



WDMを用いて量子暗号通信をやってみた！

Quantum Key Distribution



Question

量子暗号通信

って聞いた事ありますか？





初めて



聞いた事ある



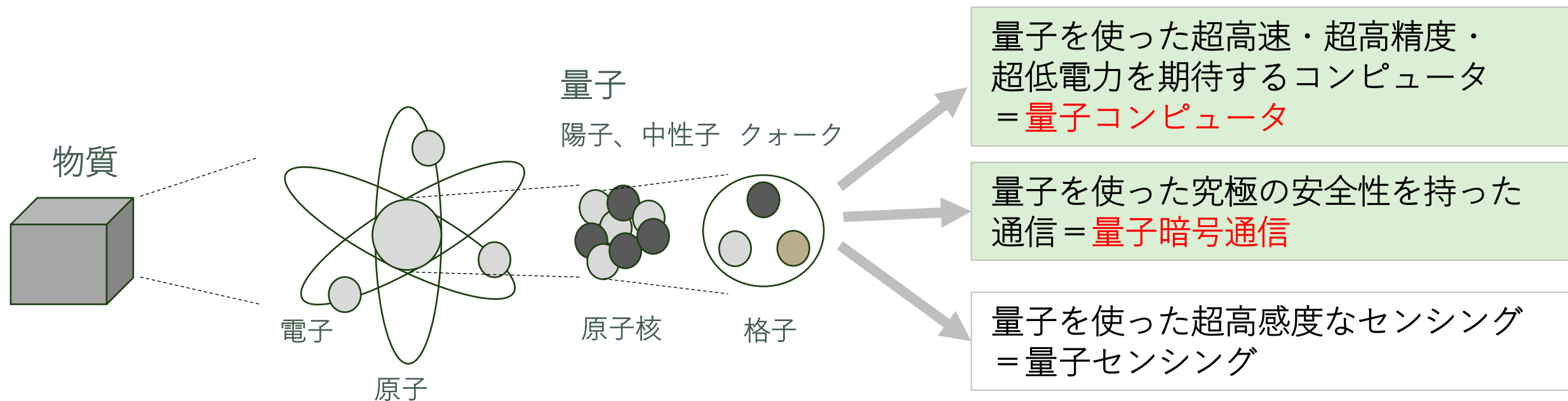
結構
知ってる

今日皆さんに持ち帰って欲しいこと **2つ**

1.量子コンピュータとは何か？

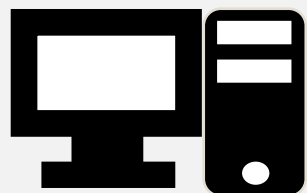
2.量子暗号通信の重要性

◆2019年10月グーグルは、量子コンピュータが世界最速のスーパーコンピュータでも1万年かかる問題を200秒で解くことに成功したと発表



量子とは、粒子と波の性質をあわせ持った、とても小さな物質やエネルギー
※世の中の全てのものはミクロにみると量子

◆量子は複数の状態を同時に持つ！

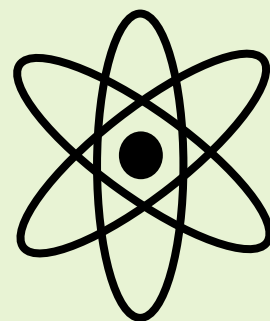
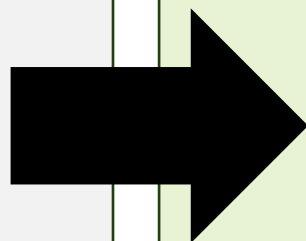


