IMES DISCUSSION PAPER SERIES

量子鍵配送の安全性証明の進展と普及に向けた課題

菅 和聖・佐々木寿彦

Discussion Paper No. 2024-J-6

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2024-J-6
2024 年 4 月

量子鍵配送の安全性証明の進展と普及に向けた課題

菅 和聖*・佐々木 寿彦**

要　　旨

本稿では、量子鍵配送を用いた暗号通信の安全性証明の進展を概観するとともに、量子鍵配送を用いた暗号通信の意義と課題について考察する。量子鍵配送は、量子力学的な性質と既存の暗号技術を組み合わせることにより、盗聴者が無限の計算能力を有しても解読できない情報理論的安全性を保証できる。このため、公開通信路から暗号文を複製しておき、後から解読するハーベスト攻撃を始めとする任意の攻撃や盗聴に対して耐性をもたせることができる。その安全性証明にはさまざまなバリエーションがあり、1984 年に最初期の量子鍵配送プロトコル BB84 が発表されて以来、通信方式の進化や装置不完全性を悪用する実装攻撃を考慮する方向で理論が進展している。2020 年には、既存の光回線と併存しやすい連続量量子鍵配送方式（CV 方式）に対して初めて安全性証明が付与された。これらの利点がある一方で、量子鍵配送は、専用の通信装置を要するため暗号化通信網を構築するコストが高い。現時点で量子鍵配送は、複数拠点間で機密度の極めて高い情報を送受信する場合に適している。その普及に向けては、量子中継などの技術開発、通信性能の向上、通信方式の標準策定、通信装置の安全性に関する確認・認証の制度的枠組みの整備が課題である。

キーワード：量子鍵配送、連続量量子鍵配送（CV-QKD）、実装攻撃
JEL classification: L86、L96、O36

*　日本銀行金融研究所企画役（E-mail: kazutoshi.kan@boj.or.jp）
**　東京大学講師（E-mail: sasaki@qi.t.u-tokyo.ac.jp）

本稿は、日本銀行金融研究所からの委託研究論文である。本稿の作成に当たっては、玉木潔教授（富山大学）、國廣昇教授（筑波大学）、藤原幹夫氏（情報通信研究機構）および福島優氏（情報通信研究機構）から有益なコメントを頂戴した。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、日本銀行や東京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。

目　　次

１．はじめに

量子鍵配送（quantum key distribution: QKD）は、光子の状態を利用して表現される量子ビットに暗号鍵の情報を埋め込み、量子ビットが持つ量子力学的な性質によりその情報を安全に守る通信プロトコルである。現在、インターネットにおいて標準的に利用される RSA（Rivest-Shamir-Adleman）暗号や楕円曲線暗号は、理論的には、十分な性能を備えた量子コンピュータによって効率的に解読されてしまうことが知られている [1]。QKD は、量子コンピュータの脅威に対して安全な暗号技術の 1 つであり、量子力学的な性質を用いない耐量子計算機暗号（post quantum cryptography: PQC）と並ぶ重要な選択肢であるとされる。現在、世界中で QKD を用いた暗号通信の実証実験が進められている [2]。QKD を用いた暗号通信は、まず二者間で任意の乱数（鍵）を共有する QKD を実行し、その後、共有された鍵と古典暗号（ワンタイム・パッド、one-time pad）を用いて安全に任意のメッセージを送信するプロトコルである。以下では、QKD について論じる。

QKD の強みは、盗聴されていないことを保証し、情報理論的安全性（information-theoretic security）を確保できる点にある。情報理論的安全性は、攻撃者が無限の計算能力を有している場合や、物理法則で許される任意の盗聴が行われる場合にも保証される強力な性質である。将来的なコンピュータの能力向上や暗号解読アルゴリズムおよび盗聴技術の進歩の影響を受けることがないため、無期限で通信内容の秘匿性が確保できる。この性質により、理想的な量子コンピュータによる暗号解読の脅威に対しても、QKD は安全であるとされる。とりわけ、公開通信路を通過する暗号文を蓄積しておき、計算能力が向上した将来に解読を試みるハーベスト攻撃（harvest attack）[3]にも耐性がある点は、PQC にはない QKD の最大の利点である。PQC や RSA 暗号などは、計算量的安全性（computational security）に依拠しており、その安全性は攻撃者の計算能力と暗号解読アルゴリズムの効率性に依存している。このため、将来における予期せぬ計算能力の向上やアルゴリズムの進歩の脅威に対しては原理的に対処で

---

[1] RSA 暗号と楕円曲線暗号が解読困難であることは、それぞれ素因数分解問題と楕円離散対数問題の求解が効率的にできないとの仮説に依拠している。量子コンピュータは、ショアのアルゴリズムによってこれらの問題を効率的に（多項式時間で）解けることが理論的に知られている。ただし、暗号解読に利用できる量子コンピュータの要求スペックは非常に高く、実現の見通しは立っていない。

[2] 日本では東京 QKD ネットワーク（藤原［2023］）、欧州では SECOQC（Secure Communication based on Quantum Cryptography）ネットワーク、欧州連合（EU）27 か国による EuroQCI（European Quantum Communication Infrastructure）ネットワーク、中国では上海と北京を結ぶ 4,600 キロメートルの QKD ネットワーク等の実証実験が行われている。

[3] ハーベスト攻撃は、store now, decrypt later attack とも呼ばれる。

きず、ハーベスト攻撃にも安全性を確保することが難しい。

ただし、QKD プロトコルにはさまざまなバリエーションがあり、それぞれの安全性には数学的証明による裏付けがあるものの、実装方式の安全性は不透明なものも多い。実装された QKD が理論通りの安全性を達成するには、以下の 3 つの条件が必要である。

(a) 採用した通信方式とプロトコルに安全性証明が付与されていること
(b) 安全性証明で仮定する通信装置（装置モデル）が現実的であること
(c) 実装された通信装置が(a)の安全性証明における装置モデルのとおりに動作すること

条件(a)は、QKD としてさまざま通信方式やプロトコルが提案されている中、そのすべてに完全な安全性証明が付与されているとは限らないために必要となる。2021 年、既存の光通信技術との親和性が高い連続量量子鍵配送（continuous-variable quantum key distribution: CV-QKD、詳しくは 3 節（3）（ロ）を参照）と呼ばれる方式について、初めて情報理論的な安全性証明（Matsuura *et al.* [2021]）が与えられた。

条件(b)は、安全性証明が、通信装置に関する実現可能な仮定に基づくことを要請している。理論上都合のよい仮定のもとで証明された安全性が、実際の通信で保証されるとは限らない。というのも、通信装置自体の雑音によって仮定が満たされない可能性や、通信装置に攻撃者が直接働きかけることなどにより秘密の情報を盗み取る実装攻撃（implementation attack、詳細は 4 節（1）（ハ）を参照）のリスクがあるためである。このため、近年の安全性証明の理論は、通信装置が現実的に満たすことができる性質（不完全性）を考慮する方向で進展した。

条件(c)は、通信装置がセキュリティ仕様を満たすことを要請する。ユーザ企業が仕様の充足を確認することは現実的ではないため、通信装置の性能と安全性を検証し、その結果を認定する制度的枠組みを整備することが QKD の普及に向けたカギの 1 つとなる。

このように、QKD の実用化に向けた研究開発は盛んに進められているものの、上記(a)～(c)を充足しつつ十分な性能を発揮する QKD 方式の開発と実用化にはまだ時間を要すると見込まれる。また、QKD の実用化にはネットワーク構築コストも必要になる。このため、量子コンピュータの脅威への対策として具体的な検討が進められているのはもっぱら PQC であり、現在主流となっている現代暗号から PQC へ移行する機運が高まっている。米国標準技術研究所（National Institute of Standards and Technology: NIST）では PQC の標準化を進めており、候補となる暗号方式を公募のうえ、審査を行っている。NIST が公表した第 3 ラウンドの審査レポート（NIST [2022]）では、鍵共有のための公開鍵暗号（鍵カプ

セル化メカニズム、key encapsulation mechanism）の標準として CRYSTALS-KYBER を採用するとともに、第 4 ラウンドにおいて他の候補の審査を継続する旨が示された。暗号移行の動機は、理想的な量子コンピュータの登場への備えを含めて、ハーベスト攻撃による脅威への対策である。今後の動きとして、量子コンピュータの実現可能性の動向にかかわらず、より早期に、より強力な暗号に移行していくことが見込まれる。その際、PQC への移行を進めるとしても、QKD と PQC の相対的な性質の違いを理解しておくことは、QKD の導入の是非や PQC との使い分けを考慮するうえで有用である。

PQC への移行は、暗号化モジュールが組み込まれたハードウェアの更新を要する場合、10 年以上の期間を要する可能性がある。他方、QKD の導入も、ネットワークを新たに構築する必要があるため、その実用化には相応の準備期間を要すると見込まれる。このため、暗号利用の将来像について検討する場合には、早期に着手することが望ましい。とくに厳格な情報管理が求められる金融機関においても、QKD の安全性と応用可能性、実用化に向けた課題を正確に理解しておくことは、長期的な暗号利用の戦略を立てるうえで重要である。

以上を踏まえ、本稿の 2 節では、QKD の位置づけを整理する。3 節では、QKD の基礎を解説する。4 節では、QKD の安全性証明を概観する。5 節では、QKD の普及に向けた課題について考察する。

２．QKD を用いた暗号通信の位置づけ

本節（1）では、まず公開鍵暗号における量子コンピュータの脅威を解説する。次に、本節（2）および本節（3）では、PQC と QKD の原理をそれぞれ解説する。これらを踏まえて、本節（4）では、QKD の相対的な強みと弱みを整理する。

（１）公開鍵暗号と量子コンピュータの脅威

古典通信で用いられる暗号は、共通鍵暗号（symmetric key encryption）と公開鍵暗号（public key encryption）に分けられる。共通鍵暗号は、送受信者があらかじめ秘密の情報（暗号鍵）を共有していることを前提に、高速での暗号通信ができる。公開鍵暗号は、そうした前提なしに暗号通信ができるが、処理速度が遅い傾向がある。こうした両者の特長を活かし、実用的な通信では、共通鍵暗号によりデータ本体を安全に送信し、共通鍵暗号に使用する鍵は公開鍵暗号により共有する方法が主流である。

現在主流となっている公開鍵暗号は、RSA 暗号と楕円曲線暗号である。これらの暗号の安全性は、巨大な整数の素因数分解問題や楕円離散対数問題が現実的な時間では求解できないとの仮定のもとで保証されている。一般に、特定の

