量子暗号技術の研究開発動向と展望

国立研究開発法人
情報通信研究機構
未来ICT研究所
量子ICT先端開発センター
センター長

武岡（たけおか）　正裕（まさひろ）

国立研究開発法人
情報通信研究機構
未来ICT研究所
量子ICT先端開発センター
研究マネージャー

藤原（ふじわら）　幹生（みきお）

国立研究開発法人
情報通信研究機構
未来ICT研究所
主管研究員

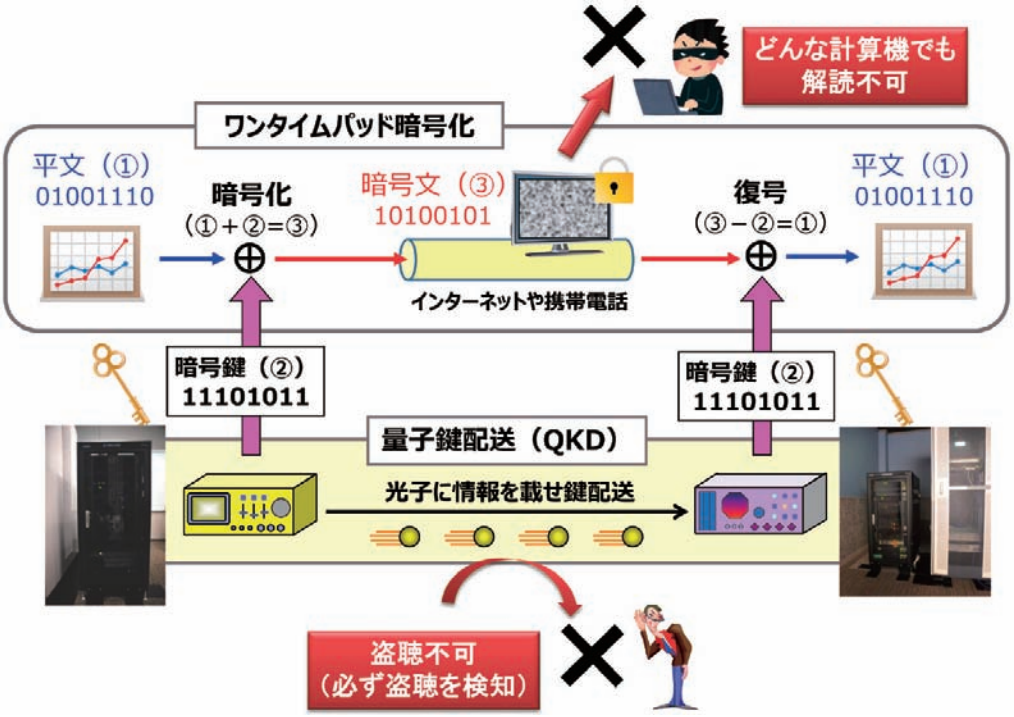
佐々木（ささき）　雅英（まさひで）

1. はじめに

現在のネットワーク社会を支える情報通信技術の発展は目覚ましく、今も日々進歩し続けている。一方、従来の技術体系の延長上では将来的に性能限界を迎える可能性も指摘されている。原子や電子、光子などを扱う最新の物理学である量子力学の性質を極限まで駆使した量子通信技術は、あらゆる計算機で解読不可能なセキュリティ技術や、宇宙での超長距離高速通信、時刻同期の超精密化など、様々な情報通信分野で抜本的な技術革新が可能になることが理論的に予言され、その研究開発が世界中で進んでいる。多くはまだ基礎研究段階にあるが、本稿では、量子通信技術の中でも実用化に向けた研究開発が最も進んでいる量子暗号技術について、その現状と国内外の取組みを紹介する。

2. 量子暗号とは

現在、社会の様々な場面で用いられているRSA暗号、楕円暗号などの数学的なアルゴリズムに基づく暗号は、非常に使い勝手がよい反面、将来的な計算技術の革新によって解読されてしまう潜在的な危険性がある。RSA暗号の解読に必要な計算量とスーパーコンピュータの性能の関係などは既に試算されている[1]。また、最近急速に研究開発が進む量子計算機の大規模化がもし実現すると、これらの暗号は一挙に解読可能になると予測されている。さらに、数学的な暗号は、たとえ現在の計算機では能力が不十分でも、まずは暗号データを盗聴・保存しておき、将来開発した高度な計算技術でそれを解読することも可能である。これは、国家機密やゲノム等の医療情報など、最高度のセキュ