古典コンピュータ

0 または 1

ビット

0か1どちらかを持つ



量子コンピュータ

量子ビット

0か1を同時に持つ

=重ね合わせ

進化するサイバー攻撃の脅威

将来への備え

今後発生し得る量子コンピューターによる暗号解読
現在広く利用されている
暗号アルゴリズムを短時間で破る可能性
大規模な量子コンピューターが完成する前に対策が必要

現在の課題

データ・ハーベスティング

- ・ 暗号化されたデータを傍受し保存しておき、時間をかけて解読する攻撃
- ・ 現在の通信データも将来解読される可能性

量子コンピューターに対抗できるソリューションが今から必要
量子力学に基づく新しいセキュア通信 = 「量子暗号通信」



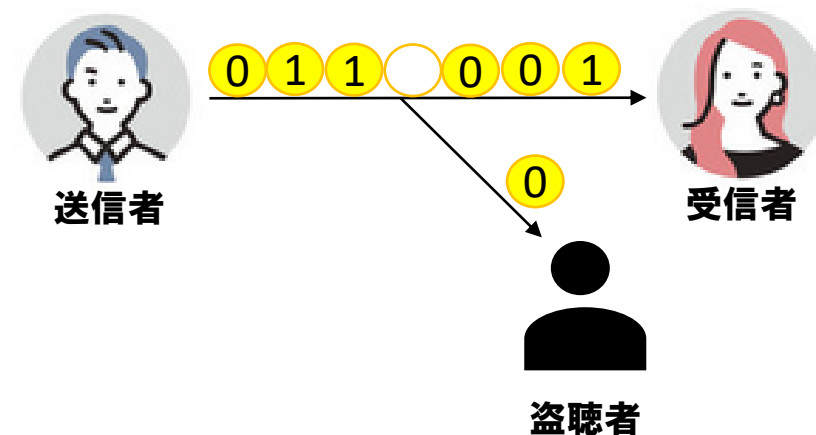
暗号鍵を分割して量子の一種である「**光子**」（光の最小単位）に載せて送ること

“光子”の量子的ふるまいに基づき、盗聴されていないことが保証された「暗号鍵」を共有する。

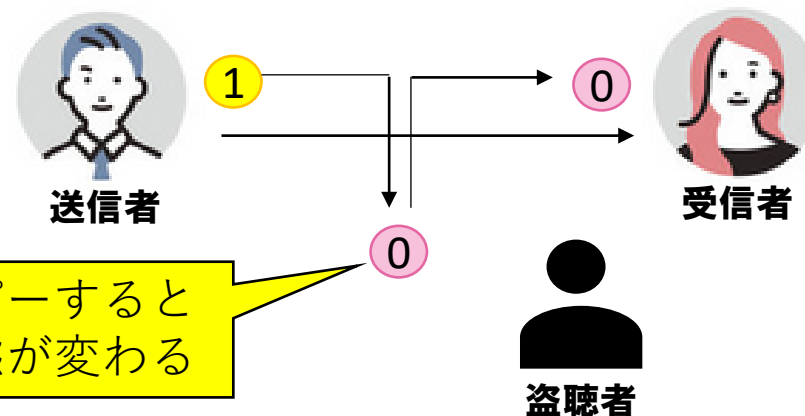
“光子”の特殊なふるまい（**分割できない、コピーできない**）を利用し、「盗聴」を検出する。