計算問題の求解困難性を仮定して証明される安全性を、計算量的安全性（computational security）と呼ぶ。計算量的安全性は、コンピュータの能力向上や計算問題を求解するアルゴリズムの進歩に伴って徐々に低下していくものであり、期限付きの安全性といえる。このため、実務では、暗号鍵の鍵長を長くしていく運用がとられている。計算量的安全性に依拠する暗号方式は原理的にハーベスト攻撃への対処が困難であるため、超長期にわたって秘密を保持すべき情報を送信する主体にとって、同攻撃は現実的な脅威である。とりわけ、RSA 暗号と楕円曲線暗号については、理論的には、十分な性能を備えた量子コンピュータによって効率的に解読できることが知られている。そうした量子コンピュータが登場すれば、ハーベスト攻撃により、それ以前に蓄積された暗号文も含めて解読されてしまう可能性がある。

（２）PQC との比較

本節（2）では、QKD と比較されることが多い PQC について概観する。量子コンピュータによる暗号解読の脅威への対応方法の一つは、現行の暗号を、解読をするのにより強力な計算能力を要する安全なものに変更することである。量子コンピュータに対しても安全性を確保できる暗号を、耐量子計算機暗号（PQC）と呼ぶ。

PQC の安全性は、量子コンピュータと古典コンピュータを利用しても効率的に求解できない（と信じられている）計算問題の難しさによって保証されている。これらの求解困難性は、計算量理論的には NP 困難[4]と呼ばれる難しい計算問題のクラスと関係が深い[5]。もっとも、こうした理論的な保証は、計算問題の入力データのサイズを無限に大きくしていく際の、計算量の漸近的な振舞いの解析に基づくものである。このため、PQC において実用的な鍵長やセキュリティ・パラメータに対応する有限サイズの計算問題が、現実的な時間で解けないことを保証するものではない点には注意が必要である。

---

[4] NP 困難（NP-hard）とは、直感的には、効率的な解の発見は困難だが、解の候補が与えられたときに解であるか否かを効率的に判定できるような難しい計算問題のクラスを表す。より正確には、NP 困難は、NP（non-deterministic polynomial）に属するどの問題よりも同程度以上に難しい計算問題のクラスである。NP は、非決定的多項式時間アルゴリズムによって解ける計算問題のクラスである。

[5] これらの計算問題の求解困難性は、問題のパラメータの分布に依存する。さらに、さまざまなパラメータが与えられたもとでの平均的な計算量、または、最悪ケースでの計算量のいずれを計算困難性の評価に採用するかによって、暗号の安全性評価の解釈が変化する。暗号の安全性評価では、平均計算量のほうが望ましい。NIST が公開鍵暗号の標準として採用するとした格子ベースの PQC（CRYSTALS-KYBER）は、パラメータがランダムなもとで、平均計算量に基づいて安全性証明が与えられている。

現実的な時間で暗号が解けないとの評価は、将来の暗号解読アルゴリズムの進歩やコンピュータの能力向上に関する予測に基づいている。このため、PQCも、RSA 暗号のように、時間とともに鍵長を長くするなどの運用が想定されている。もっとも、将来予測に対する不確実性は大きい。とくに、暗号解読のために十分な性能を備えた量子コンピュータについては、ひとたびそれが実現した場合の影響は甚大であるため無視はできないものの、実現する確率は極めて低く、予測困難なテール・リスクとの見方が少なくない。計算量的安全性では、こうしたリスクを完全に取り除くことは原理的に不可能である。

PQC の実証実験は進捗しているが、実装攻撃への耐性とアルゴリズムの安全性に関して十分に高い信頼を獲得するには時間を要すると考えられる。この点、RSA 暗号は、20 年を超える利用実績と実装ノウハウの蓄積から信頼性が高い。このため、RSA 暗号と PQC の両方を使って二重に暗号化するハイブリッド・モード（hybrid mode）が、IETF（Internet Engineering Task Force）において標準として検討されている。また、PQC とは複数の暗号の総称であり、その中から適切な暗号を柔軟に選択できるクリプト・アジリティ（crypto-agility）の実現も課題となっている。ハイブリッド・モードやクリプト・アジリティを巡る最近の議論については、宇根［2023a, b］および菅野［2023］を参照されたい。

PQC は、QKD とは異なり、原理的に盗聴の検知ができない。なぜならば、古典ビット [6]の場合、元の古典ビットの情報を書き換えることなく複製できるため、公開通信路上で送信される古典ビットを攻撃者が痕跡を残さずに複製できるからである。そして、当然ながら、盗聴された情報を将来的に暗号解読能力が向上してから解読するハーベスト攻撃を阻止できない。これに対して、QKD では事後的に盗聴を検知（統計的手法により有無を推定、詳しくは本節（3）を参照）できるため、盗聴が疑われる部分の情報を捨て去ることによって、盗聴リスクのない安全な鍵を共有できる。このように、攻撃者は鍵の情報を入手できないため、ハーベスト攻撃を実行できない。これは、量子力学的な性質を利用した QKD の長所であり、すべての情報を古典ビット列で表す古典暗号（PQC を含む）では達成できない。

（３）QKD の原理

量子コンピュータによる暗号解読の脅威に対するもう一つの対応策は、QKD である。QKD は、量子力学的性質を巧みに利用し、プロトコルを適切に設計することによって情報理論的安全性を達成する。本節（3）では、QKD の原理を

[6] 古典ビットとは、「0」または「1」を表現する状態である。古典ビットのみを用いて演算処理を行う装置を「古典コンピュータ」と呼ぶ。平文および暗号文が古典ビット列で表現される暗号を「古典暗号」と呼ぶ。

解説する。

QKD では、量子ビットを送信する量子通信路と、古典ビットを送信する古典通信路の 2 つの経路を利用する（図 1 参照）。量子通信路は、繊細な量子ビットを送信するために低ノイズ環境を実現しているが高コストであるため、古典ビットを量子通信路で送受信する費用対効果は悪い。そこで、効率よく確定的な情報（暗号鍵）を共有するために、通常は古典通信路もあわせて利用される。古典通信路については、攻撃者は通信内容を盗聴できるが、なりすましや通信内容の改ざんはできない、との前提が置かれる。この前提を満たすには、相手認証とメッセージ認証の機能を利用できることが必要条件となる。これらの認証方法は、QKD のプロトコル全体の安全性を評価するうえで重要な論点であるが、ここでは安全な認証が可能であると仮定する。認証に関する論点については、5 節（2）で詳しく説明する。

量子ビットは、「0」と「1」の両方の状態を同時にとることができる。こうした状態を重ね合わせ状態（superposition）という。また、任意の未知の量子ビットの状態は複製できない。これは、複製不可能定理（no cloning theorem）と呼ばれる量子力学において導かれる数学的帰結であり、古典ビットにはない重要な性質である。換言すれば、量子ビットの情報は、その状態に一切の影響を与えずに読み出すことが不可能である。

量子ビットから情報を読み出す際には、測定（measurement）と呼ばれる行為を行う。一般に観測者は、未知の量子ビットの状態の情報を完全に知ることはできず、測定を通じて確率的に一部の情報を得るだけである。ただし、量子ビットが複数の既知の状態のいずれかである（がいずれかは分からない）という状況に限定すれば、測定方法によっては確定的に状態を特定できる場合がある[7, 8]。

例えば、観測者がある量子ビットについて「0」と「1」を区別するための測定を行う状況を考える。測定される量子ビットが「0」または「1」の状態であった場合には、「0」と「1」を確実に特定できる。測定される量子ビットがそれら以外の重ね合わせ状態の場合には、重ね合わせの度合いに応じた確率で「0」または「1」との測定結果を得られるが、量子ビットの状態を確定的には特定できない。

QKD は、こうした限定的な測定結果と量子ビットの性質を通信プロトコルに

---

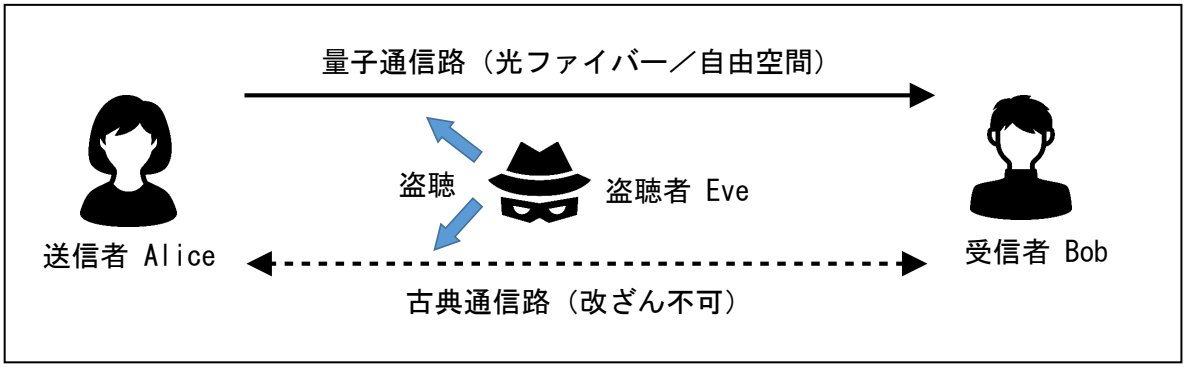
[7] 既知の状態が互いに直交している場合（直交状態の場合）には、確定的に特定できる。量子状態の測定では、観測者が区別したい量子状態に応じて適切な測定方法（観測の基底）を選択する必要がある。量子状態の直交と基底選択の詳細については、本稿では割愛する。詳しくは、Nielsen and Chuang [2010]などの量子計算の基本書を参照されたい。

[8] QKD は、盗聴を防止するために直交状態を利用しない。

応用し、盗聴の有無を事後的に推定し、盗聴が疑われる量子ビットの情報を捨て去ることにより、安全に乱数列を共有するプロトコルである。ただし、送信する量子ビットのうち、どの部分が盗聴されるかは事前にはわからないため、QKD でメッセージの暗号文を直接送信することはできない。これが、QKD で共有できる情報が、あくまで乱数列に限られる理由である。また、盗聴の影響と、環境によるノイズの影響を区別することはできないため、実際に盗聴があったと断定することもできない。盗聴は量子ビットから情報を抜き出す行為であるため、量子ビットの状態を変化させてしまう。送受信者は、巧みに設計された QKD プロトコルに従うことにより、（環境のノイズや盗聴など何らかの理由による）量子状態の変化をとらえることはできるが、そうした変化の原因を特定することまではできない。したがって、QKD の安全性解析では、量子状態のあらゆる変化はすべて盗聴によるものであるとみなすことで、変化の原因いかんにかかわらず安全であることを証明する枠組みとなっている。