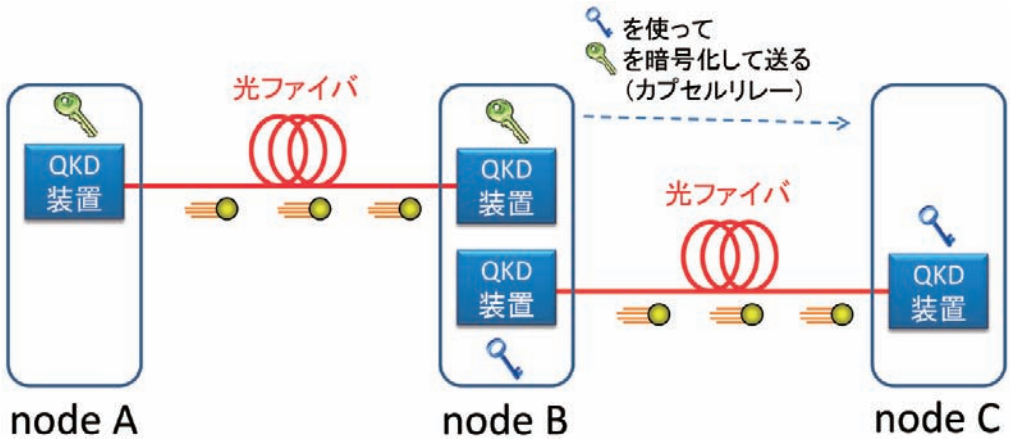
■図1.　量子暗号による暗号通信の概要（写真はNECのQKD送受信機）

リティが数十年単位の長期にわたって求められるような情報の通信においては重大な脅威となる可能性がある。

量子暗号は、数学的な計算困難性ではなく、量子力学と統計学に立脚した安全性を持つ質的に新しい暗号方式であり、現状の暗号で唯一、量子計算機を含むあらゆる計算機を使っても原理的に解読不可能なことがが証明されている。このような安全性は計算量的安全性に対して「情報理論的安全性」と呼ばれる。つまり、量子暗号が正しく動作すれば、将来、計算機や数学がどれだけ発達しても永久に解読できない暗号化が実現できることになる。

図1に、量子暗号において暗号鍵生成を行う量子鍵配送（Quantum Key Distribution：QKD）、及び鍵を使った暗号化の概略を示す*。QKDでは、鍵となる乱数の配送のため、光の最小エネルギー単位である光子が平均して1個以下しか含まれない超微弱な光パルス（通常の光通信では10～100万個レベル）を光ファイバ等により伝送する。光子レベルの信号には光の量子性が強く現れる。特に量子力学の基本原理の1つである不確定性原理に由来する「信号に対するいかなる測定（盗聴）行為も信号の量子状態に必ず痕跡を残す」という性質を利用して、信号に対する盗聴行為の有無を判別し、盗聴がされていないことが保証できる信号のみを鍵として用いることで、安全な鍵を共有する。また、鍵となる乱数列は好きなものを準備すればよいため、物理乱数源等で生成される何の数学的構造も持たない乱数を用いれば、暗号化されたデータへのいかなる計算機攻撃も無意味となる。こうして、鍵配送へのあらゆる物理的な盗聴を検知し、かついかなる計算機攻撃でも解読不可能な暗号を実現することができる。実際のQKD装置は、光子の送受信デバイスに加え、鍵情報の誤り訂正や純粋化（秘匿性増強）などを行う信号処理ボードなどから構成される。また、鍵そのものは0, 1の乱数列であり、鍵を共有した後のデータの暗号化や復号化、伝送は通常の計算機やインターネット等の通信回線で実行できる。

