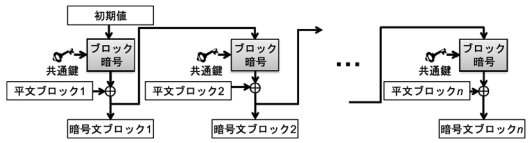
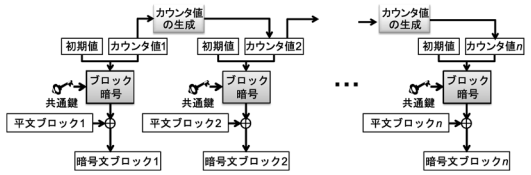
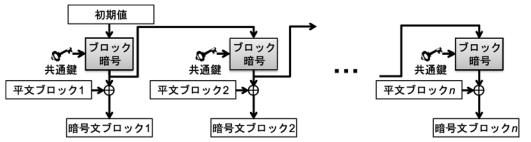
メッセージ認証用の暗号利用モードは、データの改ざんの有無を検証するデータ（認証子）を生成するために用いられる。ISO 16609、EMV 仕様、CRYPTREC 暗号リストに規定されているものとして、CBC-MAC（Cipher Block Chaining Message

9 このように、攻撃者が自身の都合のよいデータに対する暗号文を入手できるという攻撃モデルは選択平文攻撃と呼ばれる。この攻撃モデルは、一見すると現実的な脅威となりえないと考えられるが、近年、ウェブ・ブラウザの実装上の脆弱性を利用することにより、これを実現できる事例が報告されている（Rizzo and Duong [2011] 等）。

10 暗号化処理に使用した初期値は、第三者に秘匿しなくとも安全性要件 2 は満たされる。そのため、送信者はこれらを暗号文の一部として受信者へ送信することができる。

11 CBC を用いてデータを暗号化する際、そのデータは平文ブロックのサイズの定数倍である必要がある。定数倍よりも短い場合には、ランダムな値を付け加えて（パディングして）定数倍となるように調整する。他方、CFB と OFB は、データが定数倍でなくても暗号化できるが、特殊な初期値（例えば、0）を用いた場合には、同じ平文ブロックに対して同じ暗号文ブロックが生成されてしまうことが知られている（CRYPTREC［2003］）。

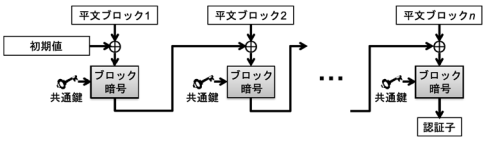
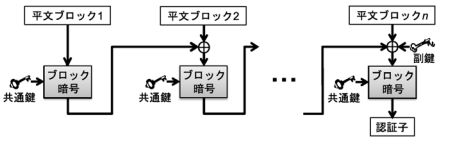
図表 2　秘匿用の暗号利用モード

方式名	概要	処理の流れ（イメージ）
CBC	平文ブロックを直前の暗号文ブロックと排他的論理和を行い、その結果をブロック暗号で変換して暗号文ブロックを生成する。最初の平文ブロックを暗号化する際には初期値を用いる。	
CFB	直前の暗号文ブロックをブロック暗号で変換し、その値と平文ブロックを排他的論理和を行って暗号文ブロックを生成する。最初のブロック暗号への入力には初期値を用いる。	
CTR	初期値とカウンタ値をブロック暗号で変換し、その値と平文ブロックを排他的論理和を行って暗号文ブロックを生成する。カウンタ値は最初のカウンタ値からある規則に基づき生成される。この規則については、送信者と受信者が共有しておく。	
OFB	直前にブロック暗号で変換した値を再度ブロック暗号で変換し、その値と平文ブロックを排他的論理和を行って暗号文ブロックを生成する。最初のブロック暗号への入力には初期値を用いる。	

Authentication Code）と CMAC（Cipher-based Message Authentication Code）が挙げられる（図表 3 を参照）。ここでは、データを *n* 個の平文ブロックに分割して、認証子を生成する状況を想定する。

各方式の安全性については、安全性要件 1 に加えて、任意に選択したデータとそれに対応する認証子を入手できたとしても、あるデータに対する認証子を偽造できないこと（安全性要件 3 と呼ぶ）が求められる。ここで、偽造する認証子に対応するデータについては、攻撃者が事前に認証子を入手したもの以外であることが前提となる。CBC-MAC について、構成要素として用いるブロック暗号が安全性要件 1 を満たし、さらに、初期値として用いられる乱数が適切に選択されている場合に

図表 3　メッセージ認証用の暗号利用モード

方式名	概要	処理の流れ（イメージ）
CBC-MAC	ブロック暗号による直前の変換結果と平文ブロックを排他的論理和を行い、その結果をブロック暗号で変換する。最後にブロック暗号で変換した値を認証子とする*。最初の平文ブロックを処理する際には、初期値を用いる。	
CMAC	ブロック暗号による直前の変換結果と平文ブロックを排他的論理和を行う。最後にブロック暗号で変換した値を認証子とする。最後の平文ブロックを処理する際には、共通鍵から生成した副鍵を用いる**。	

備考：＊厳密には、ブロック暗号で変換した値の一部を認証子とする（CMAC も同様）。認証子のサイズは、用途や安全性のレベルに基づき定められる。例えば、ISO 16609 では、ブロック暗号として AES を用いた場合、認証子のサイズは 32～128 ビットに設定することを推奨している。

＊＊厳密には、共通鍵から 2 種類の副鍵を生成する。認証子を生成するデータが平文ブロックのサイズの定数倍である場合には、一方の鍵を用いる。定数倍よりも短い場合には、パディングを行ったうえで、もう一方の鍵を用いる。

は、安全性要件 3 が満たされることが知られている[12、13]。

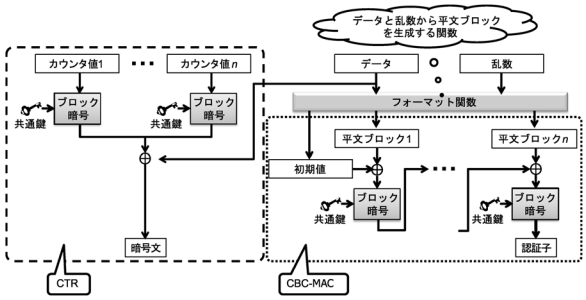
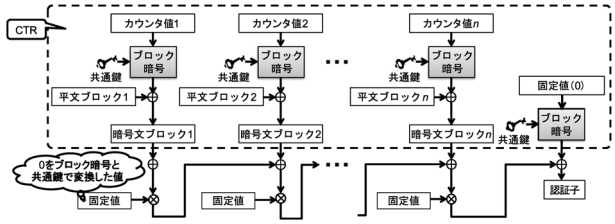
ハ．認証付き秘匿用の暗号利用モード

秘匿とメッセージ認証の両方を実現する方法として、それぞれの暗号利用モードを組み合わせることが考えられる。例えば、単純な方法として、データに対して暗号文と認証子をそれぞれ独立に生成するという方法が挙げられる。もっとも、この方法では安全性要件 2 と 3 がともに満たされないことが指摘されている（Bellare, Rogaway, and Wagner [2004] 等）。これらの機能を安全に実現するためには、データの暗号文と認証子の間に一定の関係性を生じさせることが必要とされている。このような暗号文と認証子の組を認証子付き暗号文と呼ぶ。

12 CBC-MAC では、認証子の生成に使用した初期値を第三者に秘匿しなくとも安全性要件 3 は満たされる。そのため、送信者は、初期値を認証子の一部として受信者へ送信することができる。

13 CBC-MAC では、CBC と同様、認証子を生成するデータのサイズが平文ブロックのサイズの定数倍でない場合には、定数倍となるようにパディングを行う必要がある。パディングを行う際、任意の値（例えば、乱数）をそのまま用いると安全性要件 2 が満たされないことが知られている（Bellare, Kilian, and Rogaway [2000]）。それへの対策として、CBC-MAC における安全なパディングの方法が示されている（International Organization for Standardization and International Electrotechnical Commission [2011] 等）。