乱数列が安全に共有された状態で、情報理論的に安全な古典暗号であるワンタイム・パッドを組み合わせると、任意のメッセージを安全に共有できる。このときのメッセージの長さが、共有された乱数列と同じ長さであれば、メッセージは情報理論的安全性を確保できる[9]。

図 1 QKD の概略図



（4）QKD の位置づけ

QKD は、量子コンピュータによる暗号解読への対応策との観点から PQC と比較されることが多い。実際、5 節（1）で紹介する通り、各国のホワイト・ペーパーやポジション・ペーパーをみても、そうした観点からの比較に基づいて、

[9] 例えば、安全に共有された乱数列を$x = 010111$、送信したいメッセージを$y = 111000$とする。ワンタイム・パッドによる暗号文は、各ビットの排他的論理和$z = x \oplus y = 101111$で定められる。このとき、乱数列xの情報が攻撃者に全く知られていないとき、暗号文zからメッセージyの情報は全く漏洩しないこと（情報理論的安全性）が保証される。

QKD に対して否定的な評価を与えている。もっとも、そうした評価は、インターネットにおいて広く利用されている汎用途の暗号技術としての評価である点には注意を要する。以下では、QKD と、それ以外の鍵共有手法として、現代暗号（RSA 暗号、楕円曲線暗号）、PQC、信頼できる人による乱数の直接運搬（Trusted Courier）を比較する。

後段の表のとおり、現時点の技術水準では、QKD と最も応用例が近い比較対象は、人手による運搬（Trusted Courier、以下では Trusted Courier と呼ぶ）である。Trusted Courier は、基本的には一対一での通信に適している。多数の拠点に乱数を運搬できれば一対多の通信手段としても活用できるが、多対多の通信手段には不向きである。これは、事前に行う鍵（乱数列）の輸送に時間を要するほか、一定期間に通信するメッセージの総量と同じ長さの鍵を安全に管理する負担が生じるためである。これに対して、QKD は、通信経路が確保されていれば、多対多の拠点間通信に相対的に適しており、通信の都度、高速で鍵を共有することができる。

前述のとおり、QKD の最大のメリットは情報理論的安全性である。QKD は、秘匿性を守る期間が超長期に及ぶ場合や、機密度が極めて高い情報を取り扱う場合において、（多対多でも）限られた拠点間での通信に向いている。例えば、生命保険会社が取り扱う遺伝子情報や、金融機関が取り扱う一部の信用情報がこれに該当しうる。ただし、送信者の建物と受信者の建物の間の基幹線のみを QKD で守る場合には、受信者側では、QKD の受信装置から各利用者の端末までの間（last one mile）の通信内容について、別途の手段で秘匿する必要が生じるケースも想定される。また、量子中継（quantum relay）[10]の技術が確立していない現状では、現在の中継装置を信頼する必要がある。

他方、10 年程度で機密解除できる程度の情報であれば、PQC がコスト面で適していると考えられるし、金融機関のワンタイム・パスワード生成器などによって共有した乱数列の安全性を何らかの理由で信頼する場合にも、QKD の優位性は下がる。また、QKD は、通信相手の真正性を確認する相手認証を提供しないため、こうした認証手段は別途必要になる。この点については、5 節（2）で考察する。このように、QKD と PQC では、安全性、用途、前提条件などが大きく異なるため、適切な使い分けが重要である。

[10] 量子中継は、中継装置が量子ビットを受信し、次の中継装置に転送する間に、古典ビットへの変換を行わない中継方式を表す。

表 QKD と他の鍵共有手法の比較

	RSA暗号、楕円曲線暗号 （RSA、ECC）	耐量子計算機暗号 （PQC）	量子鍵配送 （QKD）	人手による運搬 （Trusted Courier）
手法	公開鍵暗号	公開鍵暗号	量子暗号通信	人間による直接配送
安全性	計算量的安全性	計算量的安全性	情報理論的安全性	—
安全性の原理	素因数分解問題等の 求解困難性	NP困難問題の 求解困難性(注1)	量子力学的性質 （物理法則）	運搬手段の秘匿性と信頼性
量子コンピュータへの耐性	×	△	○	○
盗聴検知	×	×	○	×（ただし、運搬中の情報の窃取は困難）
サイド・チャネル攻撃への耐性	信頼性が高い	十分ではないためハイブリッド方式が推奨される	対策は考慮されているが検証枠組みは未整備	信頼性が高い
専用装置	不要	不要	DV-QKDは既存の光通信との回路共有が困難 CV-QKDは既存の光通信との回線共有が容易	不要
通信形態	多対多	多対多	多対多	1対多
保護の範囲	End-to-End	End-to-End	通信装置間のみ 中継装置も要保護(注2)	End-to-End
相手認証	○	○	PQCによる認証の場合は、認証部分のみ計算量的安全性に基づく Wegman-Carter認証では少量の乱数の事前共有が必要	運搬者の本人確認

備考：（注1）PQCは複数の暗号アルゴリズムがあり、安全性の根拠となる計算問題もこれに応じて複数ある。

（注2）量子中継が実現された場合には、中継装置内部での盗聴を検出できるため、中継装置に要求される保護の強度は下がる。

３． QKD の基礎

（１）量子ビットの光への埋め込み

QKD では、量子ビットの情報を運ぶ媒体として、常温でも安定しており最速で移動できる光が利用される。量子ビットの例として、偏光（polarization）と呼ばれる光の状態を利用するものがある。光は電磁波の一種であり、自然状態では電場や磁場がさまざまな方向に振動しているが、偏光フィルタを通過させて、特定の方向のみに振動する光を抽出したものを偏光と呼ぶ。この振動の方向（角度）に送信したいデジタルな情報を埋め込む [11]が、偏光には、振動の方

[11] 古典通信の場合には、光の点滅によってビットの「0」と「1」に対応させて、送信したい情報を表現する。

向が一定の直線偏光（典型例は、0 度、45 度、90 度、135 度の 4 状態）のほかにも、光の進行に伴い振動の方向が回転する円偏光（右回り、左回り）もあり、こちらを用いることもある。また、偏光の替わりに、位相差の制御された 2 つの光パルスを用いることもある。これらのいずれを用いて量子ビットを実現しても、理論的には等価である。

単一光子を量子ビットとして扱うQKDプロトコルは、安全性の理論的証明が容易である一方、実装上は、単一光子の生成を完全に制御することは難しい。このため、実用上は、エネルギーを 1 光子レベルに落とした微弱な光パルス（短時間のレーザー光）を用いるのが一般的である。

（２）QKD の通信路と中継装置

量子通信路は、地上間通信であれば光ファイバー・ケーブル、衛星地上間通信であれば大気となる。この点、通常の古典光通信や衛星通信と同様である。ただし、量子通信の場合、光信号の強度が極めて弱いため、通信路において許容されるノイズは極めて小さい。QKD の実現方式によっては、1 光子レベルの信号を取り扱うことになるため、ノイズが大きくなる長距離通信での実現は困難となる。このため、一定間隔で信頼できる中継地点（trusted node、または、trusted point）を設ける必要がある。

一般的に、中継地点の間隔を長くとるほど、ネットワーク構築のコストは低下する反面、通信路による光の減衰の影響を受けて暗号鍵の生成速度が低下する。執筆時点（2024 年 2 月）では、最も典型的な QKD の実現方式であるデコイ BB84 方式[12]（Hwang [2003]、Lo, Ma, and Chen [2005]、Wang [2005]）では、光ファイバーの通信距離が 50 キロメートル伸びるごとに、鍵生成の速度が 10 分の 1 に低下している。50 キロメートルの通信速度は高々1 秒当たり 1 メガビット程度であるため、鍵生成に求める速度に応じて中継地点の距離が制約を受けることとなる。

中継の方法には、古典中継と量子中継がある。

- 古典中継では、各中継装置において、量子ビットの情報を読み出して古典ビットに変換してから、再び量子ビットを作成して次の中継装置に送信する。各中継装置の内部にある古典ビットの情報が漏出しないように、中継装置を厳重に保護する必要がある。

[12] BB84 方式については、本節（4）を参照されたい。デコイ BB84 方式は、BB84 方式において単一光子の代わりに安価で扱いが容易な微弱なレーザー光（光パルス）を用いる方式。送信者は、事前に数種類の中からレーザー光の強度をランダムに選択し、その強度のレーザー光を送信することにより、単一光子を使った方式と同等の性能を確保できる。

- 量子中継は、実質的には、通信路による光の減衰の影響を除去する方法である。この方法は、古典ビットへの変換がないため、中継装置の厳重な保護は不要となる。もっとも、実用的な量子中継の技術は現時点で確立していない。

（３）QKD 方式の分類

QKD の実証実験や商用化において、最も典型的に用いられるのはデコイ BB84 方式であるが、それ以外にもさまざまな通信方式が提案されている。これらは、送受信方式、光検出器、通信装置の信頼性に応じて分類される。

（イ）送受信方式による分類

2 者間での送受信方式に応じて、QKD プロトコルは以下の 3 つに分類できる。

- Prepare-and-Measure（PM）方式：一方が光を送信し、他方が光を測定する方式。具体例は、BB84 方式やデコイ BB84 方式である。
- Measurement-Device-Independent（MDI）方式（Lo, Curty, and Qi [2012]）：双方が光を送信し、中間地点にある観測装置がそれらの光を干渉させたうえで測定し、その結果を公開する方式。具体例は、ツイン・フィールド（Twin-Field）方式（Lucamarini *et al.* [2018]）である。
- Entanglement-Based（EB）方式：中間地点にある通信装置が、相関をもった光の対（量子もつれ[13]光子対）を生成して送信者と受信者に片方ずつを送り、それぞれが受け取った光を測定する方式。具体例は、BBM92 方式 (Bennett, Brassard, and Mermin [1992])や E91 方式（Ekert [1991]）である。

それぞれの特徴について述べると、PM 方式は最も単純な方式であり、既に製品として売られているものが多い。

MDI 方式では、通信路の中間地点に観測装置を置く必要がある。この方式の利点は、この観測装置が仮に盗聴者の完全な制御下に置かれているような場合であっても盗聴行為をエラーとして検知可能であり、仮に中間地点の測定結果を信頼できなくてもプロトコルの安全性が保証されることである。また、具体的なプロトコルにもよるが、PM 方式と比較して、距離による性能低下の影響を半減（換言すれば、同程度の性能低下をもたらす通信距離を 2 倍に）できる。

さらに、MDI 方式では、正規の通信者は 2 者とも送信装置を用いていること

[13] 量子もつれ（quantum entanglement）の関係にある粒子の観測結果は、どれだけ離れていても互いに相関を持つ。量子もつれは、量子コンピューティングにおいて重要な量子力学的性質であるが、QKD では必須ではない。

