東芝の量子暗号通信技術の研究開発

Research and development of Toshiba quantum cryptography

東芝研究開発センター　鯨岡 真美子

Toshiba R&D Center Mamiko Kujiraoka

E-mail: mamiko.kujiraoka@toshiba.co.jp

近年のサイバー攻撃の高度化に伴い、サイバーセキュリティの重要性が増している。さらに、量子コンピュータの研究開発が加速しており、2030 年ごろには実用的な規模の量子コンピュータが登場するとの予測がある。現在の暗号通信で広く利用されている公開鍵暗号技術 (RSA 等) は、量子コンピュータを使うと短時間で破られる可能性がある。また、今すぐ暗号が破られる恐れがなくとも、暗号化されたデータを傍受して保存しておき、時間をかけて解読する攻撃も存在するため、現在通信されている暗号化データも将来的に破られる危険性がある。そこで、量子コンピュータでも破られない次世代のセキュリティ技術として注目を集めているのが量子暗号通信である。量子暗号通信は、量子力学の原理に基づく暗号通信技術で、計算の難しさを安全性の根拠とする既存の暗号技術とは異なり、物理的な理論で安全性が証明されており、将来にわたって破られる危険性が無い暗号通信技術として知られている。

東芝では、量子暗号通信の研究開発に長年従事し、微弱光の検出技術、ソフトウェアの高速化技術、安定性向上技術を中心とした研究開発の成果として、鍵配送速度・安定性・相互運用性の高い量子暗号装置の開発に成功し、フィールド実証の実績を数多く積み重ねてきた。

本講演では、東芝の量子暗号通信技術の特長と、長距離化を含めた最近の研究開発の取り組みについて紹介する。

（謝辞）

本研究の一部は，内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP)「光・量子を活用した Society 5.0 実現化技術」（管理法人：量研）によって実施されました。