図表 4　認証付き秘匿用の暗号利用モード

方式名	概要	処理の流れ（イメージ）
CCM	CTR と CBC-MAC を組み合わせる方式。乱数や同一の共通鍵を用いてデータの暗号文と認証子を生成し、それらを認証子付き暗号文とする。	
GCM	CTR と（ビット列同士の）乗算を組み合わせる方式。暗号文は、CTR を用いて生成する。認証子は、各暗号文ブロックを固定値との乗算で順次変換して生成する。	

認証付き秘匿用の暗号利用モードのうち、TLS および CRYPTREC 暗号リストに規定されているものとして、CCM（Counter with CBC-MAC）と GCM（Galois/Counter Mode）が挙げられる（図表 4 を参照）。ここでは、データを *n* 個の平文ブロックに分割したうえで、認証子付き暗号文を生成する状況を想定する。これらの方式に共通する特徴は、最初にデータの暗号化処理を行って暗号文を生成した後、当該暗号文に対して認証子を生成するという点である。

各方式の安全性については、一般に、構成要素として用いられるブロック暗号が安全性要件 1 を満たし、乱数が適切に選択されている場合、安全性要件 2 と 3 がともに満たされることが知られている[14]。

14 CCM においては、認証子付き暗号文の生成に使用した乱数を第三者に秘匿しなくとも安全性要件 2 と 3 は満たされる。そのため、送信者はこの乱数を認証子付き暗号文の一部として受信者へ送信することができる。

3. 量子コンピュータが共通鍵暗号の安全性に与える影響

(1) 量子ゲート型コンピュータ

量子コンピュータは、その原理の違いにより量子ゲート型コンピュータと量子アニーリング型コンピュータに分類される。量子ゲート型コンピュータは、任意の問題を解くことを目的としている。他方、量子アニーリング型コンピュータは、特定の組合せ最適化問題を解くことを目的としており、現時点では暗号を効率よく解読することは難しいと考えられている[15]。このため、本稿では、共通鍵暗号の安全性に影響を与えうる量子ゲート型コンピュータに注目する。

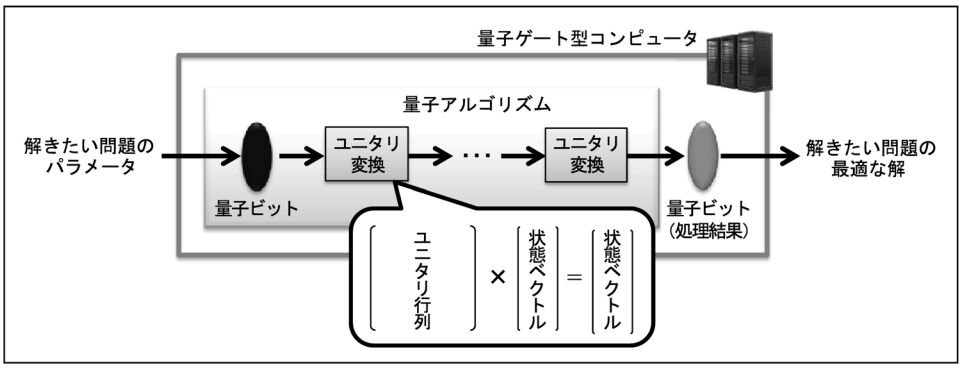
量子ゲート型コンピュータは、複数の状態が同時に存在するという性質（重ね合わせ状態）を利用する量子コンピュータである。従来のコンピュータでは、処理されるデータの最小単位であるビットによって0か1のどちらか1つの状態のみ表現することができる。そして、1回の演算処理により、ビットで表現されている1つの状態に対する演算結果のみが得られる。これに対して、量子ゲート型コンピュータでは、処理されるデータの最小単位は量子ビットと呼ばれる。重ね合わせ状態を利用することによって、1つの量子ビットで0と1の両方の状態を同時に表現することができるため、1回の演算処理によって、両方の状態に対して同時に（並列的に）処理を行うことができる。一般に、量子ゲート型コンピュータにおいて取扱い可能な量子ビットの数が2倍や3倍に増えると、1回で処理できる状態の数はそれぞれ4（$= 2^2$）倍や8倍（$= 2^3$）となる。このように、量子ゲート型コンピュータは、量子ビットの数が大きくなるにつれて、より大量のデータを同時に処理できるため、従来のコンピュータよりも格段に少ない演算回数で（すなわち、高速で）処理を実現できる。

量子ゲート型コンピュータを実現するうえで最も重要となるのが量子ビットの制御である。量子ビットは、外部から何らかの手段によって状態を観測すると、重ね合わせ状態が失われ、従来のコンピュータのビットと同様にいずれかの状態（1量子ビットの場合には0か1）に変化する。どの状態に変化するかは、量子ビットに設定される確率に依存する。したがって、量子ビットの重ね合わせ状態を維持しつつ、演算結果の量子ビットの状態を観測した際に正しい解を得られるように上記の確率を操作することが必要となる。

量子ビットに設定される確率を適切に操作する仕組みを実現するために、量子

15 量子アニーリング型コンピュータでは、対象とする問題をある種の物理問題（スピングラス問題と呼ばれる）に変換し、量子効果が働く装置を用いて行ったスピングラス問題の実験結果から、元の問題の解を求める。カナダのD-Wave System社が実用化し、2011年から販売を開始している量子コンピュータは量子アニーリング型コンピュータに属する（D-Wave Systems, Inc. [2011, 2017]）。

図表 5　量子ゲート型コンピュータと量子アルゴリズム（イメージ）



ゲート型コンピュータでは、状態ベクトルとユニタリ行列の乗算を繰り返し行うという手法が用いられている（図表 5 を参照）。状態ベクトルは、量子ビットの重ね合わせ状態を表現するベクトルである。また、ユニタリ行列は、問題を解くためのアルゴリズムを表現する行列であり、重ね合わせ状態を維持できるように設定される。

ユニタリ行列による変換（ユニタリ変換）の具体的な内容（ユニタリ行列の要素、それらの組合せや手順等）は、特定の問題の解を高い確率で得られるように定めることになる。ユニタリ変換を含む、量子ゲート型での処理の内容や手順は、量子アルゴリズムと呼ばれる。量子アルゴリズムを構成することは容易でなく、暗号に関する数学的問題を解くための量子アルゴリズムの提案例はまだ少ない。本稿では、共通鍵暗号の安全性に影響を与えうるものとして、グローバーのアルゴリズム（Grover [1996]）と、サイモンのアルゴリズム（Simon [1997]）を取り上げて説明する[16]。