から、一般に受信装置に対する攻撃が多いとされる実装攻撃に対しても頑健といえる。この点、一般に受信装置は、盗聴者の影響を受ける通信路からの信号を受け入れる必要があるため、送信装置よりも実装攻撃のリスクが高いと考えられている。実装攻撃については、4節を参照されたい。

EB方式では、量子もつれ光子対を発生する特殊な光源が必要となることから、他の方式と比べてコストや手間がかかる傾向にあり、通常は利用されない。しかし、必要とされる乱数生成器を削減できるといった利点がある。また、特定の光ファイバーを選択する必要はあるが、周波数多重化通信をする場合において有用との見方もある（Wengerowsky, *et al.* [2018]）。

（ロ）光検出器による分類とCV-QKDの優位性

QKDプロトコルは、光検出器に応じて、DV-QKD方式とCV-QKD方式の2つに分類できる。DV、CVという名前は、もともとは送受信する情報が離散量であるか、連続量であるかという違いに由来した。もっとも、今日では、CV-QKD方式でも離散量の情報を送信する場合があることから、DV、CVという接頭語は、単純に使用する検出器の違いを表すものとなった。

- Discrete-Variable（DV）方式：光子検出器を使用する方式であり、単一光子の有無を検出する。例えば、偏光フィルタ（または、偏光ビーム・スプリッター）の後ろに光子検出器を配置することで、偏光の角度がわかる。これまでに述べてきたQKDプロトコルは、すべてこちらの方式に該当する。
- Continuous-Variable（CV）方式：光検出器を使用する方式であり、ホモダイン検出またはヘテロダイン（デュアル・ホモダイン）検出[14]により光の振幅を観測する。送信者は、光の振幅に情報をエンコードしている。歴史的にはGG02方式（Grosshans *et al.* [2003]）が有名だが、近年の方式は、特定の名前を冠していないものが多い。

光子検出器は、単一光子という極めて微弱な光の有無を検出する装置である。実際に使われる光子検出器では、0光子か1光子以上かを判別する。この検出をon-off光子検出と呼ぶ。単一光子の性質を利用するDV-QKD方式は、量子状態を簡素に記述できることから、安全性証明を与えやすい。他方、これと近い周

[14] 微弱な光信号を測定するための検出技術である。周波数の異なる雑音光の影響を受けにくいという特長がある。ホモダイン検出では、測定対象の光が参照光と合波されて増幅されたのちに、検出器により電気信号に変換される。この際、測定対象の光と参照光は同一周波数である必要がある。ヘテロダイン（デュアル・ホモダイン）検出は、入力光を2つに分配して、4分の1波長分だけ異なる位相にした参照光でそれぞれホモダイン検出する方式である。

波数で行われる古典通信において使用する強い光の影響をうけやすいという留意点があるほか、光子検出器が高価であることから安価に DV-QKD を実装するのは現状困難である。

光検出器は、光の強度を検出する装置であるが、単一光子ほどの微弱な光は検出できない。このため、ホモダイン検出およびヘテロダイン検出では、単一光子レベルの微弱な光を、レーザー光と干渉させて実質的な増幅を行ってから光検出器で測定する。CV 方式は安価な光検出器により実装できる方式であるため、DV 方式と比較してコスト面で優位性がある。

CV 方式のもう一つの利点は、古典通信と光ファイバー網を共有できる点である。一般に、光通信では、波長の異なる光パルスに独立に信号をのせることにより、一本の光ファイバー通信を多重化し、通信容量を増大できる。こうした通信技術を波長多重と呼ぶ。とくに、CV 方式で用いる光の測定方式は、狙った波長の光だけを選択的に取り出す波長フィルタとして高い性能（モード選択性）をもっているため、異なる波長の光信号の影響を受けにくい。このため、CV-QKD は、DV-QKD と比較して頑健であるといえる。この波長多重を応用して、CV-QKD に専用の波長を割り充てることで既存の光通信と併存させられれば、光ファイバー網を新たに敷設する必要はなくなる。

Pirandola *et al.* [2017]によれば、CV 方式は、理論と実装技術を発展させていくことができれば、通信速度の面でも DV 方式よりも高性能となりうると考えられている。ただし、CV 方式では、安全性証明の付与が容易ではなく、現実的に実装可能な離散変調の CV 方式に初めて安全性証明が与えられたのは Matsuura *et al.* [2021]である。執筆時点（2024 年 2 月）において安全性証明が付与された CV-QKD プロトコルをみると、いずれも DV 方式と比較して通信性能が劣っている。このため、今後の CV 方式の性能向上は、プロトコル、通信装置の実装、安全性証明の理論に関する研究の進展にかかっているといえる。

（ハ）装置の信頼性による分類

通信装置の性質に関する想定に応じた分類もある。この前提の違いを映じて、QKD の安全性証明と通信プロトコルが異なるものとなる。

- デバイス・ディペンデント（Device-Dependent）方式：通信装置が想定する装置モデル通りに動作すると仮定して、安全性を保証する方式。上述の QKD プロトコルは、すべてこの方式に該当する。
- デバイス・インディペンデント（Device-Independent）方式：通信装置について、送受信者に宛てた出力を盗聴者には出力しない、真正乱数を使用できる、内部に記憶装置を持たない（Barrett Colbeck, and Kent [2013]）ことの

みを仮定して、安全性を保証する方式。具体例として、E91 方式がある。

Device-Independent 方式は、通信装置に特定の装置モデルを仮定せずに、安全性を証明する方式である。安全性証明に利用できる前提が少ないため、QKD プロトコルの開発とそれへの安全性証明の付与は困難である。また、特定の装置モデルを仮定しないことから、Device-Independent 方式では、通信装置の性質を検証する際の検査項目数は、Device-Dependent 方式に比べて少ない。

なお、Device-Independent 方式と Device-Dependent 方式の差異をみるうえで、以下の 2 点に留意する必要がある。第 1 に、Device-Independent 方式では、装置モデルを仮定しないことから、通信装置の検証が不要であると誤解されることがあるが、実際には、理論に関する基本的な仮定を通信装置が満たすことを検証する必要がある。そこでの仮定は、特定の装置モデルに関するものではなく、ベル実験が要請するような量子力学的にみて普遍的かつ基礎的なものである。第 2 に、装置モデルで仮定される「送受信者に宛てた出力を盗聴者には出力しない」という性質の確認については、実装攻撃への対策を考慮する際には両方式の間で大差はない。以上から、両方式の本質的な差異については議論の余地があるといえる。

もっとも、性能面についていえば、量子状態を記憶する量子メモリといった高度な素子を使わない場合には、Device-Independent 方式は Device-Dependent 方式と比べて性能が極端に低くなるというデメリットがある。また、量子状態の長期間の保持は技術的に困難であるため、Device-Independent 方式の実用化には 20 年以上の歳月を要するとの見方もある。このため、以下では特段の断りがない限り Device-Dependent 方式を前提とする。

（４）プロトコルの基本構造

代表的な QKD プロトコルは、BB84 方式（Bennett and Brassard [1984]）である。Charles Bennett と Gilles Brassard が 1984 年に発表した本方式は、提案者の頭文字と提案年にちなんで BB84 と呼ばれている。現在、さまざまな国で実証実験が行われている QKD の多くは、BB84 方式を採用している。このプロトコルの詳細については、すでに優れた解説が世に出ているため、例えば小芦・小柴［2008］や後藤［2009］、Nielsen and Chuang [2010] などを参照されたい。

本節（4）では、抽象化した QKD プロトコルの概略を述べる（図 2 参照）。BB84 方式を始めとするほとんどの QKD プロトコルは、大まかには以下の 3 つのステップにより実行される。すなわち、第 1 ステップで不完全な乱数列（ふるい鍵、sifted key）を共有したあと、第 2 ステップと第 3 ステップにおいて、このふるい鍵から安全な部分を抜き出し、最終的な暗号鍵を得る。それぞれの

ステップを詳述すると以下のとおりである。

第 1 ステップでは、まず、量子通信路と古典通信路を使って乱数列を共有したり量子通信路の状況を監視したりする。例えば、PM 方式では、送信者が量子通信路を通じて量子ビット列を送信し、受信者が量子ビットを測定する。この際、送信する状態の種類や測定の方法（観測の基底、脚注 7 参照）を確率的に切り替えることで、乱数列の共有や量子通信路の監視を行っている。これらの切り替えの選択は、量子通信路の使用が終わったあと、古典通信路を用いて送受信者で共有される。このステップで共有された乱数列は、ノイズなど[15]の影響から送受信者で完全には一致しておらず、部分的に盗聴されている可能性もある。この乱数列をふるい鍵と呼ぶ。

第 2 ステップは、誤り訂正（error correction）である。ふるい鍵の一部の情報（誤り訂正符号におけるシンドローム）を古典通信路[16]で通信することにより、送受信者間で一致していない部分を明らかにし、片方の鍵を修正する。この手続きは、ノイズのある古典通信における誤り訂正と同様の手続きである。この不一致の割合をエラー率と呼ぶ。最終的に得られる暗号鍵は、エラー率が低いほど長くなる。

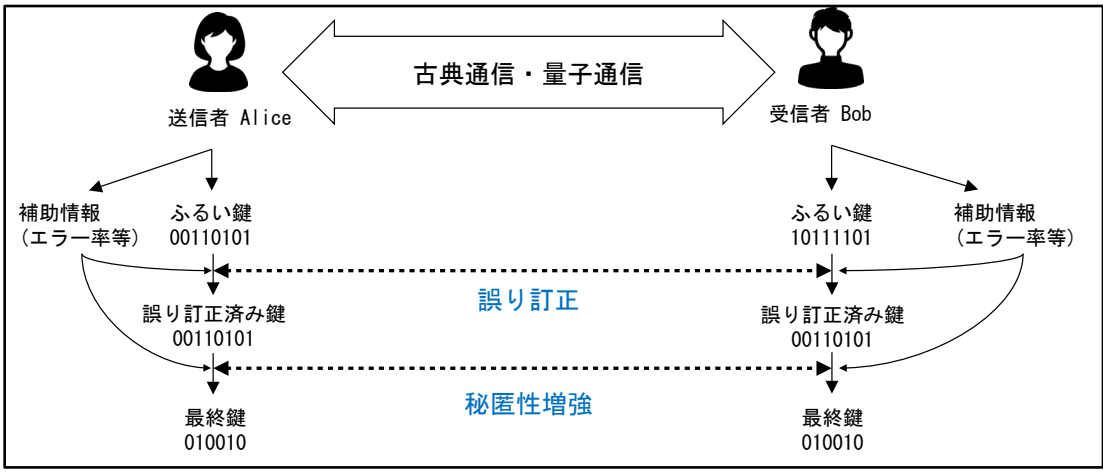
第 3 ステップは、秘匿性増強（privacy amplification）である。公開通信路で鍵とは独立な乱数列を共有し、所定のアルゴリズムに従って鍵を短くすることで、部分的に情報が漏洩している可能性のある鍵を全く情報が漏れていない安全な鍵に補正する。漏洩が疑われる情報が多いほど、鍵をより短く補正する必要がある。これらの結果として、非常に高い確率で安全で一致した鍵が共有できる。

