PacketLight™ NETWORKS

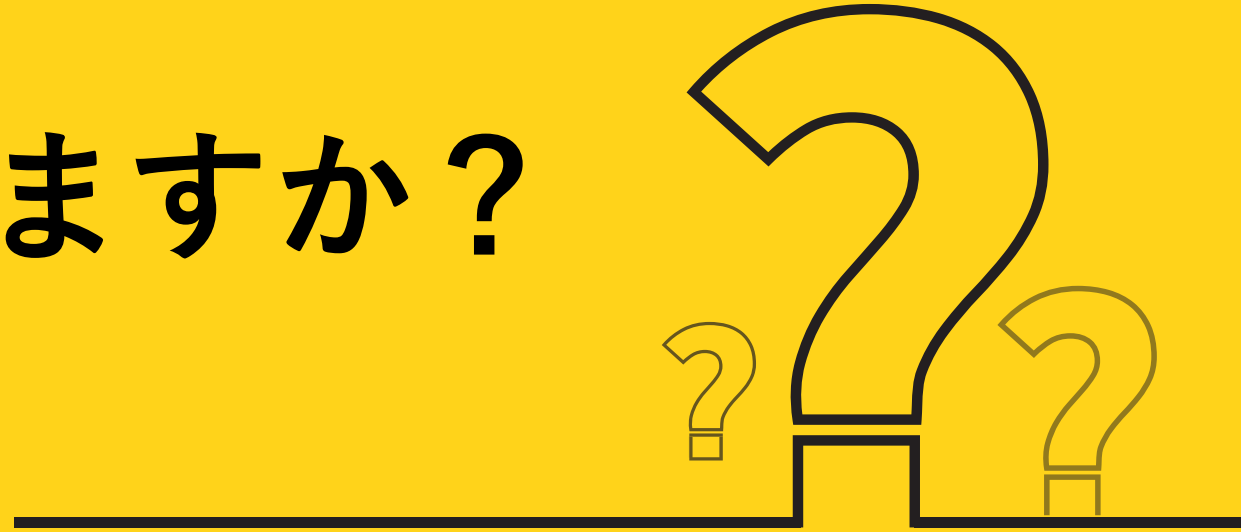
量子技術

～量子コンピュータと量子暗号通信～

PacketLight NETWORKS

Question

量子コンピュータ、量子暗号通信って聞いた事ありますか？



PacketLight NETWORKS

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

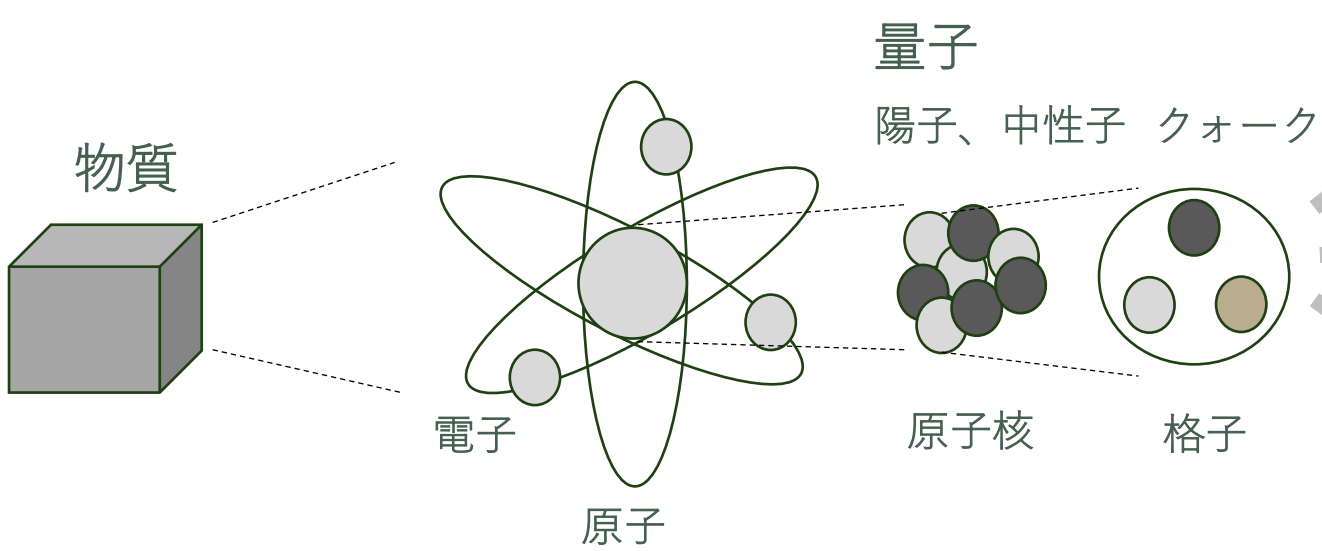
1.量子コンピュータとは何か？

2.量子暗号通信の重要性

PacketLight™ NETWORKS

量子コンピュータとは何か？

◆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



量子を使った超高速・超高精度・超低電力を期待するコンピュータ＝量子コンピュータ

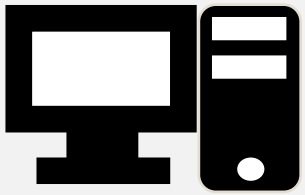
量子を使った究極の安全性を持った通信＝量子暗号通信

量子を使った超高感度なセンシング＝量子センシング

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

量子コンピュータとは何か？

◆量子は複数の状態を同時に持つ！

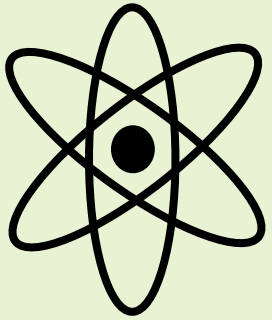


古典コンピュータ

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

量子コンピュータと古典コンピュータ

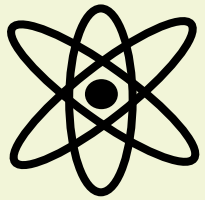
◆量子の性質で数億、数兆通りであっても
全ての　組合せを同時に探索できる！

古典コンピュータ

10億回計算

000000000000000000000000000000
000000000000000000000000000001
000000000000000000000000000010
000000000000000000000000000011