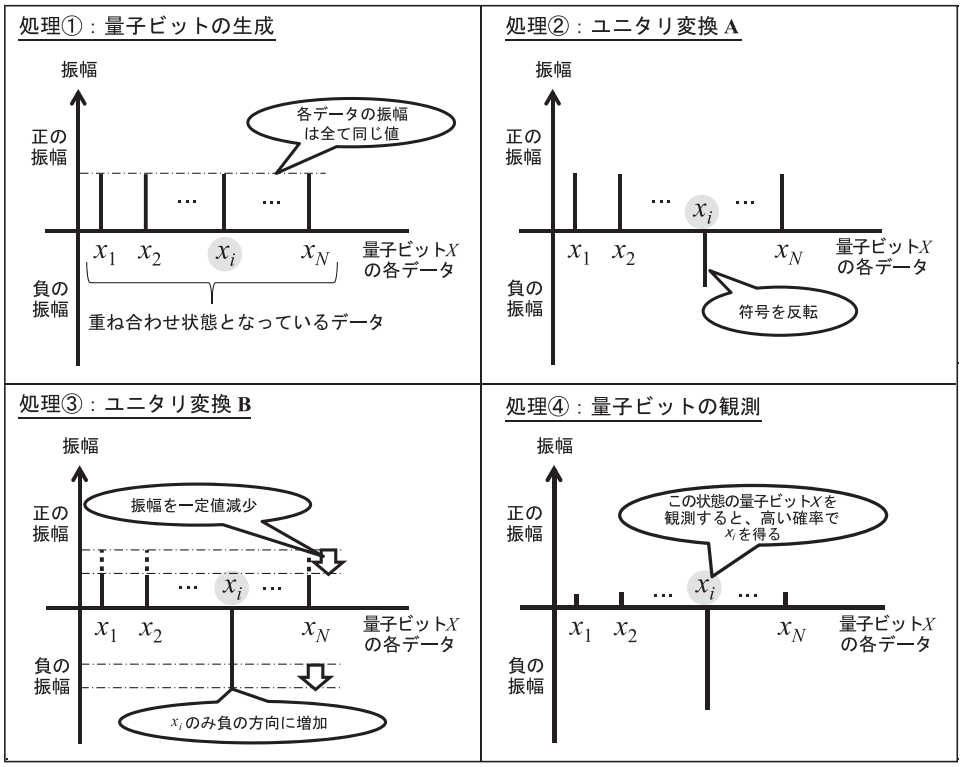
(2)　グローバーのアルゴリズム

グローバーのアルゴリズムは、データ探索問題を解くための量子アルゴリズムである。データ探索問題とは、一定の条件（探索条件）を満たす 1 個のデータを探索する問題である。グローバーのアルゴリズムでは、主に 2 種類のユニタリ変換を利用する。1 つは、探索条件に合致するデータにおける振幅の符号（正または負）を反転させるもの（ユニタリ変換 **A** と呼ぶ）である[17]。もう 1 つは、重ね合わせ状態

16 暗号に影響を与えうる量子アルゴリズムとしては、ショアのアルゴリズムも有名である（Shor [1994, 1997]）。ショアのアルゴリズムは、現在主流の公開鍵暗号（RSA 暗号や楕円曲線暗号）を高速に解読できることが知られている。

17 振幅は、量子の物理状態を示す尺度の 1 つである。この振幅を 2 乗した値が、対応するデータが観測される確率として用いられる。例えば、あるデータに対応する状態での振幅が 1/2 の場合には、こ

図表 6　グローバーのアルゴリズム（イメージ）



となっている全てのデータにおける振幅を一定の値だけ減らすもの（ユニタリ変換 **B** と呼ぶ）である。グローバーのアルゴリズムでは、ユニタリ変換 **A**、**B** を巧みに組み合わせることによって、探索条件に合致するデータにおける振幅のみを増大させ、それ以外の振幅を減少させる。

グローバーのアルゴリズムの処理の概要を以下に示す（図表 6 を参照）。ここで、探索対象となっているデータ（系列）を $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N$（$N$ は正の整数）とし、探索条件に合致するデータを $\boldsymbol{x}_i$ とする（$1 \leqq i \leqq N$）。はじめに、①探索対象の全てのデータが重ね合わせ状態となり、かつ各データの振幅が全て同じ正の値となるように量子ビット $\boldsymbol{X}$ を生成する。次に、②ユニタリ変換 **A** を用いて、探索条件に合致するデータ（$\boldsymbol{x}_i$）の符号を正から負に変更する。この時点では、$\boldsymbol{x}_i$ の値は判明していない。その後、③ユニタリ変換 **B** を用いて、全てのデータにおける振幅を一定の値（全てのデータの振幅の平均値）だけ減少させる。このとき、符号が負のデータ

のデータが観測される確率は $(1/2)^2 = 1/4$ となる。振幅は正と負の両方の符号をとることができる。この性質は、特定の状態（データ）の振幅を増加させる必要のある演算処理に有用であり、多くの量子アルゴリズムで利用されている。

は振幅の値が負の方向に増加し、観測時に確定する確率が増加する。④上記③を適切な回数繰り返した後、処理結果の量子ビットを観測することにより、高確率で探索条件に合致するデータ $\boldsymbol{x}_i$ を得る。

グローバーのアルゴリズムを利用すると、従来のコンピュータよりも少ない処理回数でデータ探索問題を解くことができる。例えば、探索対象のデータの総数 N を 2^{100} とすると、従来のコンピュータを利用した場合、各データが探索条件を満たすか否かを順次検証する必要があるため、最大で 2^{100}（10 進数で 30 桁）回の処理が必要となる。一方、グローバーのアルゴリズムを利用した場合、上記③を 1 回実行することにより、データ $\boldsymbol{x}_i$ を観測する確率を $1/2^{50}$ 程度増加させることができる[18]。そのため、処理③を 2^{50} 回程度繰り返すことにより、ほぼ確率 1 で $\boldsymbol{x}_i$ を得ることができる。探索に必要となる処理の回数を計算量としたとき、上記の例においては、従来のコンピュータを用いてデータ探索問題を解くためには 2^{100} 程度の計算量が必要となるが、グローバーのアルゴリズムを用いると 2^{50}（10 進数で 15 桁）程度の計算量で解くことができる。

(3) サイモンのアルゴリズム

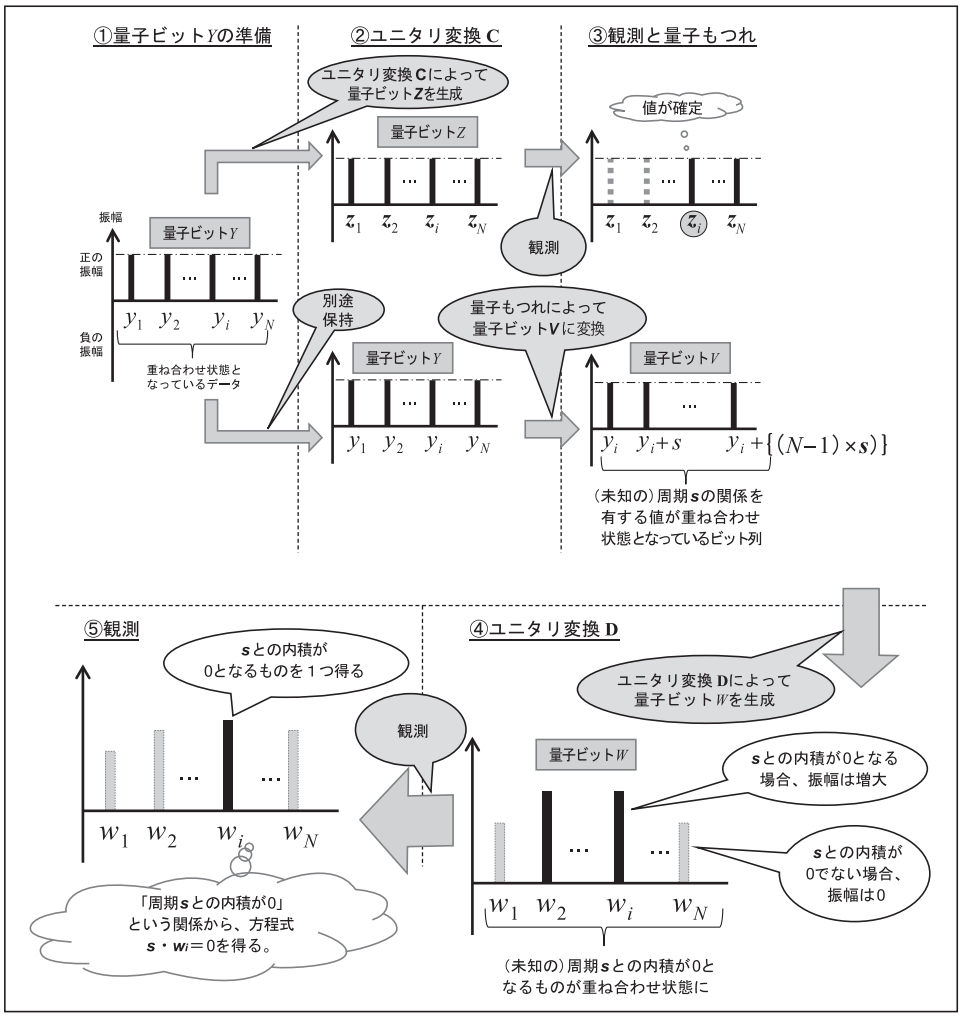
サイモンのアルゴリズムは、長さ n のビット列を入出力値とする関数 G が与えられたとき、出力値が同一となる異なる入力値の間に存在する周期性を求める問題（周期探索問題と呼ぶ）を解くための量子アルゴリズムである。例えば、$n = 3$ の場合、任意の入力値 $\boldsymbol{x}$ に対して $G(\boldsymbol{x}) = G(\boldsymbol{x} + 011)$ という関係が成り立つとき、G の周期 s は 011（2 進数表記。10 進数表記では 3）となる。このような周期が存在する関数は周期関数と呼ばれ、サイモンのアルゴリズムは周期関数における周期を求めるものである。