QKDは、数理暗号の根本的な問題を解決し、ある意味究極的な安全性を実現できるが、一方で実装上の大きな制限もある。光子は伝送路の損失で容易に失われてしまう上、長距離ファイバ通信では必須の光増幅器は信号の量子状態を破壊してしまうため用いることができない。このためファイバ通信においては、単体のQKD送受信装置では伝送距離が50～100km程度、また鍵生成速度についても、距離や装置性能によるが、現状では波長当たり数10k～数Mbps程度に制限されている。今後の技術開発や波長多重化などによりある程度の改善は見込まれるが、抜本的に解決するには量子中継技術と呼ばれるある種の光量子計算の処理が必要となり、その実現にはまだ時間がかかると予想されている。このため、QKDのネットワークを構成するには、現在はtrusted nodeと呼ばれる安全性の保証された局舎でQKD回線をつなぎ、鍵をリレーしている（図2）。これにより任意の構成のQKDネットワークを構成できるが、中継する局舎の安全性は必ず確保しなくてはならない。



■図2.　安全な局舎（trusted node）を介した鍵リレーによるQKDのネットワーク化

＊　QKDで作られた鍵を使った暗号化には複数の方法があるが、あらゆる計算機で解読不可能な情報理論的安全性を達成するためには、1ビットの鍵で1ビットの情報を暗号化し、さらに一度使った鍵は二度と使わない「ワンタイムパッド」方式を用いる必要がある。したがって、「量子暗号は情報理論的に安全である」という場合、それはQKD+ワンタイムパッド暗号化による暗号通信のことを指している。

3. 国内外の研究開発動向

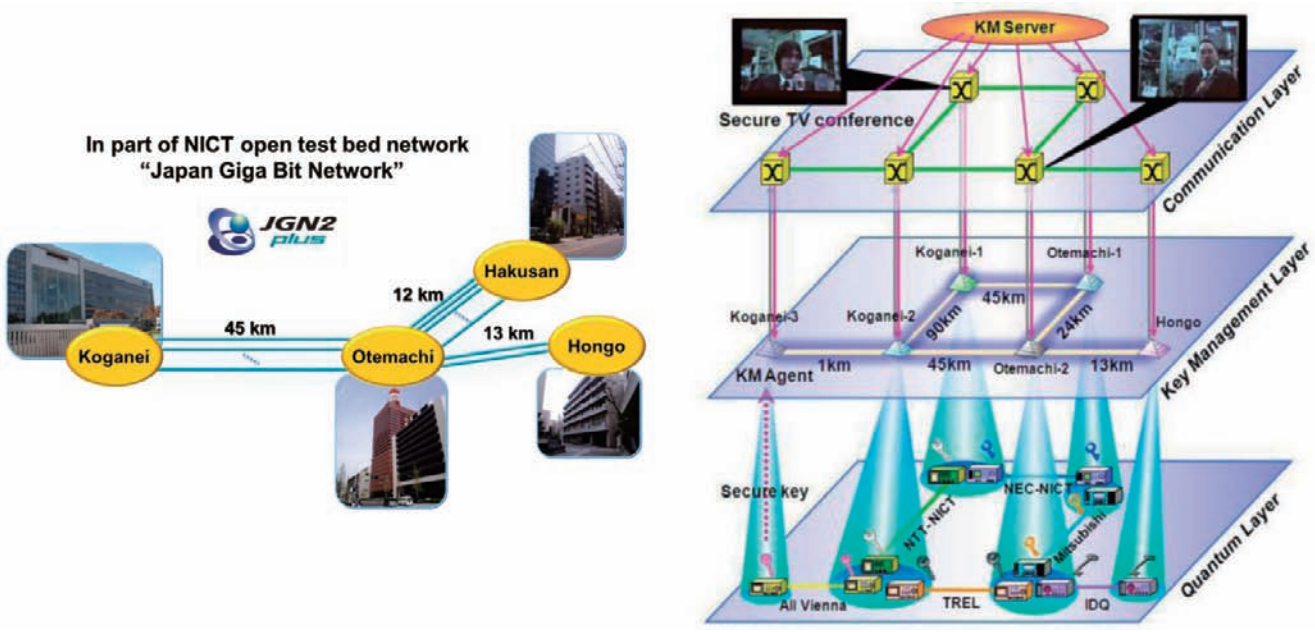
このように、量子暗号は技術的にはまだ発展途上であるが、従来暗号では不可能な安全性を実現できることから、世界各国で研究開発が活発に進められている。ここでは、QKDのフィールド実装に関する研究開発動向を紹介する（それぞれの詳細・文献については [2、3] などを参照）。