---

15 例えば、通信路のノイズ、盗聴者による盗聴、測定結果の量子力学的なゆらぎなど。

16 プロトコルによっては、事前共有鍵を使用して暗号化し、この情報を送る必要がある。その場合に最終的に生成される鍵からこのステップで使用した鍵を差し引いた正味の鍵生成量がプロトコルの鍵生成量とされる。

図 2 QKD プロトコルの概略図



４．QKD の理論的安全性

（１）QKD の安全性基準と安全性証明の前提条件

QKD の安全性証明の構成要素は、証明すべき安全性に関する基準、通信装置の性質を数学的に表現した装置モデルなどの前提条件、および QKD プロトコルである。

（イ）安全性に関する基準

証明の目標である安全性に関する基準は、暗号学の概念である情報理論的安全性である。すなわち、現実のプロトコルP_{real}により共有された鍵が、理想的なプロトコルP_{ideal}（通信路でのノイズや盗聴がなく、完全な秘匿性を達成するもの）により共有された鍵との識別が困難であることをもって、そのプロトコルは安全であるとする [17]。この識別不可能性は、ϵ–識別不可能性（ϵ–indistinguishablility）と呼ばれ、次のように定義される。

ある正の定数ϵに対して、現実のプロトコルP_{real}と理想的なプロトコルP_{ideal}がϵ–識別不可能であるとは、任意の識別者（distinguisher）に対して

$$\Pr[B = 1|P_{\mathrm{real}}] - \Pr[B = 1|P_{\mathrm{ideal}}] \leq \epsilon$$

が成り立つことである。ここでいう識別者とは、現実のプロトコルと理想的なプロトコルを見分けようとする仮想的な主体であり、判定結果に応じて推定値Bを出力するものである。識別者は、理想的なプロトコルであると判定したときには$B = 1$と回答し、現実のプロトコルと判定した場合には$B = 0$と回答する。プロトコルPのもとで推定値Bを得る確率は$\Pr[B|P]$と表現される。このϵ–識別

[17] この安全性基準は、理想的な状況と実際の状況とのトレース距離の近さを保証する。

不可能性が任意の識別者に対して成立することが、任意の盗聴に対する安全性、すなわち情報理論的安全性を保証する理由となっている。

また、共有された鍵がこうした性質を満たすプロトコルは、ϵ–安全（ϵ–secure）であるという。QKD のユーザが任意の値に設定できる正の定数ϵは、直感的には、理想的なプロトコルによる通信とは異なる結果を得る確率の最大値と捉えることができる。

（ロ）安全性証明の前提条件

QKD の情報理論的安全性（または、無条件[18]安全性）という数学的性質の証明は、以下に掲げるさまざまな前提条件（仮定）に基づいて証明される。これらの仮定は、送受信者と盗聴者の能力、装置のモデル化、QKD プロトコルに関するものである。

(a) 攻撃者は、量子通信路において、遮断や盗聴などのあらゆる攻撃ができる
(b) 攻撃者は、古典通信路において、盗聴はできるが、なりすましと改ざんはできない
(c) 送信者と受信者は、それぞれ乱数を生成できる
(d) 通信装置は、装置モデルの通りに動作する
(e) 盗聴者は、通信装置の内部に直接的にはアクセスできない

仮定(a)では、盗聴者がすべての量子ビットを観測して通信を妨害する DoS（ドス、denial of service）攻撃や回線の切断といった極端な攻撃をも想定する。このような場合、得られる鍵長は 0 になる。このように、QKD では安全性は常に保証されるが、鍵が常に生成できることは保証されない。

仮定(b)は、相手認証とメッセージの認証が安全に行えることを意味する。古典通信においては認証技術が確立されているものの、利用する認証技術の安全性が QKD プロトコル全体の安全性評価に含まれる点には注意が必要である（5 節（2）を参照）。

仮定(c)では、送信者と受信者が安全な物理乱数生成器をもっているという状況を想定している。安全であれば、量子乱数と（古典の）疑似乱数のいずれでもよいが、それぞれでリスク特性は異なる。例えば、疑似乱数の場合には、乱数生成器へのバックドア攻撃のリスクがあるほか、原理的に乱数を推定されるリスクが残る。他方、量子乱数の生成器はバックドア攻撃のリスクは低いと考

[18] この無条件とは、量子通信路に対する条件をつけていないという限定的な意味である。

えられるが、別のアプローチに基づく攻撃のリスクはある[19]。

仮定(d)の装置モデルは、通信装置を数学的対象として抽象化したものであり、量子力学の枠組みで記述される。

仮定(e)では、通信装置の内部に格納された古典ビットの乱数列を直接的には窃取できないと仮定している。この仮定では、攻撃者による遠隔からの窃取の可能性を排除はしていないが、実装攻撃の考慮の仕方は後述の装置モデルの仮定に依存している。こうした仮定のもとで、QKD プロトコルの安全性が証明される。

（ハ）安全性証明の前提条件と実装攻撃の脅威の関係

QKD の安全性は、通信装置が装置モデルの通りに動作するとの前提に基づいて証明される。しかし、現実の通信装置と装置モデルの性質に乖離がある場合には、攻撃者が現実の通信装置に何らかの干渉を行い、通信内容の盗聴や改ざん等を行いうるとのリスクがある。このリスクは、QKD に対して、実装攻撃による重大な脅威をもたらす。

実装攻撃とは、暗号プロトコルのデザインの欠陥や暗号学的な脆弱性を突く方法以外の方法で暗号解読を試みる、あらゆる攻撃の総称である[20]。QKD では、装置モデルの仮定を破るような攻撃は、実装攻撃とみなせる。実装攻撃に対しては、数学的証明による安全性の保証は無効である。

QKD において、実装攻撃に悪用されうるリスクの例を挙げる。例えば、受信側の素子に非常に強い光をあてると光子検出器が故障し、一定の光強度以下の光には反応しなくなる。この現象を悪用することで、攻撃者が意図した観測の基底のみで受信装置の信号の受信が起こるようにし、盗聴しているにもかかわらず、その影響がエラーとして検知されないようにできる攻撃がある。この攻

---

[19] 例えば、乱数生成器から出力された乱数を、何らかの方法で複製する攻撃のリスクは考慮する必要がある。

[20] 実装攻撃の詳細については、例えば、鈴木・菅原・鈴木［2015］を参照されたい。古典暗号では、実装攻撃は、装置内部に直接的にアクセスする侵襲攻撃（invasive attack）と、そうしたアクセスを行わない非侵襲攻撃（non-invasive attack）に分類される。さらに、非侵襲攻撃は、装置の通常の動作を受動的に観測するサイド・チャネル攻撃（side-channel attack）と、能動的に装置にエラーを引き起こし、異常動作を観測する故障利用攻撃（fault-injection attack）に分けられる。サイド・チャネル攻撃の例として、暗号化または復号にかかる情報処理中に、演算装置から漏れる電磁波や演算装置の消費電力を観測することで平文に関する情報を得るなどの攻撃方法が考案されている。

QKD の場合には、上記のような古典暗号における実装攻撃の分類が確立しているとは言い難い。また、実装攻撃をサイド・チャネル攻撃と呼んでいるとみられるケースもあるため、用語の用法には注意されたい。

撃だけを考慮するのであれば、3 節（3）（イ）で述べた MDI 方式を使うことや、受信装置に入射する光の強度を調べることで、攻撃の検出は可能である。

これに対して、未知の実装攻撃に予め対処することは一般に困難である。このため、実装攻撃への対処は、既知の攻撃手段への対策を講じることが中心となる。QKD についても、40 年近い歴史の中の最近の 20 年間で、現実の通信装置に即した装置モデルや実装攻撃への対策に関する知見が蓄積されつつある。

対策についていえば、理論面では、実装攻撃のリスクの源泉となる装置の不完全性を仮定に含めてプロトコル（特に秘匿性増強の量）を再設計し、安全性証明を与えることにより、リスクを無効化する研究が進展してきた。

通信装置については、通信装置が装置モデルに従って動作しているか否かについて、理論とは別に、実機を使った検証を行うべきであり、今後、装置に関する標準の策定や、検証と認証の制度的枠組みの整備が必要となる。この点については、5 節（3）を参照されたい。

なお、QKD においても、末端の通信装置で情報を古典ビットに変換したあとは、通常の古典暗号化通信と同様の実装攻撃への対策が求められる。

（２）QKD の安全性証明の進展

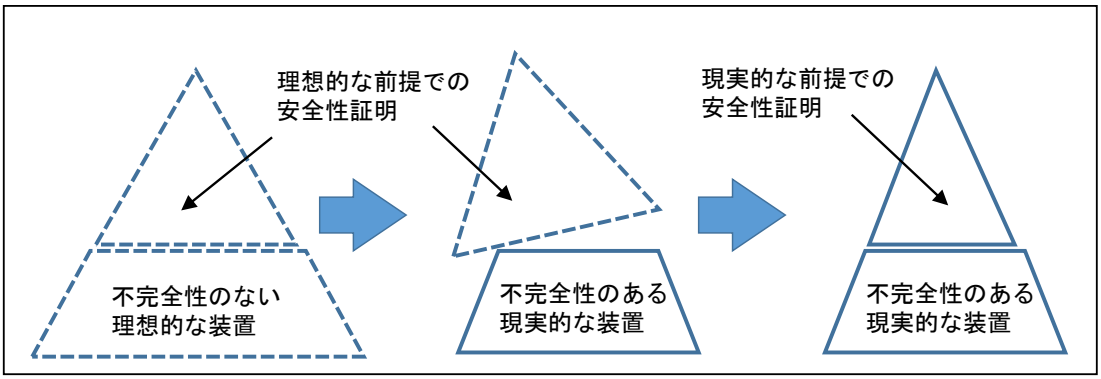
本節（2）では、QKD の安全性基準と装置不完全性に関する研究の変遷を概観する。

QKD の安全性証明の理論は、BB84 方式の提案以来、現在に至るまで進展が続いている。通常、QKD の安全性証明では、まず証明に都合のよい理想的な前提条件から出発して安全性を証明することを目指す。そうした過程で、QKD プロトコルの安全性基準に関する研究が発展した。