サイモンのアルゴリズムでは、G の周期を未知数とする連立方程式を構成したうえで、それを解いて周期を一意に求める。これを実現するために、2 種類のユニタリ変換を利用する。

サイモンのアルゴリズムにおける処理の概要を以下に示す（図表 7 を参照）。ここで、G が取りうる入力値（の系列）を $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_N$、これらに対応する出力値（の系列）を $\boldsymbol{z}_1, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_N$ とする（ただし、$N = 2^n$）。はじめに、① G の全ての入力値が重ね合わせ状態となっている量子ビット $\boldsymbol{Y}$ を生成する。次に、②量子ビット $\boldsymbol{Y}$ を量子ビット $\boldsymbol{Z}$ に変換する（この変換をユニタリ変換 $\mathbf{C}$ と呼ぶ）。量子ビット $\boldsymbol{Z}$ では、G の全ての出力値が重ね合わせ状態となっている。このとき、量子ビット $\boldsymbol{Y}$

18 直感的には、上記③において、全てのデータの振幅が $1/2^{50}$ 程度減少する。この値は、全てのデータの振幅の平均値となっている。

図表７　サイモンのアルゴリズム（イメージ）



を別途保持する。③量子ビット $\boldsymbol{Z}$ を観測し、ある出力値 $\boldsymbol{z}_i$ を確定する。このとき、（別途保持している）量子ビット $\boldsymbol{Y}$ は、量子もつれにより、（出力値が $\boldsymbol{z}_i$ となる）入力値 $\boldsymbol{y}_i, \boldsymbol{y}_i + \boldsymbol{s}, \ldots, \boldsymbol{y}_i + \{(N-1) \times \boldsymbol{s}\}$ の重ね合わせ状態となっている量子ビット $\boldsymbol{V}$ に変化する[19]。④量子ビット $\boldsymbol{V}$ を量子ビット $\boldsymbol{W}$ に変換する（ユニタリ変換 **D** と呼ぶ）[20]。⑤量子ビット $\boldsymbol{W}$ を観測し、$\boldsymbol{s}$ との内積が 0 となるビット列 $\boldsymbol{w}_i$ を確定する。

19 量子もつれとは、ある量子ビットの状態の変化が他の量子ビットの状態に影響を与える性質である。ここでは、量子ビット $\boldsymbol{Y}$ が量子もつれによって量子ビット $\boldsymbol{V}$ に変化するようにユニタリ変換 **C** を制御する。

20 量子ビット $\boldsymbol{W}$ は、長さ n の全てのビット列 $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_N$ が重ね合わせ状態となっており、周期 $\boldsymbol{s}$ と

長さ n のビット列同士の内積は、各ビットの値の乗算の和として表現されるため、ビット列 $\boldsymbol{w}_i$ は $\boldsymbol{s}$ との内積が 0 となることから、$\boldsymbol{s}$ の各ビット（n 個）を未知変数とする n 元 1 次方程式が得られる[21]。⑥上記①～⑤を n 回程度繰り返し、$\boldsymbol{s}$ を未知数とする n 元連立 1 次方程式を構成する。最後に、⑦この連立方程式を解き、周期 $\boldsymbol{s}$ を一意に特定する[22]。

サイモンのアルゴリズムを利用すると、従来のコンピュータよりも少ない計算量で周期探索問題を解くことができる。例えば、G が取り扱うビット列の長さが $n = 100$ の場合、従来のコンピュータを用いると、入力値と出力値の組が最大で 2^{100} 個必要となることが知られている。一方、サイモンのアルゴリズムを用いると、上記①～⑤を 100 回程度繰り返すことにより、周期 $\boldsymbol{s}$ を一意に求めるために必要な連立方程式を構成できる。連立方程式を構成するために必要な情報を集める手間を計算量としたとき、上記の例においては、従来のコンピュータを用いて周期探索問題を解く際には 2^{100} 程度の計算量が必要となるが、サイモンのアルゴリズムを用いると 100 程度の計算量で解くことができる。

4. 量子アルゴリズムを利用した攻撃手法

(1) 2 つの攻撃モデル

既存の研究では、攻撃者のみが量子ゲート型コンピュータを利用できる環境を想定してきた。この環境においては、送信者と受信者は従来のコンピュータを用いて暗号処理を行う。したがって、攻撃者が選択したデータに対する暗号文を入手する場合、攻撃者が入手できる暗号文は従来のコンピュータを用いて生成されたものとなる。整理すると、攻撃者は、通信路上のデータや任意に選択したデータに対する暗号文等を入手するとともに、量子ゲート型コンピュータを用いて任意の量子アルゴリズムを実行可能であるとする[23]。通信路上のデータや暗号文等は、従来のコンピュータを用いて生成されるとする。これを量子攻撃モデル 1 と呼ぶことにする。

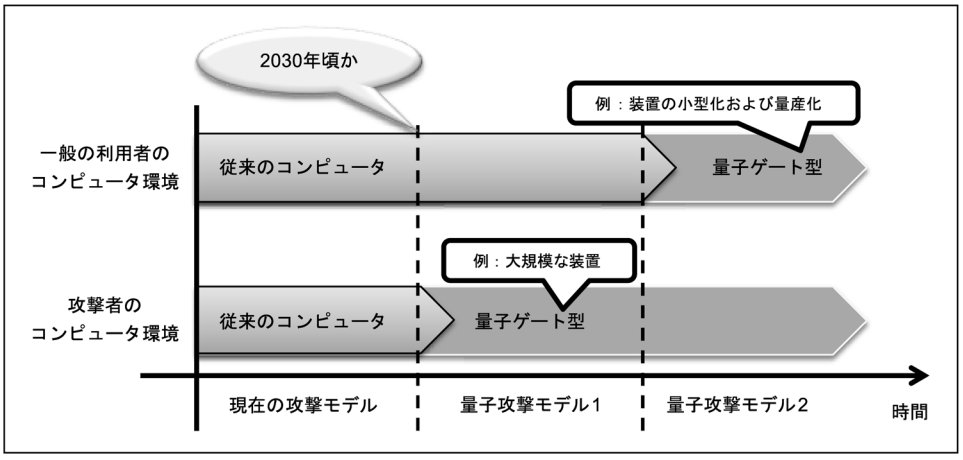
の内積が 0 となるビット列以外の振幅は全て 0 となっている。

21 $\boldsymbol{s}$ と $\boldsymbol{w}_i$ の各ビットをそれぞれ $\boldsymbol{s}[j]$、$\boldsymbol{w}_i[j]$（$j = 1, 2, \ldots, n$）としたとき、$\boldsymbol{s}$ と $\boldsymbol{w}_i$ の内積は $\boldsymbol{s}[1] \times \boldsymbol{w}_i[1] + \boldsymbol{s}[2] \times \boldsymbol{w}_i[2] + \cdots + \boldsymbol{s}[n] \times \boldsymbol{w}_i[n]$ と表現される。

22 連立方程式を解く処理は、従来のコンピュータ上でも効率よく解くアルゴリズム（ガウスの消去法等）が知られているため、従来のコンピュータを用いて計算を行ってもよい。