ファイバによる地上のQKDネットワークでは、2004年、米国国防高等研究計画局（DARPA）のDARPA Quantum Networkプロジェクトが、ボストン地区の3地点約10kmを結ぶ世界初の都市圏QKDネットワークを実証した。2008年には欧州連合のSECOQC（Secure Communication based on Quantum Cryptography）プロジェクトが、ウィーン市内の6地点を結ぶQKDネットワークを構築して30kmで約1kbps程度の鍵生成を実現し、音声（電話回線）の暗号化通信などが実証された。また、複数の研究機関がそれぞれ開発した異なる方式のQKD装置の相互接続にも成功した。

我が国では、総務省と情報通信研究機構（NICT）が中心となって産学官連携プロジェクトを推進し、2010年には、鍵生成速度をそれまでの100倍向上させる100kbps級のQKD装置によるネットワーク「Tokyo QKD Network」を東京圏に構築し、QKDによる動画（ビデオ会議）の秘匿伝送の実証に世界で初めて成功した[4]。また、このネットワークは前の2つと異なり、その後現在に至るまで運用を続けており、日本の様々な研究機関が開発したQKD装置の開発・試験運用やネットワーク実験などが進められ、現在では、伝送距離50kmで約1Mbpsと、フィールド実装としては世界最高性能を実現している。また、QKDネットワークを安全かつ適切に管理するための鍵管理プラットフォーム技術や、アプリケーション層へ適切に鍵を供給するインタフェースなど、実用化に向けたシステム全体の開発もいち早く進めており、これらを総称してQKDプラットフォーム技術と呼んでいる。Tokyo QKD Networkで開発・試験されたQKD技術は、実際のユーザ環境へ展開されており、2015年には、NECは自社内のサイバーセキュリティ関連施設内の回線で、東芝は仙台にある東芝ライフサイエンス解析センターと東北大学東北メディカル・メガバンク機構の間約7kmをつなぐ回線で、それぞれ自社開発したQKD装置の試験運用を開始している。

一方、ここ数年では中国の進展が目覚ましい。約3年半をかけて北京−上海間の約2,000kmを32個の安全な局舎でつないだ世界最大のQKDネットワークを構築し、2017年からその運用を開始している。また、英国、イタリア等でも国家プロジェクトによるQKDネットワークの構築が進められ、米国では、量子暗号企業によるボストン−ワシントンDC間でのQKDネットワークサービスの計画が発表されるなど、世界的な研究開発・実用化競争が続いている。