しかし、大抵の場合において、実際に利用可能な装置に対して要求できる前提条件と、安全性証明で用いた前提条件にはギャップがあるという課題があった。そこで、実装攻撃を想定し、装置不完全性を取り込んだ前提条件から QKD の性能を保ちつつ安全性を示せるように証明を改良する研究が進展した（図 3）。

前者の安全性基準に関する研究について次の（イ）、後者の装置不完全性を取り込む研究について（ロ）で解説する。

図 3 装置不完全性と安全性証明



（イ）安全性基準に関する研究の進展

最初に提案された QKD プロトコルは、BB84 方式である。この方式では、送信者は理想的な単一光子を生成し、その偏光状態を 4 種類（0 度、45 度、90 度、135 度）のうち 1 つに設定し、受信者に送る。受信者は光子検出器を用いて、単一光子の偏光状態を測定する。原論文（Bennett and Brassard [1984]）は、ノイズのない通信路などの極端に理想的な状況を仮定したもとで、プロトコルは情報理論的に安全であると主張した。しかし、こうした主張に対して、実際の通信路にはノイズが存在するので、安全性証明は不完全であると批判された。

こうした批判を受けて、Mayers [1996]は、ノイズのある通信路や不完全な観測装置を前提として、BB84 方式の安全性証明を拡張した。この研究により、QKD は情報理論的安全性を達成できるとの認識が研究者の間で広がったが、この証明で採用された安全性基準は、本質的には相互情報量（mutual information）[21]という尺度に基づくものであった。

その後、相互情報量を用いた安全性基準では基準として不十分であることが Müller-Quade and Renner [2009]によって指摘された。この指摘を受けて、情報理論的な安全性基準としてϵ-安全（ϵ–security、定義は本節（1）（イ）を参照）を採用するべきであるとの認識が研究者の間で広がった。今日では、ϵ–安全が安全性基準の標準となっている [22]。

---

[21] 相互情報量とは、2 つの確率変数の依存度の高さを表す指標であり、一方の確率変数から得られる他方の確率変数の情報量と解釈することができる。QKD プロトコルを実行する量子情報処理系の情報（何らかの確率変数の値）から得られる秘密鍵の情報が少なければ、プロトコルが直感的には安全であると考えることもできる。こうした直感にもとづいて、相互情報量に基づく安全性基準が作られたが、直感に反して安全であるとは限らないことが反証によって示された。

[22] ϵ –安全に基づく安全性証明のアプローチについては、補論を参照されたい。

（ロ）装置不完全性を取り込む研究の進展

ϵ–安全が保証されていても、その保証の前提条件によって安全性の意味は大きく変わる。特に、装置モデルについては、装置モデルが要求する性質を持つ装置の調達困難性や、装置に生じる損失やノイズの程度、性能指標の正確性やその保証方法の考慮の有無など、注意を払うべき点が多い。

それらのうち、まず BB84 方式における光源の問題を取り上げる。BB84 方式では、もともと単一光子を生成する光源が使えることを仮定して安全性が証明されていた。しかし、理想的な単一光子光源の実現は容易ではない。このため、実際の実験では、平均光強度を 1 光子レベルにまで低く抑えたレーザー光源が利用されている。もっとも、レーザー光源は、一定の確率で 2 光子以上を放出することから、そもそも安全性証明の前提が崩れているという問題がある。しかも、こうした前提の崩れを悪用した攻撃も想定できる。例えば、同一の量子状態をもつ光子が 2 個以上放出された場合において、盗聴者は、生成された光子のうち 1 つを盗聴用に確保し、受信者に残りの光子を送るとする。この場合、受信者に送られた光子に盗聴者は触れていないため、一切の痕跡を残さずに盗聴ができてしまう。このため、いかに解析を工夫しても BB84 方式では、2 光子以上を生成した場合の信号からは、安全な鍵は得られない。

さらに、上記の議論では、レーザー光が 1 光子または 2 光子以上の状態が確率的に出現する状況を想定していたが、実際のレーザー光はそれらの重ね合わせ状態である。その性質を用いて効率的な盗聴を行う実装攻撃のリスクが考えられる。こうしたリスクへの対策として、レーザー発振の不安定性や位相変調器を利用して、レーザー光の位相をランダム化する処理が考案された。この処理を行ったレーザー光は、各光子数に対応する状態を確率的にとるもの（古典状態の確率混合）と同等となることから、もはや重ね合わせ状態の性質を利用した攻撃ができなくなることや、このケースでの安全性証明の方法論が Gottesman *et al.* [2004]によって示された。ただし、この手法では、理想的な単一光子光源を使用する場合と比較して、長距離通信での性能が大きく低下するという問題があった。

そこで、そうした通信性能の低下を改善する手法として、デコイ法（Hwang [2003]、Lo, Ma and Chen [2005]、Wang [2005]）が考案された。この方法は、送信者がレーザー光源の強さを確率的に切り替えて、それに伴う受信側での検出率の変化を調べるものである。仮に、攻撃者が 2 光子以上の場合を選択的に攻撃すると、受信側は検出率の比を手掛かりに攻撃の有無を判定できる。また、デコイ法を用いることで、長距離通信での性能（1 光パルス当りの平均鍵生成数）は、理想的な単一光子光源を用いる場合と遜色ないレベルに改善できるほか、レーザー光源は光パルスの繰り返し速度が速いため、単一光子光源を使う

場合よりも高い性能（時間当りの平均鍵生成数）を得られることがわかった。

デコイ法は、図3のようなQKDにおける装置不完全性を考慮したプロトコルの改良と安全性証明の拡張の典型例である。これ以外の装置不完全性[23]については、例えば、Sajeed *et al*. [2021]がサーベイ結果を提供している。これらの装置不完全性を悪用した既知の実装攻撃に関しては、既に基本的な対策が考案されている。また、未知の実装攻撃と安全性が未解明の装置不完全性についても、採用した装置モデルと理想的な装置モデルとの差異が（fidelity に近い指標で）が十分に小さい場合に対処する方法（Pereira *et al.* [2020]）が考案されている。

装置不完全性については、装置のノイズ量を確かめることを含めて安全性を保証する枠組みになっている場合が多い。このため、いかに装置の性質を簡単に試験した上でQKDプロトコルとしての性能を確保するか、というのが重要な課題になっている。

５．考察

本節では、QKD の普及に向けた課題を考察する。本節（1）では、各国の情報セキュリティ関連機関等が公表したQKDに対するポジション・ペーパーを概観する。本節（2）では、QKD における相手認証について考察する。本節（3）で QKD の標準化動向を整理したうえで、本節（4）で普及に向けた課題を考察する。

（１）QKD に対する海外の評価

各国の情報セキュリティ関連機関等（当局）では、QKD の評価を含む文書を公開しており、その多くにおいて、QKD の実用性やコスト面について否定的な評価をしている。ただし、こうしたQKDに対する評価は、インターネットで用いられる汎用の暗号化通信において利用する場面を想定して行われた PQC との相対比較である点には注意が必要である。

こうした文書をみる限り、現時点において QKD は、性能とコストの両面から、各国において PQC の代替となることは展望されていない。QKD を導入した場合に得られる最大の恩恵は情報理論的安全性であり、そうした安全性は、超長期での秘匿性を要するケースのほか、PQC が秘密裡に破られているリスクやハーベスト攻撃の脅威に備えるのに適している。したがって、QKD の重要性は、その用途に依存する。2節（4）で述べた通り、QKDは、用途を限定した、特段に高い機密度が求められる情報の通信に適していることから、その適切な比較対象は Trusted Courier であろう。いずれにせよ、他の方式と比較する際に

[23] 例えば、送信側が所望の状態の量子ビットを誤りなく準備できるとの仮定が満たされない不確実性が考慮されている。

は、暗号の専門家による評価も踏まえつつ、QKD の用途や PQC との使い分けについての建設的な議論が必要である。

以下では、各国当局の QKD に対する評価の概要を紹介する。

米国 NSA（National Security Agency [2021]）は、以下に掲げる QKD の技術的制約が解消されない限り、国家安全保障システム（National Security Systems）における QKD の利用を推奨しないとしている。

① QKD は、デジタル署名に相当する認証手段を提供しない。
② QKD は、専用の通信装置を必要とする。
③ 中継器を信頼しなければならず、インフラ・コストが増す。
④ QKD が保証する実際の安全性は、通信装置の実装に依拠する。

NSA や後述する各国の議論においても制約とされているこれらの点について、筆者らは次のように考える[24]。①については、QKD の有用性を大きく損なうものではない。詳しくは本節（2）を参照されたい。②と③については、主として導入コストの問題であるが、超長期的な秘匿性が必要となるケースでは、そうしたコストを払ったうえでも QKD は有望な選択肢となろう。また、既存回線と QKD の回線を共存させることで、コストを抑制する方式が研究されていることもサポート材料である。④については、PQC を含む古典暗号でも同様の制約がある。ただし、QKD の場合、装置の安全性を認証する制度的枠組みの整備が課題ではある。詳しくは、本節（3）を参照されたい。

英国の国家サイバー・セキュリティ・センター（National Cyber Security Centre: NCSC）も、2020 年 11 月に公表した暗号移行に関するホワイト・ペーパー（National Cyber Security Centre [2020b]）において、上記①、②を理由に挙げて、あらゆる政府機関や軍における QKD の利用を推奨しないとしている。また、理由の仔細について、同年 3 月に公表された QKD と量子乱数生成に関するホワイト・ペーパー（National Cyber Security Centre [2020a]）でも詳述されている。

オランダ通信安全委員会（Netherlands National Communications Security Agency [2022]）も、①を理由に QKD は中間者攻撃（man in the middle attack）に対して脆弱であるとしている。中間者攻撃とは、送信者と受信者がお互いに正しい相手と通信していると信じている状況において、攻撃者が両者の通信を仲介して

[24] このほか、Renner and Wolf [2023] が、NSA の評価に対して検討を加え、反論している。同稿では、NSA の掲げた QKD の問題の多くが、中期的および長期的な将来において解消されると結論している。ここでの中期的な将来とは、安価な光学装置や量子中継器が利用できる時代を指す。長期的な将来は、量子コンピュータが量子ネットワークで結ばれている時代を指す。

通信内容の盗聴および改変を行うことにより情報を窃取する攻撃である。なお、こうした脆弱性を解消するために PQC を認証に利用すると、QKD が有する相対的な優位性が失われるとしている。また、QKD を組み込んだアプリケーション全体が考慮されていないことから、安全性証明は不完全であるし、通信装置について置かれた多くの仮定は現実的ではないとしている。さらに、通信距離も短く、trusted points が多く、スケーラビリティに乏しいとしている。以上から、QKD は PQC の本格的な代替にはならないと結論付けている。