23 アイ・ビー・エム社は、2017 年 5 月よりクラウドを介して 16 量子ビットを取り扱うことができる量子コンピュータのサービスの提供を開始したほか、マイクロソフト社も同様のサービスを今後提供する予定であるとのプレスリリースを公表している（IBM [2017]、Microsoft [2017]）。

図表 8　量子コンピュータを用いる攻撃モデルの変化



最近では、攻撃者だけでなく一般の利用者も量子ゲート型コンピュータを利用できる環境も想定されている。この環境においては、送信者と受信者は量子ゲート型コンピュータを用いて暗号処理を行う。そのため、攻撃者は量子ビットで表現されたデータとその暗号文の組を得られる。整理すると、攻撃者は、通信路上のデータや任意に選択したデータに対する暗号文等を入手するとともに、任意の量子アルゴリズムを実行可能であるとする。ただし、通信路上のデータや暗号文等は、利用者が量子ゲート型コンピュータを用いて生成するものとする。これを量子攻撃モデル 2 と呼ぶ（図表 8 を参照）。量子攻撃モデル 2 は、量子攻撃モデル 1 よりも強力な攻撃であり、量子攻撃モデル 1 では安全とみられていた一部の共通鍵暗号を解読できることが示されている。

量子ゲート型コンピュータは、まずは大規模な装置によって実現されるとみられる。政府機関と同程度の開発力を有する攻撃者を想定すると、攻撃者は、まず大型の量子ゲート型コンピュータを利用する可能性がある（European Telecommunications Standards Institute [2017b]）。したがって、まずは、量子攻撃モデル 1 が現実的な脅威となりうると考えられる。米国連邦政府等の検討を踏まえると、量子攻撃モデル 1 については、2030 年頃を目途に現実的な脅威となる可能性がある（Mulholland, Mosca, and Braun [2017] 等）。

一方、一般の利用者にとってはクラウド等を介して共同で利用できる状況が考えられるものの、量子ゲート型コンピュータを利用してエンド・ツー・エンドでデータを暗号化するための対応はまだハードルが高く、当面は、暗号化処理には従来のコンピュータを用いる可能性が高いとみられる。今後、技術進歩により量子ゲート型コンピュータを実現する装置の小型化と量産化が進み、一般の利用者に普及するようになれば、それを用いてデータの暗号化等を行うことになると考えられる。こ

のような状況では、量子攻撃モデル 2 も現実的な脅威となりうる。この攻撃モデルの脅威が現実的なものとなる時期は、今後の量子ゲート型コンピュータの研究開発の進捗に依拠するため、現時点で厳密に推測することは難しく、余裕を持って対処できるように検討を進めることが重要である。

本節では、2 つの攻撃モデルのもとで、量子アルゴリズムに対するブロック暗号の安全性について説明する。ブロック暗号に対する攻撃手法は、全数探索法とショートカット法に大別できる。全数探索法は鍵候補をしらみつぶしに試してみるという手法である。ブロック暗号の内部構造の知識が不要であるものの、共通鍵のサイズに比例して鍵候補の数が指数関数的に増大する。ショートカット法は、複数の平文ブロックと暗号文ブロックの組やブロック暗号の内部構造に関する知識を用いて、鍵候補を絞り込むというものである。具体的な手法としては、差分攻撃（Biham and Shamir [1991, 1992]）、線形攻撃（松井［1993］、Matsui [1994]）、積分攻撃（Knudsen and Wagner [2002]、Todo [2017]）等が挙げられる。こうした手法と量子アルゴリズムを組み合わせることで、攻撃に要する計算量を削減できることが知られている（Bennett *et al.* [1997]、Brassard, Høyer, and Tapp [1998]、Kaplan *et al.* [2016b]）。

(2) 量子攻撃モデル 1 における安全性の評価と対策

イ. 全数探索法とグローバーのアルゴリズムの組合せ

全数探索法は、鍵候補から正しい共通鍵を探索するデータ探索問題を解く手法の 1 つと考えられる（Bennett *et al.* [1997]、Brassard, Høyer, and Tapp [1998]）。これをグローバーのアルゴリズムによって解く場合、まず、①全ての鍵候補の状態が重ね合わせ状態となっている量子ビット $\boldsymbol{X}$ を生成する。次に、②正しい共通鍵の振幅の符号のみを反転させるように、量子ビット $\boldsymbol{X}$ にユニタリ変換 **A** を適用する[24]。さらに、③上記②の処理結果に対してユニタリ変換 **B** を複数回適用し、正しい共通鍵の振幅のみを増大させる。最後に、④処理結果を観測し正しい共通鍵を得る。

共通鍵のサイズが 128 ビットの場合、攻撃者が従来のコンピュータを用いて共通鍵を導出するために必要となる計算量は、最大で 2^{128}（10 進数で 38 桁）となる。一方、グローバーのアルゴリズムを用いて共通鍵を導出するために必要となる計算量は、2^{64}（10 進数で 19 桁）程度となる。

24 ユニタリ変換 **A** は、正しい共通鍵であるか否かを判定できるように構成する必要がある。具体的には、攻撃者が任意に選択したデータとその暗号文の組を用いて、暗号文を復号した結果がデータと一致するか否かの判定を行う。攻撃者は予めデータと暗号文の組を入手していることが前提となる。

ロ．ショートカット法とグローバーのアルゴリズムの組合せ

ショートカット法では、①入手したデータと暗号文等の組から鍵候補を絞り込み、②縮退した鍵候補の集合に対し共通鍵の全数探索を行う。上記②の全数探索にグローバーのアルゴリズムを適用することができる。共通鍵の鍵候補の数を 2^a 個（ただし、$a > 0$）に絞り込んだ場合、攻撃者が従来のコンピュータを用いて共通鍵を導出するために必要となる計算量は最大で 2^a 程度となる。一方、グローバーのアルゴリズムを用いて共通鍵を導出するために必要となる計算量はで $2^{a/2}$ 程度となる。

ハ．対策

上記の各攻撃に対して各安全性要件を満たすためには、共通鍵のサイズを伸長する方法が知られている。グローバーのアルゴリズムを用いた場合の計算量は、従来のコンピュータの場合と同様に、共通鍵のサイズに比例して指数関数的に増大する。例えば、AES について、量子攻撃モデル 1 において従来の 128 ビットの共通鍵を用いた場合と同程度の安全性を確保するためには、共通鍵のサイズを少なくとも 2 倍（256 ビット）に伸長することが必要であると考えられる[25]。

(3) 量子攻撃モデル 2 における安全性の評価と対策

量子攻撃モデル 2 では、サイモンのアルゴリズムを用いた攻撃がいくつかの暗号利用モードに対して、有効であることが知られている。安全性要件 1 を満たすブロック暗号を利用し、共通鍵の伸長を行ったとしても、安全性要件 2 や 3 が満たされない場合がある（Kuwakado and Morii [2010, 2012]、Kaplan *et al.* [2016a]、Anand *et al.* [2016]）[26]。以下では、各暗号利用モードにおける具体的な攻撃手法について説明する。

25 近年、AES に対してグローバーのアルゴリズムと全数探索法を組み合わせた攻撃を行う際に必要となる量子ゲート型コンピュータのリソース（必要となる量子ビットの数やユニタリ変換を実装した回路の規模等）を評価した結果が示されている（Grassl *et al.* [2016]）。

26 サイモンのアルゴリズムを利用した攻撃がはじめて適用された共通鍵暗号は、エヴァン＝マンソール（Even-Mansour）暗号であった（Even and Mansour [1997]）。その後、ある特殊な関係を有する 2 つの異なる共通鍵を用いて収集した情報によって鍵候補を絞り込む攻撃（関連鍵攻撃と呼ばれる。Biham [1994]、Biryukov and Khovratovich [2009]）とサイモンのアルゴリズムを組み合わせた攻撃手法も提案されている（Hosoyamada and Aoki [2017]）。現時点では、筆者たちが知る限り、エヴァン＝マンソール暗号が金融サービスで用いられている事例はなく、当該攻撃が金融分野に与える影響はないと考えられる。もっとも、関連鍵攻撃は、AES に対する有効な攻撃の 1 つとされており、今後、サイモンのアルゴリズムと組み合わせた新しい攻撃手法が提案される可能性がある。