これにより、**解読できない暗号通信**を実現している。

1) 光子は分割できない
⇒ 数が減ったら盗聴されている証拠



2) 光子は完全にコピーはできない
⇒ 光子の状態は変化したら盗聴の疑いあり



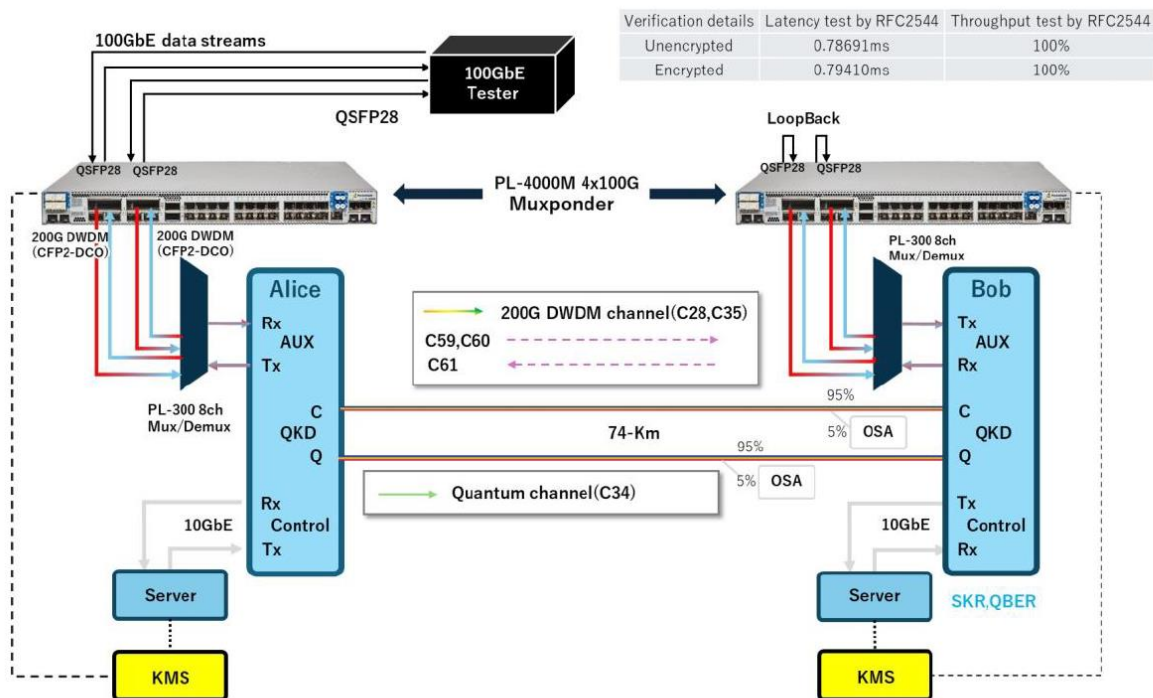
量子暗号通信の実証実験をやってみました！



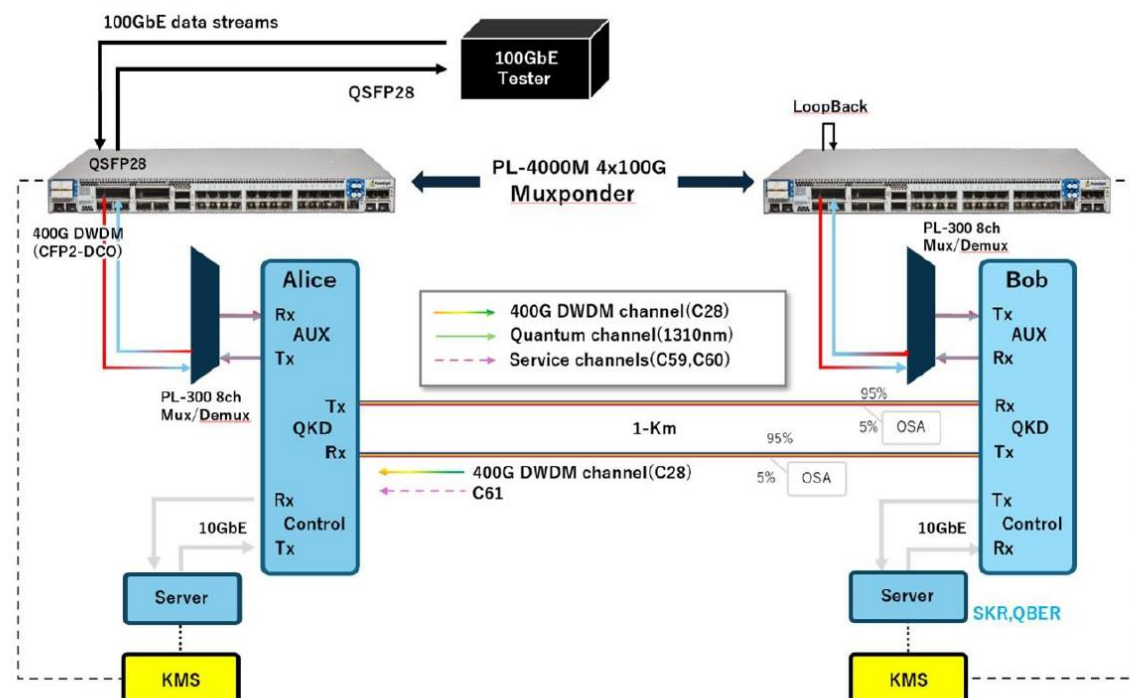
- 実証実験で、東芝デジタルソリューションズ社様協力のもと、**QKDシステム**を使用！
- 暗号通信装置にはPacketLightの光レイヤ暗号装置を用いて、400G波長のデータ信号と量子チャネルを多重化！

※**Quantum Key Distribution; QKD** 量子鍵配送とは、光ファイバー伝送路において、1ビットあたり1個の光子に鍵情報を載せて伝送することで、2者間で安全に暗号鍵を共有する技術。盗聴を検知・防止できる。

- 2024年2月に行われた国立研究開発法人情報通信研究機構（NICT）主催の雪まつり実験において、札幌と沖縄の2会場で実施
- 従来のDWDMデータ信号とQKDを同時に伝送し、QKD暗号による量子セキュアなデータ伝送を実証



沖縄での長距離QKDリンク構成図



札幌での多重QKDリンク構成図

QKDと光ネットワークインフラとの互換性を検証し、その実用性を示した

結果・まとめ

QKD技術で伝送される暗号鍵と従来のデータ通信が同じ光ファイバー上で伝送されることを実証し、QKD技術導入のために**新たに光ファイバーを用意することなく**、既存光ネットワークに容易に導入できることを示した！

量子暗号通信を適用しても従来のシステムと比較して遜色のない**通信速度**や**低遅延性**が維持できることを確認



Thank you

ご清聴ありがとうございました



www.packetlight.jp/



packetlight@iland6.com