QKDはファイバだけでなく、空間光通信回線でも動作可能である。例えば日米間など、大陸間レベルの超長距離鍵



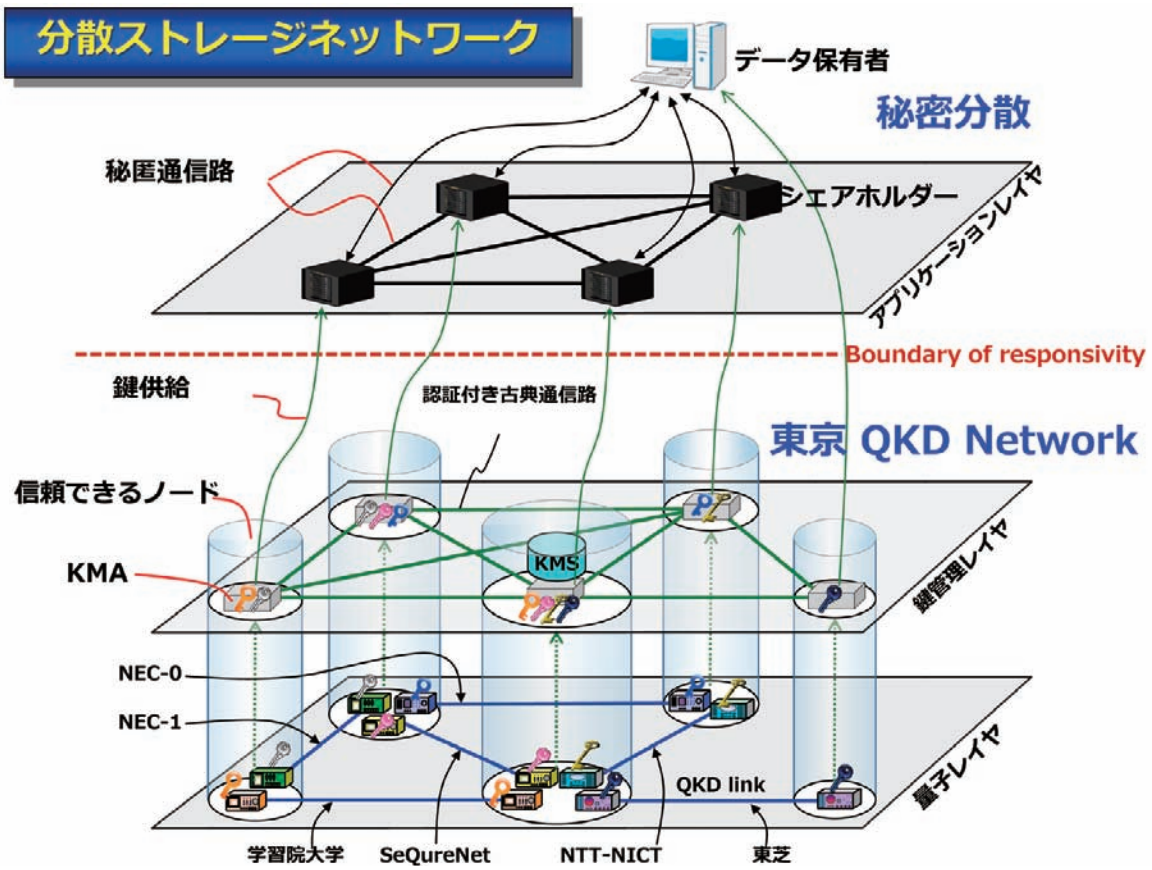
■図3. 2010年に構築されたTokyo QKD Network（左）とQKDプラットフォーム（右）[4]。現在のネットワーク稼働状況については [5] 参照。

配送を実現しようとすると、局舎でつながれた地上QKDネットワークではその実現は難しい。一方、人工衛星が飛ぶ上空では大気も薄く、損失の極めて少ない光通信が可能である。衛星QKDの実現に向けた研究は各国で進められていたが、2017年に中国が衛星－地上局間でのQKDによる鍵生成に世界で初めて成功し、さらに衛星を介した中国－オーストリア間の鍵配信にも成功し、配信された暗号鍵を使った5kBの画像の暗号化伝送も実証している。日本ではNICTが将来的な実用技術を見据えて、中国の衛星よりも10分の1以下の重量であり、コスト的にも優れた超小型衛星を用いた量子通信基礎実験（光子レベルの微弱信号送受信）に世界で初めて成功している[3]。衛星量子暗号のプロジェクトは世界中で開始されており、今後の競争がより激化すると予想されている。

4. 量子暗号と現代セキュリティ技術の融合：QKD秘密分散ストレージネットワーク

QKDはデータ伝送時の究極的な安全性を保証するが、ストレージに保存されているデータを守るものではない。一方、現代暗号の分野ではデータを分割・暗号化して保存する、秘密分散という手法が知られている。例えば、シャミアの（n, k）閾値分散法という方法では、元のデータをn個のシェアに分割・暗号化する。n個のうち、k個以上のシェアを集めれば元のデータが復元できるが、k個以下のシェアだけでは、いかなる計算機を使っても元のデータの復元が原理的に不可能、すなわち情報理論的な安全性を実現できるという性質を持っている。したがって、これをn箇所の離れたストレージに分散保存しておけば、仮にその一部が盗まれたとしても情報理論的に安全であり、逆に一部が例えば災害等で欠損しても情報復元が可能であるという、データの秘匿保存とバックアップを同時に実現できる優れた数理アルゴリズムである。ただし、シェアを分散したストレージまでどうやって安全に伝送するかについては回答を与えていない。つまり、QKDと秘密分散が伝送と保存を互いに補完しあえば、秘密分散の持つ安全性のポテンシャルを十分に発揮し、システム全体が情報理論的に安全なストレージネットワークの実現が可能になる。