イ．秘匿用の暗号利用モードにおける攻撃手法

マユラシュ・ヴィベカナンド・アナンド（Mayuresh Vivekanand Anand）らは、秘匿用の暗号利用モードである CBC と CFB について、サイモンのアルゴリズムを用いて共通鍵を効率よく推定する手法を提案した（Anand *et al.* [2016]）。CBC と CFB について、構成要素であるブロック暗号が安全性要件 1 を満たし、初期値として適切な乱数が用いられたとしても、正しい共通鍵を得ることができるというものである。まず、①暗号利用モードを構成する一部の関数から、周期が共通鍵の値と一致するような周期関数 G を構成する。次に、② G が取りうる全ての入力値が重ね合わせ状態となっている量子ビット $\boldsymbol{Y}$ を、G の全ての出力値が重ね合わせ状態となっている量子ビット $\boldsymbol{Z}$ に変換するユニタリ変換 $\mathbf{C}$ を構成する[27]。そのうえで、③ユニタリ変換 $\mathbf{C}$ を用いてサイモンのアルゴリズムを実行し、G の周期（すなわち共通鍵）を得る。このように、CBC と CFB は、任意の暗号文を復号できるため、安全性要件 2 が満たされない。

共通鍵のサイズが 128 ビットの場合、攻撃者が従来のコンピュータを用いて共通鍵を導出するために必要となる計算量は、2^{128} 程度となる。一方、サイモンのアルゴリズムを用いて共通鍵を導出するために必要となる計算量は、128 程度となる。

ロ．メッセージ認証用の暗号利用モードにおける攻撃手法

マーク・カプラン（Marc Kaplan）らは、CBC-MAC について、サイモンのアルゴリズムを用いた攻撃手法を提案した（Kaplan *et al.* [2016a]）。ブロック暗号が安全性要件 1 を満たし、初期値として適切な乱数が用いられたとしても、認証子を偽造できるというものである。まず、①認証子を生成する処理から周期関数 G を構成し、②秘匿用の暗号利用モードにおける攻撃手法と同様の手順により、周期 $\boldsymbol{s}$ を得る[28]。次に、③任意のデータ $\boldsymbol{m}$ を選択した後、$\boldsymbol{m}$ に対応する認証子 t を利用者から得る。このとき、t は、$\boldsymbol{m}$ に $\boldsymbol{s}$ を加えたデータ（$\boldsymbol{m}+\boldsymbol{s}$）に対する正当な認証子となっており、攻撃者は $\boldsymbol{m}+\boldsymbol{s}$ に対応する認証子を得たことになる。このように、任意のデータに対する認証子を偽造することが可能であり、CBC-MAC は安全性要件 3 を満たさない。

共通鍵のサイズが 128 ビットの場合、攻撃者が従来のコンピュータを用いて認証

27 ユニタリ変換 $\mathbf{C}$ を構成する際に、任意のデータが重ね合わせ状態となっている量子ビットを、それらのデータに対する暗号文が重ね合わせ状態となっている量子ビットに変換する機構（量子オラクルと呼ばれる）が必要となる。暗号利用モードの暗号化処理が G の構成要素として組み込まれていることから、ユニタリ変換 $\mathbf{C}$ を構成するためには、量子ビットの重ね合わせ状態を維持したまま、暗号処理を行う必要がある。量子攻撃モデル 2 では、利用者が量子ゲート型コンピュータによって暗号文を生成することが前提となっており、攻撃者は、利用者による暗号文の処理を量子オラクルとして用いることもできる。

28 周期 $\boldsymbol{s}$ は、同一の認証子に対応する（異なる）複数のデータの差分値として設定される。例えば、データ $\boldsymbol{m}$ とデータ $\boldsymbol{M}$ が同一の認証子に対応するとき、差分値 $|\boldsymbol{m}-\boldsymbol{M}|$ が周期となる。

子を偽造するために必要な計算量は、最大で 2^{64} 程度となる（Kaplan *et al.* [2016b]）。一方、サイモンのアルゴリズムを用いて認証子を偽造するために必要な計算量は、共通鍵の導出の場合と同様に 128 程度となる。

ハ．認証付き秘匿用の暗号利用モードにおける攻撃手法

カプランらは、認証付き秘匿用の暗号利用モードである GCM についても、サイモンのアルゴリズムを用いて認証子を効率よく偽造する手法を提案した（Kaplan *et al.* [2016a]）。具体的な攻撃手法の手順や計算量は、CBC-MAC に対するものと同様である。この結果、GCM は安全性要件 3 を満たさないことになる。

ニ．対策

サイモンのアルゴリズムを用いた攻撃手法への対策については、現時点では研究途上である。学界でコンセンサスが得られた対策は確立していないものの、これまでに一部の研究者により提案されている方法を適用することが考えられる。例えば、共通鍵の値が周期と一致する周期関数を構成できないブロック暗号（耐量子計算機ブロック暗号と呼ばれる）を利用する方法（Banerjee, Peikert, and Rosen [2012]、Zhandry [2016] 等）や、サイモンのアルゴリズムの適用を困難にするための仕組みを導入する方法が知られている[29]。また、サイモンのアルゴリズムを用いた攻撃手法の適用が困難とみられている暗号利用モード（CTR、OFB、CMAC、CCM）を利用することも考えられる。

5. 金融分野に関連する標準規格への影響と対応方針

本節では、4 節で説明した量子ゲート型コンピュータによる攻撃手法が、金融分野に関連する標準規格にどのような影響を及ぼしうるか、また、それに対して金融機関がどのように対応する必要があるかについて整理する。

（1） EMV 仕様

EMV 仕様に基づく IC カードを用いた金融取引においては、端末（ATM 等）が、

29 一般に、サイモンのアルゴリズムでは、整数を入出力値とする周期関数の周期を効率よく求めることは現時点では難しいと考えられている（Kuperberg [2005]、Friedl *et al.* [2014] 等）。これに基づき、暗号利用モードで実行される演算を整数を用いたものに変更するという対策が提案されている（Alagic and Russell [2017] 等）。

カードの真正性やカード所持者の確認（カード認証、本人確認）、取引データ（金額や本人確認の結果等）の完全性の検証等を行うアプリケーション・クリプトグラム（Application Cryptogram）を生成する（EMVCo [2011]）。EMV 仕様では、カード認証と本人確認には公開鍵暗号（RSA 暗号）の利用が推奨されている。一方、アプリケーション・クリプトグラムの生成には共通鍵暗号、具体的には AES を構成要素とする CBC-MAC の利用が推奨されている。

量子攻撃モデル 1 を想定する場合には、公開鍵暗号の耐量子計算機暗号への移行を推奨するとともに、共通鍵のサイズ伸長に関する現行の規定を見直すことが望ましい。仮に共通鍵のサイズを 3 倍に伸長するとすれば、メッセージ形式を含めた仕様の見直しが必要となる可能性もある。一方、量子攻撃モデル 2 も想定する場合には、共通鍵暗号に関しては、共通鍵のサイズ伸長を行ったとしても、原理的に CBC-MAC の認証子を偽造できるため、取引データの完全性を確保できないと考えられる。攻撃を実行するためには、IC カードでの量子ビットの演算が実現している状況が前提となり、量子ゲート型コンピュータの小型化よりもさらにハードルが高いと考えられる。もっとも、急速な技術革新に備え、サイモンのアルゴリズムによる攻撃に耐性を有する暗号利用モード（CTR 等）を新たに仕様に追加し推奨する方向で検討することが望ましい。

