量子暗号通信の研究開発から事業化への取り組みと今後の展望

Toshiba Group's Approaches to Quantum Cryptography Communication from Research and Development through to Commercialization and Its Future Prospects

村井　信哉 MURAI Shinya

近年の量子コンピューター技術の急速な進展は，新たな計算機応用の創出に期待が集まる一方で，現在の情報通信で広く利用されている暗号アルゴリズムが，短時間で解読される危険性を高めている。この問題への対策として，量子暗号通信が注目されており，社会実装も進みつつある。

東芝グループは，長年培ってきた量子暗号通信技術の実用化と事業化を推進している。既に，商用サービス化を前提としたトライアルを世界各国で開始し，将来にわたって安全な暗号鍵を多くのユーザーに届ける量子鍵配送（QKD）サービスの実現を目指している。

The rapid progress of quantum computer technologies in recent years has raised expectations for the creation of unprecedented applications, while at the same time increasing the risk of rapid decryption of the encryption algorithms that are widely used in current communication networks. Quantum cryptographic communication technologies are now attracting attention as a solution to this issue, and their social implementation has been accelerating.

The Toshiba Group has been taking the initiative in constructing quantum cryptographic communication technologies based on its long accumulation of development experience and know-how in this field, and is making efforts to promote the commercialization of such technologies. We have been conducting a variety of trial services in various countries toward the inauguration of commercial services, with the objective of realizing quantum key distribution (QKD) services that will make it possible to continuously provide large numbers of customers with secure cryptographic keys into the future.

1. まえがき

情報通信ネットワーク（以下，ネットワーク）は，今や私たちの生活に欠かせないものとなっている。日常的に利用される電子マネーやクレジットカードはネットワークを介して決済され，家庭内にはスマート家電が普及し，自動車も情報通信機能を具備したコネクテッドカーが当たり前になりつつある。また，ビジネス領域においては，製造業では，多様な設備・施設が連携するスマートマニュファクチャリング，農業などでは，センサーを使って集めたデータが品質や生産性などの向上に生かされている。

このように，様々な領域でクラウドサービス化や，IT（情報技術）化，IoT（Internet of Things）化が進み，今後，人間社会におけるネットワークへの依存度は，ますます高まっていくと考えられる。

ネットワークを流れる情報は，暗号化により守られ，通信の安全性が担保されている。そして，多くの暗号通信技術は，現在のコンピューターでは暗号の解読に膨大な時間が掛かることが，安全性の根拠となっている。

しかし，量子コンピューターの登場とその急速な進化により，この安全性が脅かされ始めている。圧倒的な計算能力を持つ量子コンピューターは，社会を大きく変える機器として期待されている。世界各国における研究によりその実用化が進む一方で，量子コンピューターは，これまで，解読するための計算に数千年から数万年掛かるといわれていた暗号でも，瞬時に解読してしまう可能性がある。

特に，現在通信路を流れるデータを大量に傍受しておき，大規模な量子コンピューターの完成を待って解読するという攻撃（“Harvest now，decrypt later攻撃”と呼ばれる）が存在し，長期間にわたり機密性を保持する必要のある情報は，今から対策が必要となっている。

このような状況の中，将来にわたって安全な通信を行うための新しい技術として，量子暗号通信が注目されている。

現在の暗号通信では，暗号を解くための秘密の「鍵」（暗号鍵）を，公開鍵暗号アルゴリズムを使って秘匿してインターネットなどで送ることが一般的であるが，量子暗号通信では，暗号鍵を光の最小単位である光子（光の粒子）に乗せて，送信装置から受信装置に光ファイバーなどの光伝送媒体を使って送る。この，光子を用いて暗号鍵を送信する仕組みをQKDと呼ぶ。秘匿された暗号鍵の解読に膨大な