NICTと東京工業大学は、Tokyo QKD Network上の5つ



■図4．QKDを用いた秘密分散ストレージネットワーク［2、6］。

のノードを使って、上記の秘密分散プロトコルを実装したQKD秘密分散ストレージネットワーク（**図4**）を構築した。さらに、1つのパスワードで情報理論的に安全な認証を実現できるプロトコルを開発し、情報理論的に安全な認証・伝送・保存・復元の実証実験に世界で初めて成功している（[6] 及び [2] の3-2節）。このような分散ストレージは、例えば医療情報など、極めて高い秘匿性が要求されつつ、一方で地震や火災などの災害に備えたバックアップが同時に実現できる方法として、近い将来の社会実装が期待される。50〜100km圏のQKDネットワークを構築し分散保存できれば、大地震・津波などに対しても有効な秘匿バックアップとして機能すると考えられる。

5. 標準化活動

欧州のSECOQCプロジェクト後に、欧州電気通信標準化機構（ETSI）においてQKDについて検討を行うIndustrial Specification Group、ISG-QKDが設置され、これまで包括的な議論のほか、QKD装置の実装安全性（実際のデバイスの性能・物理的性質を考慮した安全性）、アプリケーションインタフェース等が詳しく議論されてきた。QKDの標準化活動は長らくETSIでのみ続いてきたが、ごく最近、他の標準化機関でも議論が始まっている。国際電気通信連合電気通信標準化部門（ITU-T）では、今年に入りStudy GroupのSG13、SG17でQKDのネットワークフレームワークやネットワークセキュリティなどに関する提案がなされている。国際標準機構（ISO/IEC）においても、技術レポート作成などが行われている。また、中国では、中国通信標準化協会（CCSA）において量子通信技術の包括的なフレームワークの議論を進めている。今後の活発な議論やリエゾンなどが進むものと予想される。

6. おわりに

量子暗号は、いかなる計算機でも解読不可能という、適切に実装されれば究極的な安全性を実現できる反面、距離・速度の制限、さらにはコスト面など、数理暗号にはなかった実用上の課題も存在する。このため、まずはハイエンドの技術としての社会実装から進むものと考えられる。また、QKDの要素技術である物理乱数源や鍵管理・運用アーキテクチャなどは、それ自体を切り出した応用展開も進んでいる。一方、数理暗号の中には、たとえ計算量的な安全性であっても、量子計算機による攻撃に対しても安全であるといわれる耐量子計算機暗号のような新しい技術も存在する。今後は、量子暗号を含めた様々なセキュリティ技術を適材適所で活用し、また暗号を含めたシステム全体において、必要な場面に必要な安全性を提供するトータルソリューションを見据えた研究開発が重要になってくると考えられる。

参考文献

[1] CRYPTREC “暗号技術評価委員会報告”、2013年。
[2] 情報通信研究機構研究報告 “量子情報通信技術特集”、Vol. 63, No. 1 (2017).
[3] 藤原 幹生、竹中 秀樹、Alberto Carrasco-Casad、北村光雄、佐々木 雅英、豊嶋守生、“量子通信に向けた超小型衛星−地上間の光通信実験”、第38回 量子情報技術研究会資料QIT2018-17、2018年。
[4] M. Sasaki et al., “Field test of quantum key distribution in the Tokyo QKD Network”, Opt. Express, 19, 10387 (2011).
[5] The Project UQCC (Updating Quantum Cryptography and Communications). http://www.uqcc.org/
[6] M. Fujiwara et al., “Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing”, Sci. Reports, 6, 28988 (2017).