(2) 暗号通信プロトコル TLS

TLS による通信は、公開鍵暗号（RSA 暗号等）を用いたサーバ認証および暗号通信用のセッション鍵共有、共通鍵暗号を用いた暗号通信の 3 つのフェーズから構成される。共通鍵暗号による暗号通信には、主にブロック暗号として AES が規定されており、暗号利用モードとして、CBC、CCM、GCM が規定されている（Dierks and Rescorla [2008]）。量子攻撃モデル 1 を想定する場合、公開鍵暗号については耐量子計算機暗号へ移行するとともに、共通鍵暗号については、いずれの暗号利用モードにおいても、共通鍵のサイズを伸長することによって安全性を確保しうると考えられる。その場合、TLS の仕様を見直す必要が生じる可能性がある。一方、量子攻撃モデル 2 も想定する場合、CBC と GCM に関しては、共通鍵のサイズを伸長したとしても、安全性の問題が生じる。CBC の場合には、セッション鍵が盗取されるリスクがあるほか、GCM の場合には、認証子の改ざんが行われるリスクが考えられる。そのため、サイモンのアルゴリズムによる攻撃に耐性を有する暗号利用モード（CCM）の利用を推奨するように規定を見直すことが考えられる。

(3) 国際標準

イ. ISO 9564-2

ISO 9564-2 は、PIN の安全性を確保するために、ブロック暗号として AES を規定している。また、秘匿用の暗号利用モードとして、CBC、CFB、OFB、CTR を規定している。量子攻撃モデル 1 を想定する場合には、共通鍵のサイズを伸長することにより、安全性を確保できると考えられる。その場合、共通鍵のサイズ伸長のために規定の見直しが必要になる可能性がある。量子攻撃モデル 2 も想定する場合、CBC または CFB を利用するケースでは、共通鍵のサイズ伸長を行ったとしても、PIN の機密性を確保するのが困難となる。そのため、サイモンのアルゴリズムによる攻撃への耐性を有する暗号利用モード（OFB、CTR）を推奨するように規定を見直すことが考えられる。

ロ. ISO 16609

ISO 16609 は、金融分野で利用するメッセージ認証用の暗号利用モードとして、CBC-MAC と CMAC を規定している（International Organization for Standardization [2012]）。量子攻撃モデル 1 を想定する場合には、共通鍵のサイズ伸長にかかる規定の見直しが必要になる可能性がある。量子攻撃モデル 2 も想定する場合には、共通鍵のサイズ伸長に加えて、サイモンのアルゴリズムによる攻撃への耐性を有する CMAC を推奨するように規定を見直すことが考えられる。

(4) CRYPTREC 暗号リスト

CRYPTREC 暗号リストは、ブロック暗号として、AES 等 3 つの方式を記載しているほか、①秘匿用の暗号利用モードとして、CBC、CFB、OFB、CTR、②メッセージ認証用として CMAC、③認証付き秘匿用として CCM と GCM を記載している。量子攻撃モデル 1 を想定する場合には、共通鍵のサイズ伸長に関する記載を追加することが望ましい。さらに、量子攻撃モデル 2 も想定する場合には、サイモンのアルゴリズムによる攻撃に耐性を有する暗号利用モードのみを記載する方向で見直すことを検討することが考えられる[30]。

30 CRYPTREC 暗号リストに記載されている公開鍵暗号（RSA 暗号や楕円曲線暗号等）についても、量子アルゴリズムを利用した攻撃を想定する場合には、耐量子計算機暗号のみを記載する方向で見直すことを検討する必要がある。

6. 結びに代えて：金融機関による対応について

従来、量子ゲート型コンピュータは、量子ビットの重ね合わせ状態を長時間維持することが難しく、実用化には相当な年月が必要と考えられてきた。しかし、近年、実装技術の研究が進展しており、量子ゲート型コンピュータの処理性能が飛躍的に向上する可能性が高まっている。その場合、5 節で示したように、公開鍵暗号だけでなく、金融分野で利用されている共通鍵暗号の安全性も低下することが懸念される。米国連邦政府は、2022 年頃までに耐量子計算機暗号の政府調達基準を策定し、現在使用している公開鍵暗号を 2026 年頃までに耐量子計算機暗号へ移行する計画を示している（National Institute of Standards and Technology [2016a, b]）。また、欧州連合においても、耐量子計算機暗号への移行時期を明確には示していないが、耐量子計算機暗号の標準化に向けたロードマップの検討を開始している（European Telecommunications Standards Institute [2017a]）。

こうした状況を踏まえると、わが国においても、今後、政府機関等を中心に量子コンピュータの脅威への対策に関する検討が進められると考えられる。金融機関においても、中長期に亘る利用が予定されるシステムについて、耐量子計算機暗号への移行の検討を開始するとともに、共通鍵暗号の安全性を確保するための対策についても検討していく必要がある。

対応方針として、①量子ゲート型コンピュータの研究開発に関する最新動向をフォローするとともに、関係する外部組織（他の金融機関、官公庁、ベンダー等）と情報共有や議論等を行うための連携体制を整備することがまず考えられる。また、②各種標準化団体に対し標準規格の見直しに向けた対応を働き掛けていくことも重要である。こうした対応と並行して、③自行内システムの移行に向けた検討を計画的に進める準備を行う必要がある。例えば、自行内システムにおける暗号の利用個所や情報資産を把握し、暗号の安全性低下がもたらす影響を分析するとともに、対応の優先順位を決定することが考えられる。こうした今後の検討項目の洗出しにまず着手し、いつまでにどのような対応・準備を行うべきかについて明確にしていくことが重要である。

量子ゲート型コンピュータの実用化には、今後、少なくとも 20 年程度の時間を要するとの見方もある。もっとも、金融業界では、これまでに、公開鍵認証基盤の導入やハッシュ関数の移行に十数年を要した事例もある。量子ゲート型コンピュータが実用化される時期を正確に予測できるまで対応を先送りするのではなく、来たる量子コンピュータの脅威に余裕をもって対処できるように準備を進めておくことが重要であろう。

参考文献

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 8 版追補改訂）』、金融情報システムセンター、2015 年

四方順司・鈴木　譲・今井秀樹、「量子計算による ECDLP の効率的解法について」、『電子情報通信学会技術研究報告』ISEC 99(329)、電子情報通信学会、1999 年、9〜15 頁

清藤武暢・青野良範・四方順司、「量子コンピュータの解読に耐えうる『格子暗号』の最新動向」、『金融研究』第 34 巻第 4 号、日本銀行金融研究所、2015 年、135〜170 頁

総務省・経済産業省、「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）」、総務省・経済産業省、2013 年（https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf、2018 年 9 月 14 日）

高木　剛、「ポスト量子暗号の構成法とその安全性評価」、『Fundamentals Review』11(1)、電子情報通信学会　基礎・境界ソサイエティ、2017 年、17〜27 頁

松井　充、「DES 暗号の線形解読法（I）」、『1993 年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、1993 年

CRYPTREC、「CRYPTREC Report 2003 ブロック暗号を使った秘匿、メッセージ認証、及び認証暗号を目的とした利用モードの技術調査報告」、CRYPTREC TR-2001-2003、CRYPTREC、2003 年（https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2003.pdf、2018 年 12 月 4 日）

Alagic, Gorjan, and Alexander Russell, “Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts,” *Proceedings of EUROCRYPT 2017 Part 3*, *Lecture Notes in Computer Science*, 10212, Springer-Verlag, 2017, pp. 65–93.

Anand, Mayuresh Vivekanand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh, “Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation,” *Proceedings of PQCrypto 2016*, *Lecture Notes in Computer Science*, 9606, Springer-Verlag, 2016, pp. 44–63.

Banerjee, Abhishek, Chris Peikert, and Alone Rosen, “Psudorandom Functions and Lattices,” *Proceedings of EUROCRYPT 2012*, *Lecture Notes in Computer Science*, 7237, Springer-Verlag, 2012, pp. 719–737.

Bellare, Mihir, Joe Kilian, and Phillip Rogaway, “The Security of the Cipher Block Chaining Message Authentication Code,” *Journal of Computer and System Sciences*, 61(3), Elsevier, 2000, pp. 362–399.

———, Phillip Rogaway, and David A. Wagner, “The EAX Mode of Operation,” *Proceedings of International Workshop on Fast Software Encryption (FSE) 2004*, *Lecture Notes in Computer Science*, 3017, Springer-Verlag, 2004, pp. 389–407.