フランスの国家情報システム・セキュリティ庁のポジション・ペーパー（Agence Nationale de la Sécurité des Systèmes d'Information [2023]）では、QKD は大規模な展開が困難であり、汎用の量子コンピュータによるリスクはすでに PQC において考慮されているとしている。また、QKD は高いセキュリティが求められる拠点間通信などのニッチな応用はありうるとしながらも、現代の通信システムに求められるさまざまな機能的要件（スケール性、通信速度、End-to-End〈端から端まで〉の暗号化など）を充足しないことから、長期的なデータ保護の目的にも PQC の方が望ましいとしている。

フランス、ドイツ、オランダ、スウェーデンの情報セキュリティ当局が合同でポジション・ペーパー（ANSSI *et al.* [2024]）を公表している。米国 NSA が掲げる QKD の制約を挙げたほか、QKD は通信速度の制約からデータ本体の暗号化には利用できないとしている。すなわち、データ本体はワンタイム・パッドではなく、共通鍵暗号で暗号化する必要があるため、情報理論的安全性はデータ本体には保証されないと主張している。また、理論的に保証される安全性は、実装された現実の通信装置には適用できないとしている。以上から、QKD は発展途上の技術であり、現時点ではニッチな用途に限られると結論づけている。

ただし、筆者らの見解ではあるが、QKD は鍵共有プロトコルを常時実行することで、鍵を平時より蓄積することができるため、ワンタイム・パッドと組み合わせることは十分に可能であると考える。また、4 節で述べたように、安全性証明も装置不完全性を考慮しているため、理論と現実のギャップは縮まっているといえる。

（２）認証手段について

本節（1）の米国 NSA の例で述べたように、QKD は認証手段を提供しないとの批判がある。相手認証を行わない場合には、QKD は中間者攻撃に脆弱となる。もっとも、QKD では、量子通信路に加えて古典通信路も利用するため、これを使って任意の相手認証手段を組み合わせることが可能である。理想的には鍵共有を行う前に通信相手の正しさを証明する相手認証を行うことが望ましい。そこで、本節（2）では、QKD に組み合わせる相手認証手段の選択が、相手認証

も含めた QKD プロトコル全体の前提と安全性評価に与える影響について述べる。とくに、後段で述べるように、相手認証が計算量的安全性に基づくものであっても、QKD の有用性が大きく損なわれるとは限らないことを説明する。

多くの QKD のプロトコルでは、QKD の最大のメリットである情報理論的安全性を認証手段も含めて達成するために、情報理論的安全性を有する Wegman-Carter 認証（Wegman and Carter [1981]）を組み合わせることが想定されている。しかし、同認証方式は、送受信者が少量（高々古典通信量の対数程度）の安全な乱数を事前に共有していることを仮定する。Wegman-Carter 認証を利用する限りにおいて、QKD は、鍵配送（key distribution）よりも、鍵伸長（key growing）と呼ぶべきである。すなわち、QKD は、Wegman-Carter 認証のために事前に共有した安全な乱数を増幅する役割を担っているとみなせる。

相手認証に、情報理論的安全性を求めない場合には、計算量的安全性に基づく認証手段を選択することも可能である。楕円曲線暗号によるデジタル署名では、量子コンピュータに対する安全性が確保できないため、攻撃者によるなりすましのリスクがある。

PQC ベースのデジタル署名では、量子コンピュータによる安全性が確保できる。この場合には、2 節（4）で述べたとおり、QKD の PQC に対する相対的な優位性が乏しくなるとの批判がある。もっとも、相手認証において情報理論的安全性を達成する重要性は、データの秘匿性に比較して小さい。相手認証では、メッセージの送受信が開始されてから完了するまでの限られた間だけ通信相手の真正性が保証されれば十分である。仮に、認証が計算量的安全性に基づくものであり、将来的に破れたとしても、通信が完了していた場合には、通信相手のなりすましは意味がなく、悪影響はない。したがって、実用的には、計算量的安全性に基づく認証方式が短時間で破られなければ、データ本体の秘匿性を確保する QKD の有用性は大きく損なわれないと考えられる。

（３）QKD の標準化動向

QKD については、通信装置の安全性に認証を与える制度的枠組みの整備が課題となっており、現在、国際標準化が進められている。こうした制度的枠組みは、暗号製品の安全性を国際規格に基づいて証明し、お墨付きを与えることから、製品の普及を後押しすることが期待される。以下では、まず、古典的な暗号製品に関する制度を概観する。

古典的な暗号製品については、第三者が評価・認証する制度的枠組みが整備されており、そのもとで運用されている。わが国では、「IT セキュリティ評価および認証制度（JISEC: Japan Information Technology Security Evaluation and

Certification Scheme）」[25]のもとで、国際標準化機構（ISO/IEC 15408）が定めたコモン・クライテリア（Common Criteria: CC）に基づいて製品・システムのセキュリティ機能が定義され、その機能が適切に実装されているか否かが評価・認証されている。また、「暗号モジュール試験および認証制度（JCMVP: Japan Cryptographic Module Validation Program）」[26]は、米国連邦政府標準規格 FIPS 140-3（またはこれをベースとした ISO/IEC 19790）などに基づく暗号モジュールの試験・認証制度である。電子政府推奨暗号リスト [27]に記載されている暗号アルゴリズム等を実装した暗号モジュールは、JIS X 19790（日本における ISO/IEC 19790 の対応規格）に基づいて第三者機関により試験・認証されている。これらの制度の歴史的背景については、田村・宇根［2008］が詳細に解説している。

QKD についても、その普及に向けて、暗号プロトコルの標準化や暗号モジュールを組み込んだ製品の評価・認証の制度的枠組みが重要になると考えられる。すなわち、QKD 製品の導入に当たり、国際標準に基づくセキュリティ評価基準を満たすことを第三者機関により認証されており、公的機関から推奨された実装方式となっていることは、重要な判断基準となる。

この点、欧州を始めとする各国において、近年、QKD に関するセキュリティ評価基準の策定が進められている。欧州では、欧州電気通信標準化機構（European Telecommunication Standards Institute）が、CC ベースの評価のためのセキュリティ要件を定めたプロテクション・プロファイル（Protection Profile、ETSI GS QKD 016）を 2023 年 4 月に公表しており、日本の情報通信研究機構（NICT）も策定に協力した [28]。

このほか、セキュリティ評価基準の国際標準化に向けた議論も大きく進展している。具体的には、電気通信に関する国際標準である ITU-T 勧告（ITU-T Recommendation）[29]の Y.3800 番台には、既に発効している QKD の標準が数多く存在し、執筆時点（2024 年 2 月）では、Y.3800～Y.3819 までの 20 個の標準が策

---

[25] JISEC の概要については、以下の情報処理推進機構のウェブ・ページを参照されたい。
https://www.ipa.go.jp/security/jisec/about/index.html

[26] JCMVP の概要については、以下の情報処理推進機構のウェブ・ページを参照されたい。
https://www.ipa.go.jp/security/jcmvp/index.html

[27] CRYPTREC（Cryptography Research and Evaluation Committees）が定めた、電子政府における調達のために推奨すべき暗号のリスト。CRYPTREC 暗号リストとも呼ばれる。

[28] 詳しくは、NICT のページ（ https://www2.nict.go.jp/qictcc/social/standard.html、2024 年 2 月 14 日）を参照されたい。

[29] ITU（International Telecommunication Union、国際電気通信連合）は 電気通信に関する国際標準の策定を目的とした国連の専門機関である。また、ITU-T（ITU Telecommunication Standardization Sector、ITU 電気通信標準化部門）は、ITU を構成する 3 つの部門の 1 つである。ITU-T が策定する国際標準は、ITU-T 勧告として公表される。

定されている。ITU-T 勧告は、WTO/TBT 協定[30]に基づく強制力を持つデジュール標準[31]の一つである。また、WTO 協定に含まれる「政府調達に関する協定」では、政府の調達における技術仕様について、適当な場合には国際規格に基づいて定めることが規定されているため、ITU-T 勧告は政府調達にも影響力を持つ。

情報セキュリティ分野の標準を策定する ISO/IEC JTC 1/SC 27 においても、QKD の安全性に関する標準が検討されている。現在、審議中の標準 ISO/IEC CD 23837-1/2 は、QKD のセキュリティ要件や、テストと評価方法の標準を定めるものである。欧州電気通信標準化機構においても、傘下の ISG（Industry Specification Group）において、QKD の標準化が進められている。これらの標準には、日本人研究者らの知見も多く取り入れられている。標準を策定したあとの制度運用に向けては、国内において認証機関や試験実施機関を養成することも重要である。

（４）普及に向けた課題

QKD の普及に当たって、以下の 4 つの課題が指摘できる。

1 つ目の課題は、プロトコルと通信装置、安全性証明に関する理論の成熟による通信性能の向上である。これらは、それぞれ独立した要素ではなく、プロトロルと装置を改良すれば、これに対応する安全性証明が必要とされる、という関係にある。

2 つ目の課題は、装置の安全性を評価・認証する制度的枠組みの整備である。さまざまな事業者が製造した QKD の通信を同一のネットワーク上で成立させるためには、プロトコルの仕様の標準化が不可欠である。また、実装攻撃を予防するための実装ノウハウの蓄積と検証も求められる。なお、わが国においては、政府調達にかかる暗号の推奨リスト（電子政府推奨暗号リスト）への掲載を検討する価値もあると考えられる。

3 つ目の課題は、量子中継（quantum relay）の実現である。古典中継による QKD では、中継装置を信頼する前提を置く必要があり、これが QKD の価値を大きく減じているといえる。執筆時点（2024 年 2 月）において、量子中継の成

---

[30] WTO 協定に包含される TBT 協定は、工業品等の各国の規格とその適合性評価手続きが国際貿易に不必要な障害（Technical Barriers to Trade）をもたらすことがないよう、国際規格を基礎として規格を制定する原則等を定めるもの。

[31] デジュール標準は、標準化機関によって公的に明文化され、公開された手続きによって作成された公的標準を指す。これに対して、フォーラム標準は、特定分野の標準化に関心がある企業・専門家らの合意により制定される標準を指す。デファクト標準とは、個別企業などの標準が市場の取捨選択・淘汰によって市場で支配的となったものである。

功例はないが、QKD が他の暗号化通信への相対的な優位性を確保するうえで、量子中継技術の実現は重要な分水嶺となる。量子中継の提案方式や課題については、Azuma *et al.* [2023]を参照されたい。

