

本件は、東芝欧州社が 6 月 6 日（英国時間）に発表したニュースリリースを抄訳したものです。

2023-6-6

Toshiba Europe Limited

東芝欧州社と仏オレンジ社が、
既存のネットワークやサービスでの量子鍵配送の実現可能性を実証
高出力な多数のデータ通信チャンネルで稼働する既設光ファイバー上に QKD サービスを提供
可能

東芝欧州社と世界的な通信事業者であるオレンジ社は、量子コンピューターによる解読から伝送を保護するために、既存の商用ネットワークに量子鍵配送（Quantum Key Distribution、以下 QKD）の導入が可能であることを実証しました。



今回発表された研究論文では、東芝の商用 QKD 技術を用いた共同実験の結果、ネットワークプロバイダーの既存の光ファイバーネットワーク上で、現行のデータサービスとともに QKD 技術を導入することが可能であることを示しています。これにより、ネットワーク事業者は、専用の量子ファイバーインフラに投資する必要がなくなり、QKD の導入コストを削減することができます。

量子コンピューターの進化と実用化は、現在の公開鍵暗号方式を危うくさせるリスクを伴います。東芝の QKD は、データの暗号化・復号のための安全な乱数鍵を、光の量子的性質を利用して生成するもので、将来の量子コンピューターの力に対抗するために開発されま

した。

従来 QKD の導入には、ネットワーク事業者が量子情報送信専用のファイバーをネットワーク全体に敷設する必要があり、導入までにコストと時間がかかっていました。波長分割多重 (Wavelength Division Multiplexing、以下 WDM) と呼ばれる技術は、スペクトル分離 (異なる波長の光を利用して干渉を避けること) を利用して、量子信号と通信事業者の通常のデータ信号を共存させることにより、既存のファイバーネットワーク上で QKD を運用することを可能にしています。しかし、これまでのテストでは、データチャネルの可能な数と電力、ネットワークの有効距離、セキュアビットレート (セキュアキーレートまたは SKR と呼ばれることもある) などにおいて、実行可能性に影響を与える問題が示されました。

2022 年から 2023 年にかけて、東芝とオレンジ社は、フランスのラニオンにあるオレンジ社の研究所で、QKD と既存データ信号の共存を検証し、データサービスを実行している既存のファイバーネットワーク上で既存の信号と量子信号の両方を送信する際の効率に異なる要因がどう影響するかを調査しました。

東芝とオレンジ社の研究者は、実験を通じて、高いビットレートで既存の信号と量子信号を効果的に重畳伝送させることを実証しました。また、両者を共存させながら最大 70km の距離で効果的に鍵を届けることができることを示し、ビル街のメトロネットワークでの展開に大きな可能性を示唆しました。

また、このようなシステムの効率を測定するための新たな知見も得られました。この指標に基づき、新しい QKD の実装は、これまでの実験を凌駕するものであると判断されました。

Orange Innovation の光通信シニアエキスパートである Paulette Gavignet 氏は、「今回の成果は、運用中の WDM リンクのエンジニアリングルールを変更することなく、量子チャネルと WDM データチャネルを同一ファイバー内で重畳伝送させることができることを示すものです。この構成で得られた秘密鍵の高い送信レートは、事業者のネットワークに QKD を導入する上で非常に有望です」と述べています。

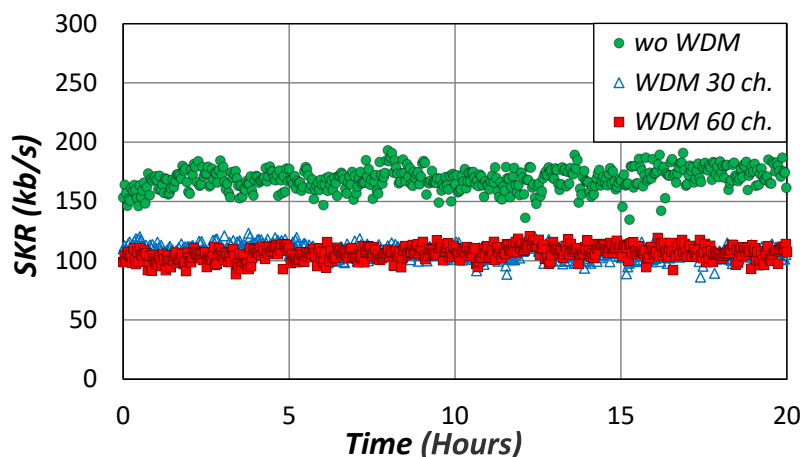
Orange Innovation Networks のグループ CTO 兼 SVP である Laurent Leboucher 氏は、「セキュリティとイノベーションへの取り組みにより、当社は量子鍵配送 (QKD) ソリューションの限界に挑戦しています。これは、光伝送ネットワークに比類なき保護を提供するキーとなり得るものです。東芝との共同研究で、専用ファイバーを使用することなく、通信事業者のネットワークに新しいセキュリティ機能を導入することが可能であることを示しました。この費用対効果の高いアプローチによって、私たちはデジタル要塞への道を開き、顧客の最