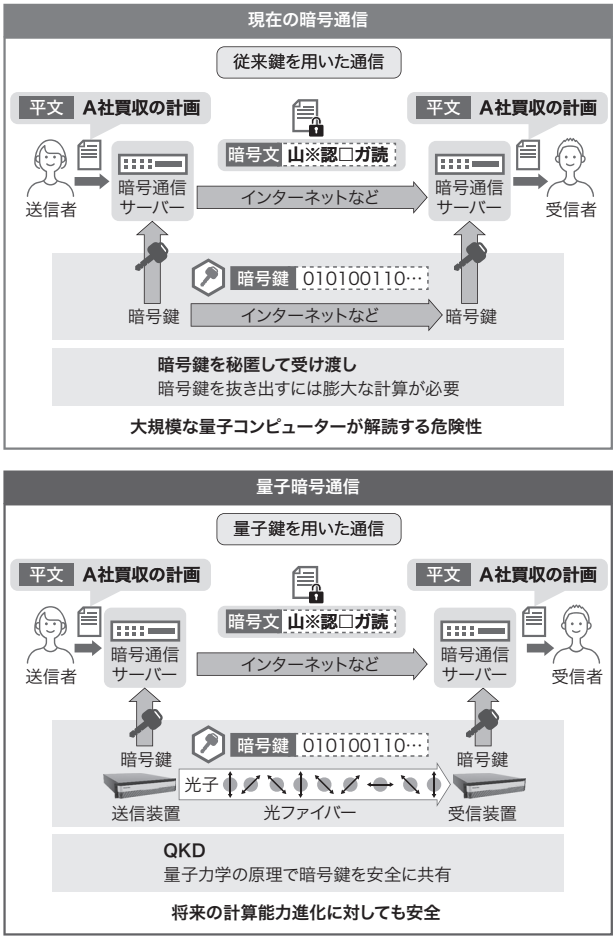

図1. 現在の暗号通信と量子暗号通信における暗号化の比較

現在の鍵配送は，大規模な量子コンピューターによる解読が脅威となるが，QKDは，将来の計算能力の進化に対しても安全である。

Comparison of encryption methods in current encrypted communication and quantum cryptography communication

時間が掛かることで安全性が担保される公開鍵暗号とは異なり，量子力学の原理によって鍵の安全性が無条件に保証されているQKDは，今後，どんなに高速なコンピューターが登場しても，暗号鍵が通信の途中で盗聴者に漏れることがない（**図1**）。

ここでは，量子暗号通信の要である，QKDの原理や，QKDを広域で利用するためのネットワーク化，東芝グループの量子暗号通信技術，社会実装に向けた取り組みと今後の展望などについて述べる。

2. QKDの原理

QKDは，光子の持つ二つの性質を利用して，安全性を保証する。一つは，光子は分割できないという性質である。これにより，盗聴者が光子に乗せた暗号鍵情報を抜き取った場合，その情報が受信者に届くことはなく，盗聴者

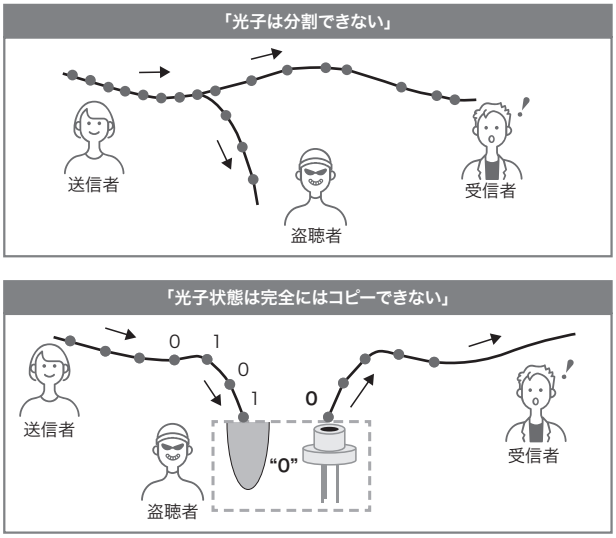

図2. QKDの原理

光子特有の二つの性質を利用することで，盗聴されていないことが保証された暗号鍵を配送できる。

Principle of QKD

が持つ情報を知らずに暗号鍵として利用することは決してない（**図2**の上側）。

もう一つは，光子状態は完全にはコピーできないという性質を用いる。盗聴者が，盗聴を気付かせぬよう，抜き取った光子と同じ光子を受信者に送ろうとしても，この性質から，盗聴者が送信する光子は，送信者が送信した光子と完全に一致させることはできない（図2の下側）。この結果，送信者と受信者が同じ暗号鍵を保持していることを確認すれば，盗聴の可能性を確実に検知できる。

これらの性質から，送信者から受信者に正しく届いた情報だけを暗号鍵として利用することで，この暗号鍵は，盗聴されていないことが保証される。

3. QKDのネットワーク化

2章で述べた原理を用いるQKDは，光子に暗号鍵情報を乗せて送信することから，一般には伝送媒体として光ファイバーが用いられるが，その場合には光ファイバーを介して直接届く相手への送信に限られてしまう。例えば，現在実用的に利用可能なQKDは，光ファイバー長100 km程度が限界となる。