4 つ目の課題は、導入と運用コストの低減である。QKD は、専用の通信装置を要することから導入コストが高い。このため、各企業が独自にQKDの専用ネットワークを構築することは現実的ではなく、公的な取り組みによる通信基盤の整備・支援が必要となろう。この点、わが国において、国立情報通信研究機構（NICT）が QKD ネットワークの実証を行っているのは、望ましい方向といえよう。また、既存ネットワークとQKDを併存する技術の開発が進めば、運用コストも低減する可能性がある。

６．おわりに

主要国・地域において実証実験が進展しているとはいえ、QKD は未だ発展途上の技術であり、その社会的有用性は、不確実性の高い将来の技術革新に大きく依存する。現時点では、QKD は、インターネットで用いられる汎用の暗号化通信を代替する技術ではなく、限られた拠点間で機密度の高い情報を通信する用途に適していると評価できる。

ただし、情報理論的安全性を達成するQKDの強みは、耐量子計算機暗号でも保証できない強力な性質である。保存期間が極めて長い機密情報を送信する場合には、QKD は有用な選択肢となりうる。また、将来における、暗号解読に利用できる量子コンピュータの登場や、耐量子計算機暗号に対する暗号解読アルゴリズムの進歩は予期しえない。こうしたテール・リスクに対処できる点においても、QKD には社会的意義があると考えられる。

さらに、本稿の範囲を逸脱するが、遠い将来には、QKD ネットワークと既存の暗号技術（秘密分散）を組み合わせて情報理論的に安全な情報の分散保管・受け渡しを可能とする量子セキュア・クラウドや、量子情報処理装置のネットワークを世界規模で展開する量子インターネットなど、新しいサービスが創出される可能性もある。QKD の研究開発は、その社会的な意義と潜在的な有用性を鑑みながら進められていくものと思われる。

目下、高いセキュリティを確保することが求められる金融機関においては、QKD の技術的な到達点および、QKD が提供するセキュリティ・サービスとその安全性を正確に理解することが重要である。

以　上

【参考文献】

宇根正志、「量子コンピュータが暗号に及ぼす影響にどう対処するか：海外における取組み」、金融研究所ディスカッション・ペーパーNo. 2023-J-13、日本銀行金融研究所、2023 年 a

――――、「量子コンピュータに耐性をもつ暗号への移行：金融分野における検討動向」、量子 ICT フォーラム・セミナー講演資料（2023 年 12 月 20 日）、量子 ICT フォーラム、2023 年 b（https://qforum.org/news/38087、2024 年 3 月 26 日）

菅野　哲、「耐量子計算機暗号（PQC）への暗号移行に向けた技術動向」、情報セキュリティ・セミナー講演資料、日本銀行金融研究所、2023 年（https://www.imes.boj.or.jp/jp/conference/citecs/23sec_semi01_docs/23sec_semi01_s2.pdf、2023 年 10 月 17 日）

小芦雅斗・小柴健史、『量子暗号理論の展開』、サイエンス社、2008 年

後藤　仁、「量子暗号通信の仕組みと開発動向」、『金融研究』第 28 巻第 3 号、日本銀行金融研究所、2009 年、107～150 頁

鈴木雅貴・菅原　健・鈴木大輔、「サイドチャネル攻撃に対する安全性評価の研究動向と EMV カード固有の留意点」、『金融研究』第 34 巻第 4 号、日本銀行金融研究所、2015 年、107～134 頁

田村裕子・宇根正志、「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において利用していくために」、『金融研究』第 27 巻別冊第 1 号、日本銀行金融研究所、2008 年、79～114 頁

藤原幹生、「量子暗号技術 拡充された東京 QKD ネットワーク」、量子 ICT フォーラム・セミナー講演資料（2023 年 12 月 20 日）、量子 ICT フォーラム、2023 年（https://qforum.org/news/38087、2024 年 3 月 26 日）

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), “Should Quantum Key Distribution be Used for Secure Communications?” Technical Position Paper, ANSSI, 2023 (available at https://cyber.gouv.fr/en/publications/should-quantum-key-distribution-be-used-secure-communications、2024 年 3 月 26 日).

――――, Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces, “Position Paper on Quantum Key Distribution,” BSI, 2024 (available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html、2024 年 2 月 13 日).

Azuma, Koji, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin, “Quantum Repeaters: From Quantum Networks to the Quantum Internet,” arXiv: 2212.10820, 2023.

Barrett, Jonathan, Roger Colbeck, and Adrian Kent, “Memory Attacks on Device-

Independent Quantum Cryptography," *Physical Review Letters*, 110, 2013, Article Number 010503.

Bennett, Charles H., and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 1984 (available at https://doi.org/10.1016/j.tcs.2014.05.025、2023 年 7 月 6 日).

———, ———, and N. David Mermin, "Quantum Cryptography without Bell's Theorem," *Physical Review Letters*, Vol. 68(5), 1992, pp. 557–559.

Grosshans, Frédéric, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, 421, 2003, pp. 238–241.

Gottesman, Daniel, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill, "Security of Quantum Key Distribution with Imperfect Devices," *Quantum Information and Computation*, 4(5), 2004, pp. 325–360.

Ekert, Artur K., "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, 67, 1991, pp. 661–663.

Hwang, Won-Young, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, 91(5), 2003, Article Number 057901.

Koashi, Masato, "Simple Security Proof of Quantum Key Distribution Based on Complementarity," *New Journal of Physics*, 11(4), 2009, Article Number 045018.

Lo, Hoi-Kwong, Marcos Curty, and Bing Qi, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, 108, 2012, Article Number 130503.

———, and F. H. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science*, 283(5410), 1999, pp. 2050–2056.

———, Xiongfeng Ma, and Kai Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, 94(23), 2005, Article Number 230504.

Lucamarini, Marco, Zhiliang Yuan, James F. Dynes, and Andrew J. Shields "Overcoming The Rate-Distance Limit of Quantum Key Distribution without Quantum Repeaters," *Nature*, 557, 2018, pp. 400–403.

Matsuura, Takaya, Kento Maeda, Toshihiko Sasaki, and Masato Koashi, "Finite-Size Security of Continuous-Variable Quantum Key Distribution with Digital Signal Processing," *Nature Communications*, 12, 2021, Article Number 252.

Mayers, Dominic, "Quantum Key Distribution and String Oblivious Transfer in Noisy Channels," *Advances in Cryptology -- CRYPTO '96*, 1996, pp. 343–357.

Müller-Quade, Jörn, and Renato Renner, "Composability in Quantum Cryptography,"

New Journal of Physics, 11, 2009, Article Number 085006.

National Cyber Security Centre, "Quantum Security Technologies," White Paper, 2020a (available at https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies、2023 年 8 月 28 日).

———, "Preparing for Quantum-Safe Cryptography," White Paper, 2020b (available at https://www.ncsc.gov.uk/pdfs/whitepaper/preparing-for-quantum-safe-cryptography.pdf、2023 年 8 月 23 日).

National Institute of Standards and Technology (NIST), "Status Report on the Third Round of the NIST Post-Quantum Cryptography," 2022 (available at https://doi.org/10.6028/NIST.IR.8413-upd1、2023 年 7 月 18 日).

National Security Agency, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," 2021 (available at https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/、2023 年 6 月 20 日).

Netherlands National Communications Security Agency (NLNCSA), "Prepare for the Threat of Quantum Computers," 2022 (available at https://english.aivd.nl/publications/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers、2024 年 3 月 27 日).

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

Pereira, Margarida, Go Kato, Akihiro Mizutani, Marcos Curty, and Kiyoshi Tamaki, "Quantum Key Distribution with Correlated Sources," *Science Advances*, 6(37), 2020, Article Number eaaz4487.

Pirandola, Stefano, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi, "Fundamental Limits of Repeaterless Quantum Communications," *Nature Communications*, 8, 2017, Article number 15043.

Renner, Renato, "Security of Quantum Key Distribution," Dissertation ETH, No. 16242, 2005 (available at https://arxiv.org/abs/quant-ph/0512258、2023 年 7 月 20).

———, and Ramona Wolf, "The Debate over QKD: A Rebuttal to The NSA's Objections," arXiv: 2307.15116, 2023.

Sajeed, Shihan, Poompong Chaiwongkhot, Anqi Huang, Hao Qin, Vladimir Egorov, Anton Kozubov, Andrei Gaidash, Artur Vasiliev, Artur Gleim, and Vadim Makarov, "An Approach for Security Evaluation and Certification of a Complete Quantum Communication System," *Scientific Reports*, 11, 2021, Article Number 5110.

Shor, Peter W., and John Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, 85(2), 2000, pp. 441–444.

Tomamichel, Marco, Christian Schaffner, Adam Smith, and Renato Renner, "Leftover Hashing Against Quantum Side Information," *IEEE Transactions on Information Theory*, 57(8), 2011, pp. 5524–5535.

Wang, Xiang-Bin, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Physical Review Letters*, 94(23), 2005, Article Number 230503.

Wegman, Mark N., and J. Lawrence Carter, "New Hash Functions and Their Use in Authentication and Set Equality," *Journal of Computer and System Sciences*, 22(3), 1981, pp. 265–279.

Wengerowsky, Sören, Siddarth Koduru Joshi, Fabian Steinlechner, Hannes Hübel, and Rupert Ursin, "An Entanglement-Based Wavelength-Multiplexed Quantum Communication Network," *Nature*, 564, 2018, pp. 225–228.

補論

ϵ-安全（ϵ-security）の証明には、大きく 2 つのアプローチがある。

1 つ目のアプローチは、量子版の残余ハッシュ補助定理（leftover hash lemma）を使う方法（Renner [2005]、Tomamichel *et al.* [2011]）である。この方法は、ふるい鍵のハッシュ値を送受信者間で比較するものである。正規の送受信者の場合、一致したふるい鍵を共有しているため、ハッシュ関数値が両者間で一致する。ふるい鍵の一部の情報しか持っていない盗聴者にとっては未知の要素が混じるため、出力の一致を確認できない。両者が十分に一致していれば、最終鍵は安全であるといえる。

2 つ目のアプローチは、仮想的な誤り訂正を考える方法（Lo and Chau [1999]、Shor and Preskill [2000]、Koashi [2009]）である。この方法は、盗聴による鍵の変化を、盗聴者が鍵の情報を得たことによって生じる誤り（エラー）とみなし、その訂正可能性を検証するものである。もし訂正が可能であれば、盗聴者は十分な量の情報を得ておらず、最終鍵は安全であるといえる。この方法は、実験的に非常に難しい量子誤り訂正を実施することなく、訂正可能性をエラー率から理論的に判定するのみであるため、仮想的な誤り訂正と呼ばれる。これらの証明のあと、ϵ-security を保証するための対象とするプロトコルにおいて、最終鍵の安全性の高さを示す特徴的な量（min-entropy、位相エラー率）をより厳密に評価する議論が発展していった。