令和　6年　3月　1日

報 道 機 関　各位

光の不完全な乱雑化の問題解決による量子鍵配送の安全性向上

■ 概要

スペインのヴィーゴ大学 マルコス・カーティー教授の研究グループ、カナダのウォタルー大学 ノバート・ルトケンハウス教授の研究グループは、富山大学学術研究部工学系の玉木潔教授との共同研究により、実際の量子鍵配送※1装置の安全性を向上させる方法を提案しました。

量子鍵配送は量子力学の原理を利用することにより如何なる盗聴からもユーザー間の通信を保護する究極の暗号として期待されている次世代暗号方式です。この如何なる盗聴からの保護という究極の安全性を達成するためには、量子鍵配送の安全性理論※2が課す条件を実際の量子鍵配送装置が満たす必要があります。しかし、これらの条件全てを実際の量子鍵配送装置が満たすのが非常に難しいということが問題でした。特に高速通信においては、光変調器※3が光パルス※4に施した位相変調※5がその後に続く光パルスへの位相変調にも影響を与えてしまう位相相関と呼ばれる効果が大きな問題となっていました。

今回我々の研究では、BB84 などの代表的な量子鍵配送方式において使用される囮法※6において位相相関などの不完全性が存在する下でも、量子鍵配送を安全に行う新手法を提案しその方法の安全性を厳密に証明しました。本研究の成果により、実際の量子鍵配送の安全性がさらに向上することになります。

本研究成果は科学誌 Quantum Science and Technology に 2023 年 12 月 22 日に掲載されました。

■研究の背景

現代の生活においてインターネットは非常に便利で欠かせないものとなっていますが、その一方でインターネット上に流れる情報が第三者（盗聴者）によって不正に盗まれてしまい悪用される危険性があります。例えば、インターネット上での買い物の際にはクレジットカードなどの重要な個人情報などを送信しますが、その情報が洩れては大変なことになります。このような盗聴によるリスクは暗号によって避けることができますが、暗号の中でも最も安全性の高く究極の暗号として期待されているのが量子鍵配送（または量子暗号とも呼ばれる）です。安全性を数学の問題の困難さに置いていた従来の数理暗号とは違って、光子と呼ばれる光の粒などの非常に小さなものがもつ量子性と呼ばれる不思議な性質を上手く用いて情報を守るのが量子鍵配送です。

このように次世代の暗号として期待できる量子鍵配送ですが、量子鍵配送通信を行う実際の装置には雑音などの不完全性があり、これを盗聴者に利用された場合の安全性を保証できない、という問題がありました。

【本発表資料の配信元】富山大学総務部総務課広報・基金室 (TEL)076-445-6028 (FAX)076-445-6063

■研究の内容・成果

上記の背景の下、今回我々の研究では BB84 などの代表的な量子鍵配送方式において広く使用される囮法に注目しました。この囮法では、それぞれの光パルスの位相と呼ばれるものを位相変調器により、独立にかつ完全に乱雑化することが要求されますが、この独立かつ完全な乱雑化は実際に実現することは非常に困難です。特に高速通信においては、光の状態を操作（変調）する装置を非常に高速に動作させるため、ある光パルスへの操作がそれに続く光パルスへ影響を与えてしまう相関の問題があり、独立性が失われてしまいます。

我々はこの相関をはじめとする不完全をどのように取り除くか、というアプローチではなくこれらの不完全性が存在することを前提とした新しい安全性理論を開発することによりこの問題を解決しました。

■今後の展開

今回の対策は理論的な提案であるので、これを実際に実装するための研究を今後行う予定です。

■用語解説

※１　量子鍵配送

量子暗号とも呼ばれる。量子力学の原理を利用することにより如何なる盗聴からもユーザー間の通信を保護する究極の暗号として期待されている次世代暗号方式。

※２　量子鍵配送の安全性理論

量子鍵配送が安全であるか否かを検証するための理論のこと。

※３　光変調器

量子鍵配送はじめ、光通信では送信したい情報に応じて光の状態を変化させる必要があるが、これを行うのが光変調器と呼ばれる素子。

※４　光パルス

狭い範囲に存在する光のこと。

※５　位相変調

光の状態を特徴づける量の一つ位相と呼ばれるパラメータがあり、このパラメータを変えることを位相変調と呼ぶ。

※６　囮法

量子鍵配送がもつ欠点の一つとして、通信距離が短いことが挙げられる。この問題を解決する方法が囮法で、量子鍵配送システムで広く使われている。

【論文詳細】

論文名：Security of quantum key distribution with imperfect phase randomization

著者：Guillermo Currás-Lorenzo, Shlok Nahar, Norbert Lütkenhaus, 玉木　潔, Marcos Curty

掲載誌：Quantum Science and Technology

DOI： https://doi.org/10.1088/2058-9565/ad141c

【本発表資料のお問い合わせ先】
富山大学学術研究部工学系
教授 玉木　潔
TEL：076－445－6747　Email：tamaki@eng.u-toyama.ac.jp