量子が拓く新たな情報セキュリティ

～量子暗号の概要と量子セキュリティ拠点の紹介～

概要

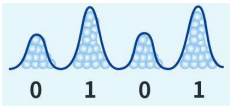
NICTは、内閣府が定める量子セキュリティ拠点として、
量子情報通信を活用した量子暗号の研究開発を通じて
新時代の安心・安全を社会へ届ける活動をしています。

【量子】

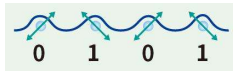
「量子(りょうし)」は、粒と波の性質を持つ、これ以上小さくできない物質やエネルギーの単位のことです。例えば、極限まで弱めた光も量子であり、「光子(こうし)」や「光量子(こうりょうし)」と呼ばれます。

【情報通信と量子】

コンピュータやインターネットで情報通信の技術(ICT)は重要です。現在、0と1の情報は電流や光の強弱によって表現されています。代わりに、量子の状態に基づいて情報を表すのが「量子情報通信」です。



情報通信の「0と1」

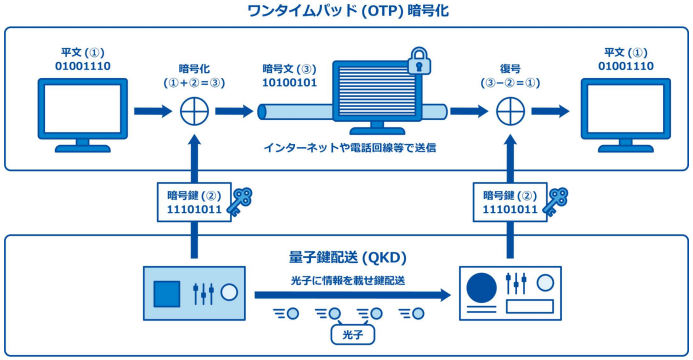


量子情報通信の「0と1」

【量子暗号】

量子の状態に基づいて暗号に必要な「暗号鍵」と呼ばれるデータを安全に共有する技術を「量子鍵配送（QKD）」と言い、この暗号鍵を使用して行う暗号通信が「量子暗号」です。

「ワンタイムパッド」という方式を用いて暗号文を作成すると、暗号鍵を持つ送信者と受信者以外からは理論上絶対に解読ができない暗号通信を実現することができます。



量子コンピュータの計算能力や量子暗号の安全性をはじめとして、
従来の情報通信では出来なかったことの実現が量子情報通信の活用に期待されています。

特徴

- 「量子」の情報通信への応用
- 絶対に解読できない暗号通信

ユースケース

- 漏らしてはいけない重要データを安全に送り届ける
- 次世代通信技術と量子鍵配送の組合せ
- 完全秘匿通信にとどまらない、量子暗号の多機能化

今後の展開

- 量子暗号の長距離・大容量伝送などの技術向上
- 量子暗号を活用した新しいネットワークの研究開発

【お問合せ先】
量子ICT協創センター（https://www2.nict.go.jp/qictcc/）
Mail : qictcc-info@ml.nict.go.jp