も貴重なデータのセキュリティを保証することができます」と述べています。

東芝量子テクノロジー事業部長の Dr. Andrew Shields は、「量子コンピューターの台頭は、現在のセキュリティ手法に深刻な影響を与えるものであり、組織は通信に対するリスクを軽減するために今すぐに行動を起こす必要があります。当社の QKD 技術で、既存のファイバーネットワークを利用しながら通信を保護する能力を検証したことは、量子的な安全性を持つ通信を現在の組織で利用できるようにするための大きな前進と言えます。オレンジ社のようなグローバルな事業者と協力して研究を行い、当社の技術を向上させることは極めて重要であり、この分野での研究を継続することを楽しみにしています」と述べています。

研究者らは、1,310nm の量子チャネルを、東芝商用 QKD システムを用いて、通信用 C バンドで最大 60 個のデータチャネル（各チャネルのビットレートは 100Gb/s）を多重化するデモを行い、評価しました。QKD の優れた性能を維持しながら、データを多重化することができたのは、量子信号の分離と従来チャネルから侵入するノイズの低減を図るための新規設計によるものです。

テストは、20km、50km、70km のファイバー長で、30 および 60 の多重化チャンネルで実施されました。研究者らは、システムが既存のデータチャネルと一緒に量子鍵をどれだけ効果的に伝送できるかを理解するために、異なる距離でセキュアビットレート (SKR) とデータサービスの光出射パワーを測定しました。

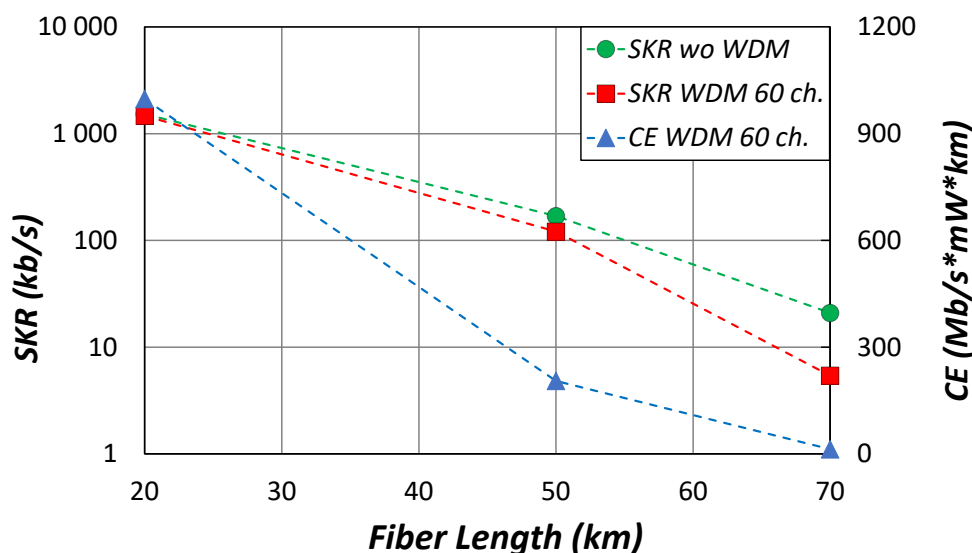


WDM を採用することで SKR は低下するが、チャンネル数の影響は少ないことを示すグラフ

テストの結果、今回の評価で使用した WDM チャンネル数が多くても（最大 60 データチャネル）、SKR への影響はほとんどないことがわかりました。その代わりに、システムで使

用されたデータチャンネル光出射パワーが、SKR と鍵の正常な配信に最も影響する要因であることが明らかになりました。その結果、Orange と東芝は、既存チャンネルの総パワーと伝送距離を考慮しながら、重畳伝送方式における QKD システムの性能（良好な SKR で安全な鍵を配送する能力）を推定できる新しい指標「重畳伝送効率（Co-propagation Efficiency, CE)」を提案しました。

この論文では、高い光出射パワーで大量の既存データチャンネルが QKD と共存できることを実証しました。つまり、東芝の QKD システムは、既存のオペレータネットワークで、現在のデータサービスと組み合わせて使用でき、QKD サービスへの投資と維持に必要なコスト、および導入までの時間を劇的に削減できるのです。



新メトリクス「Co-propagation Efficiency (CE)」が、SKR と同様に距離に応じて減少することを示すグラフ

この結果は、量子コンピューターによる攻撃から通信を保護するために QKD を利用することが、商業レベルで実現可能であることを示す 2 つの重要な示唆を与えています。第一に、東芝とオレンジ社が評価した商用の装置は、QKD を現在のファイバーネットワークでより効果的に展開することに成功していることを示します。第二に、研究者らが開発した新しい指標は、効率に最も影響を与えるのはチャンネル数ではなくパワーであることを確認し、事業者がネットワークやサービスの計画を立てる際に役立つと考えられます。

この結果を受けて、東芝、オレンジ社をはじめとする QKD の導入を検討している企業は、

既存のファイバーネットワーク上で QKD を導入することが可能となり、サイバーセキュリティの重要な形態である QKD の導入コストを削減することができるようになるでしょう。

ニュースリリース全文（英語）は、

<https://www.toshiba.eu/quantum/news/toshiba-europe-and-orange-demonstrate-viability-of-deploying-quantum-key-distribution-with-existing-networks-and-services/>

をご覧ください。

研究論文の全文は、

<https://arxiv.org/abs/2305.13742>

をご覧ください。

東芝の QKD サービスおよび量子技術に関する詳細は、

<https://www.toshiba.eu/quantum/>

をご覧ください。

以上