より遠い距離に展開するには，QKDの送信装置と受信装置の対（以下，リンクと呼ぶ）を複数用いて，ネットワーク化を行う。

最も簡単な例を**図3**に示す。これは，ネットワーク化により，拠点Aと拠点Cの間で暗号鍵を共有する例である。拠

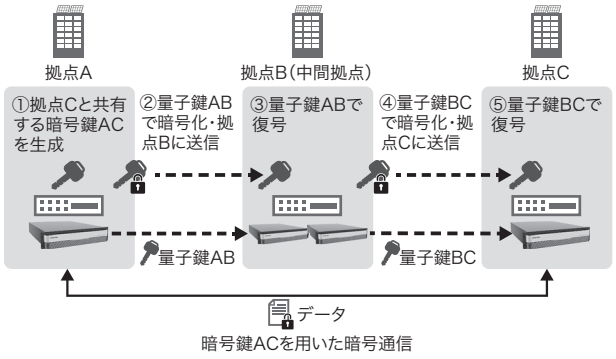

図3. 3拠点をつなぐネットワーク化の例

中継拠点を設けることで，QKDが直接届かない拠点に暗号鍵を配送できる。

Example of networking of three nodes

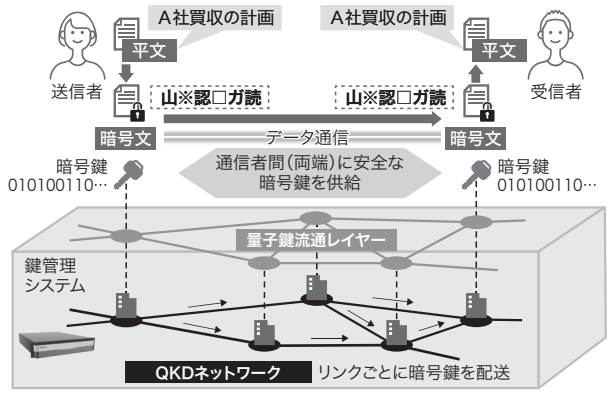

図4. QKDネットワークの拡張

QKDをネットワーク化することで，ネットワークで接続された任意の拠点に安全な暗号鍵を配送できる。

Expansion of QKD network

点Aで生成した暗号鍵ACを，拠点Aと拠点Bのリンクの QKDで配送した量子鍵AB，及び拠点Bと拠点Cのリンクの QKDで配送した量子鍵BCで暗号化し，拠点Cに転送する。このような，QKDのネットワーク化を可能にする暗号鍵転送機能をつかさどるのが，量子鍵流通レイヤーである（この特集のp.13–15参照）。このネットワーク化を拡張すれば，任意の拠点間での暗号鍵共有，暗号通信が可能となる（**図4**）。

4. 東芝グループの量子暗号通信技術

東芝グループは，約20年にわたり量子暗号通信の研究を進め，特に，鍵配送速度（単位時間当たりの暗号鍵配送量）において，世界最高（注1）の性能を維持し続けている。

（注1） 2022年8月現在，東芝デジタルソリューションズ（株）調べ。

この性能は，複数の技術の組み合わせにより実現している。一つは，高速に光子を検出する技術である。光子検出の際に発生するノイズを除去する自己差分型回路技術[1]により，短時間で多くの光子を正しく検出することを可能にしている。

もう一つは，光子検出の結果から，盗聴の可能性を排除した暗号鍵を生成する計算処理の高速化技術である。これは，大規模な行列計算の並列化[2]により実現している。

更に，QKDの動作を安定させる技術も特徴である。光ファイバーを流れる光子の状態は，光ファイバーの周囲環境の影響を受けやすい。例えば，温度変化による，光ファイバーの僅かな伸縮が，QKD動作を止めてしまうこともある。この課題は，光子が流れる通信路の状態を常に監視し，変化が起こればそれを元の安定動作状態に戻す，動的安定化技術[3]により解決している。

このほか，量子暗号通信の適用範囲を広げるために，QKD装置の小型化[4]や，QKDの長距離化[5]などの技術にも取り組んでいる。

5. 社会実装に向けた取り組みと今後の展望

東芝グループは，2020年10月に量子暗号通信の事業化を発表し，2021年4月には，東芝デジタルソリューションズ（株）で事業を開始した。以降，量子暗号通信の社会実装が始まりつつある複数の国で，商用化に向けた取り組みを進めている（この特集のp.25–28参照）。

主要な取り組みの一つが，英国の通信事業者であるBTグループ社とロンドンで開始した商用トライアルである。基幹となる三角形状のQKDネットワークを構築し，そこからユーザーの拠点にリンクを延ばす構想である。多くのユーザーがこの基幹ネットワークを共有して利用できる。