Bennett, Charles H., Ethan Bernstein, Gilles Brassard, and Umesh Vazirani, “Strengths and Weaknesses of Quantum Computing,” *SIAM Journal on Computing*, 26(5), Society for Industrial and Applied Mathematics, 1997, pp. 1510–1523.

Biham, Eli, “New Types of Cryptanalytic Attacks Using Related Keys,” *Journal of Cryptology*, 7(4), Springer-Verlag, 1994, pp. 229–246.

———, and Adi Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” *Journal of Cryptology*, 4(1), Springer-Verlag, 1991, pp. 3–72.

———, and ———, “Differential Cryptanalysis of the Full 16-Round DES,” *Proceedings of CRYPTO 1992*, *Lecture Notes in Computer Science*, 740, Springer-Verlag, 1992, pp. 487–496.

Biryukov, Alex, and Dmitry Khovratovich, “Related-Key Cryptanalysis of the Full AES-192 and AES-256,” *Proceedings of ASIACRYPT 2009*, *Lecture Notes in Computer Science*, 5912, Springer-Verlag, 2009, pp. 1–18.

Brassard, Gilles, Peter Høyer, and Alain Tapp, “Quantum Cryptanalysis of Hash and Claw-Free Functions,” *Proceedings of LATIN 1998, Lecture Notes in Computer Science*, 1380, Springer-Verlag, 1998, pp. 163–169.

Chen, Lidong, “Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?” *IEEE Security & Privacy*, 15(4), IEEE, 2017, pp. 51–57.

Dierks, Tim, and Eric Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” Request for Comments 5246, Internet Engineering Task Force, 2008.

D-Wave Systems, Inc., “D-Wave Systems Sells Its First Quantum Computing System to Lockheed Martin Corporation,” D-Wave Systems, Inc., May 25, 2011.

———, “D-Wave Announces D-Wave 2000Q Quantum Computer and First System Order,” D-Wave Systems, Inc., January 24, 2017.

EMVCo, “Book 2 Security and Key Management,” EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, EMVCo, 2011.

European Telecommunications Standards Institute, “ETSI TC Cyber Working Group for Quantum Safe Cryptography Chairman’s Report,” ETSI IQC Quantum Safe Workshop, European Telecommunications Standards Institute, 2017a.

———, “Quantum-Safe Cryptography (QSC); Limits to Quantum Computing Applied to Symmetric Key Sizes,” ETSI GR QSC, 006, European Telecommunications Standards Institute, 2017b.

Even, Shimon, and Yishay Mansour, “A Construction of a Cipher From a Single Pseudorandom Permutation,” *Journal of Cryptology*, 10(3), Springer-Verlag, 1997, pp. 151–161.

Friedl, Katalin, Gábor Ivanyos, Frédéric Magniez, Miklos Santha, and Pranab Sen, “Hidden Translation and Translating Coset in Quantum Computing,” *SIAM Journal on Comput-*

ing, 43(3), Society for Industrial and Applied Mathematics, 2014, pp. 1–24.

Grassl, Markus, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt, "Applying Grover's Algorithm to AES: Quantum Resource Estimates," *Proceedings of PQCrypto 2016*, *Lecture Notes in Computer Science*, 9606, Springer-Verlag, 2016, pp. 29–43.

Grover, Lov K., "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of Symposium on Theory of Computing (STOC) 1996*, Association for Computing Machinery, 1996, pp. 212–219.

Hosoyamada, Akinori, and Kazumaro Aoki, "On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers," *Proceedings of International Workshop on Security (IWSEC) 2017*, *Lecture Notes in Computer Science*, 10418, Springer-Verlag, 2017, pp. 3–18.

IBM, "IBM Q," IBM, 2017 (available at: https://www.research.ibm.com/ibm-q/、2017 年 10 月 18 日).

International Organization for Standardization, "ISO/TR 14742: 2010 Financial Services—Recommendations on Cryptographic Algorithms," International Organization for Standardization, 2010.

———, "ISO 16609: 2012 Financial Services—Requirements for Message Authentication Using Symmetric Techniques," International Organization for Standardization, 2012.

———, "ISO 9564-2: 2014 Financial Services—Personal Identification Number (PIN) Management and Security—Part 2: Approved Algorithms for PIN Encipherment," International Organization for Standardization, 2014.

———, and International Electrotechnical Commission, "ISO/IEC 9797-1: 2011 Information Technology—Security Techniques—Message Authentication Codes (MACs)—Part 1: Mechanisms Using a Block Cipher," International Organization for Standardization, 2011.

Kaplan, Marc, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia, "Breaking Symmetric Cryptosystems Using Quantum Period Finding," *Proceedings of CRYPTO 2016 Part 2*, *Lecture Notes in Computer Science*, 9815, Springer-Verlag, 2016a, pp. 207–237.

———, ———, ———, and ———, "Quantum Differential and Linear Cryptanalysis," *IACR Transactions on Symmetric Cryptography*, 2016(1), International Association for Cryptologic Research, 2016b, pp. 71–94.

Knudsen, Lars R., and David A. Wagner, "Integral Cryptanalysis," *Proceedings of Fast Software Encryption (FSE) 2002*, *Lecture Notes in Computer Science*, 2365, Springer-Verlag, 2002, pp. 112–127.

Kuperberg, Greg, "A Subexponential-Time Quantum Algorithm for the Dihederal Hidden

Subgroup Problem," *SIAM Journal on Computing*, 35(1), Society for Industrial and Applied Mathematics, 2005, pp. 170–188.

Kuwakado, Hidenori, and Masakatsu Morii, "Quantum Distinguisher between the 3-Round Feistel Cipher and the Random Permutation," *Proceedings of IEEE International Symposium on Information Theory (ISIT) 2010*, IEEE, 2010, pp. 2682–2685.

———, and ———, "Security on the Quantum-Type Even-Mansour Cipher," *Proceedings of the International Symposium on Information Theory and Its Applications (ISITA) 2012*, IEEE, 2012, pp. 312–316.

Matsui, Mitsuru, "Linear Cryptanalysis Method for DES Cipher," *Proceedings of EUROCRYPT 1993*, *Lecture Notes in Computer Science*, 765, Springer-Verlag, 1994, pp. 386–397.

Microsoft, "With New Microsoft Breakthroughs, General Purpose Quantum Computing Moves Closer to Reality," News Release, Microsoft, 2017.

Mulholland, John, Michele Mosca, and Johannes Braun, "The Day the Cryptography Dies," *IEEE Security & Privacy*, 15(4), IEEE, 2017, pp. 14–21.

National Institute of Standards and Technology, "Report on Post-Quantum Cryptography," NIST Internal Report 8105, National Institute of Standards and Technology, 2016a.

———, "Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process," Call for Proposals, National Institute of Standards and Technology, 2016b.

Rizzo, Juliano, and Thal Duong, "BEAST: Surprising Crypto Attack against HTTPS," presentation at ekoparty Security Conference, ekoparty, 2011 (available at: https://www.youtube.com/watch?v=-BjpkHCeqU0、2018 年 12 月 4 日).

Rogaway, Phillip, "Evaluation of Some Blockcipher Modes of Operation," Cryptography Research and Evaluation Committees, 2011.

Shor, Peter W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings of Foundations of Computer Science (FOCS) 1994*, IEEE, 1994, pp. 124–134.

———, "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.

Simon, Daniel R., "On the Power of Quantum Computation," *SIAM Journal on Computing*, 26(5), Society for Industrial and Applied Mathematics, 1997, pp. 1474–1483.

Todo, Yosuke, "Integral Cryptanalysis on Full MISTY1," *Journal of Cryptology*, 30(3), Springer-Verlag, 2017, pp. 920–959.

Zhandry, Mark, "A Note on Quantum-Secure PRPs," *Cryptology ePrint Archive*, 1076,

International Association for Cryptologic Research, 2016.
3rd Generation Partnership Project, “LTE; Evoluted Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2,” European Telecommunications Standards Institute, 2010.