もう一つが，韓国の通信事業者であるKT社との取り組みである。2022年3月に，韓国のソウル特別市と釜山市の間でQKDネットワークの実証試験を行った。この実証結果を生かし，ソウル特別市と大田市をQKDネットワークでつなぎ，QKDサービスのオープンなテストベッドの運用を進める。

図5に，東芝グループが考えるQKDネットワーク発展のステップを示す。これまでは，1リンクを特定のユーザーが利用する形態が一般的であったが，図5(a)や図5(b)に示すように，都市圏，あるいは都市間をつなぎ，複数のユーザーが利用可能なQKDネットワークの実装が始まっている。今後は，利用するユーザー数とともにその規模の拡大を見込んでいる。

また，このようなネットワークにより提供するサービスとして，安全な暗号鍵を広域に提供するサービスや，それを用

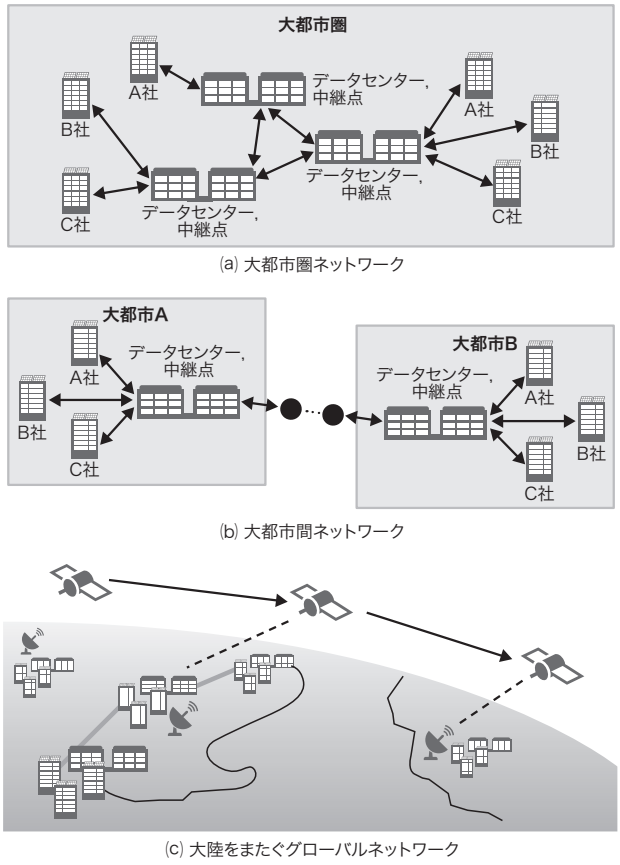

図5. QKDネットワーク発展のステップ

QKDネットワークを徐々に広域化し，最終的にはグローバルなネットワークへと展開していく。

Stepwise development of QKD networks

いた暗号通信ネットワークサービスなど，様々な形態への展開を想定している。これらのサービスを利用するユースケースは，ネットワークと利用者の拡大に伴い，利用のための障壁が下がり，広がりを見せるものと考えられる。

ネットワークの規模も，衛星QKD技術の進展とともに，更なる広域化が可能であると考える。図5(c)に示すように，衛星を用いたQKDと組み合わせることで，大陸をまたがるグローバルネットワークへの展開を目指していく。

6. あとがき

量子コンピューターの急速な発展により，コンピューターの進化に対しても安全な量子暗号通信が注目を集めている。東芝グループは，長年培ってきた量子暗号通信技術の事業化を開始し，複数の国で，社会実装を開始している。今後は，QKDネットワークをサービスとして，世界に幅広く展開していく。

文　献

(1) Comandar, L. C. et al. Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm. J. Appl. Phys. 2015, **117**, 8, 083109.

(2) Takahashi, R. et al. "Practical Implementation of Privacy Amplification in Quantum Key Distribution". 9th International Conference on Quantum Cryptography (QCrypt 2019). Montreal, Canada, 2019-08, QCrypt. 2019, Poster 77.

(3) Dynes, J. F. et al. Stability of high bit rate quantum key distribution on installed fiber. Opt. Express. 2012, **20**, 15, p.16339–16347.

(4) Paraïso, T. K. et al. A photonic integrated quantum secure communication system. Nature Photonics. 2021, **15**, 11, p.850–856.

(5) Pittaluga, M. et al. 600-km repeater-like quantum communications with dual-band stabilization. Nature Photonics. 2021, **15**, 7, p.530–535.

村井　信哉　MURAI Shinya
東芝デジタルソリューションズ（株）
ICTソリューション事業部 QKD事業推進室
電子情報通信学会・情報処理学会会員
Toshiba Digital Solutions Corp.