11111111111111111111111111111111



量子コンピュータ

同時に計算

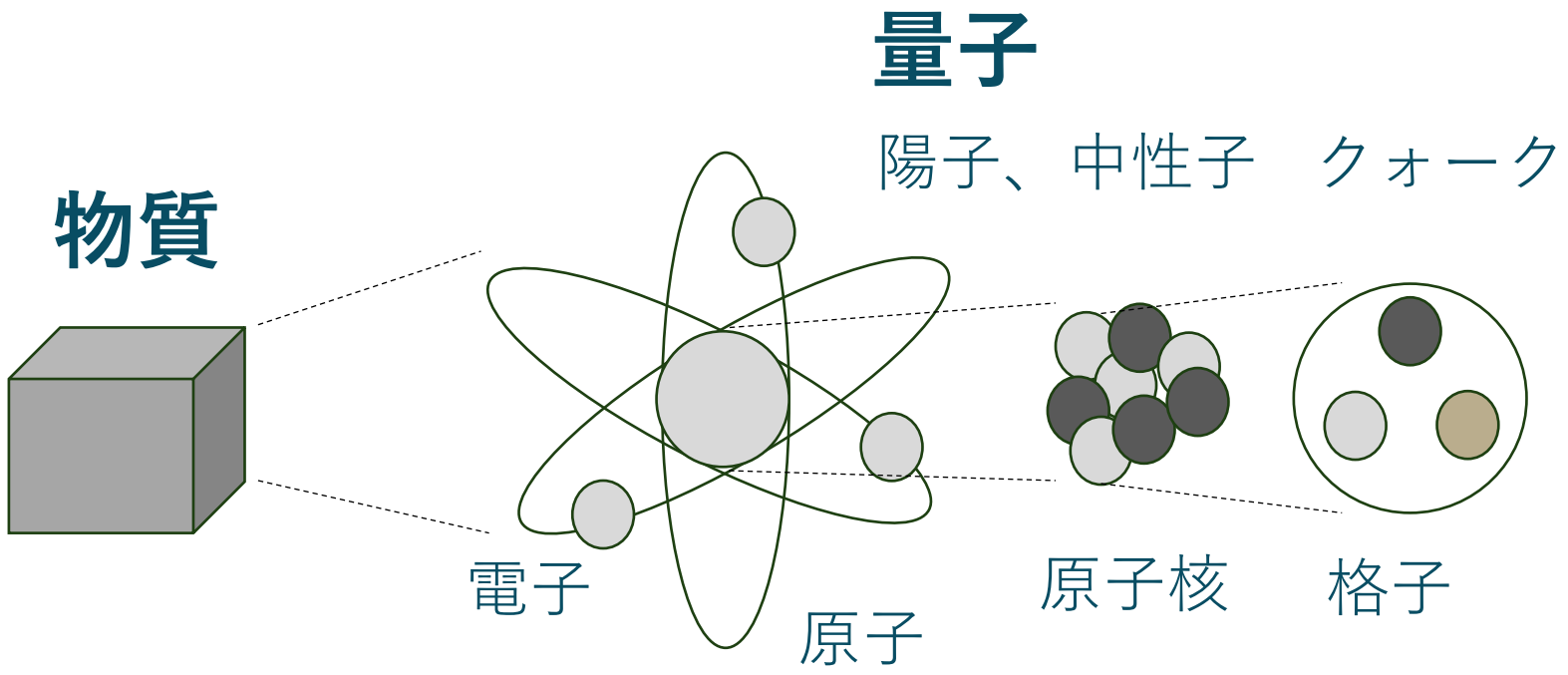
11111111111111111111111111111111

30量子ビットなら
10億通りを同時に探索

量子力学について

量子とは？

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



PacketLight NETWORKS

量子力学について

量子とは？

	0	1	重ね合わせ
古典ビット	0	1	N/A
量子ビット	0	1	0

量子暗号通信が必要となる背景とは何なのか？

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」

量子暗号通信ついて

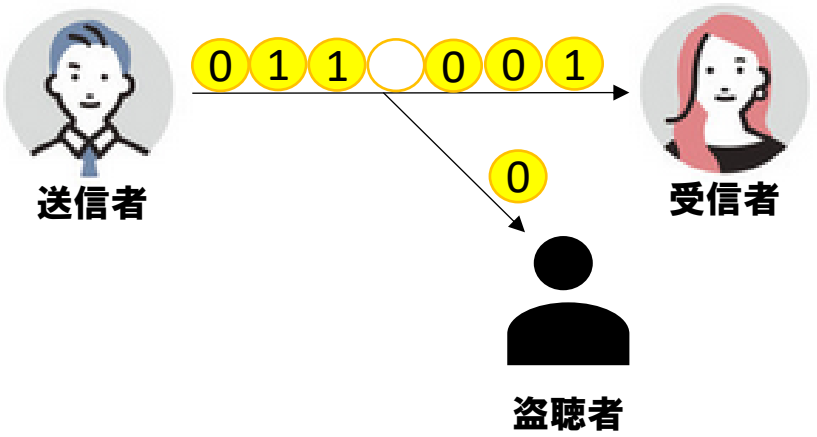
暗号鍵を分割して量子の一種である「光子」（光の最小単位）に載せて送ること

“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。

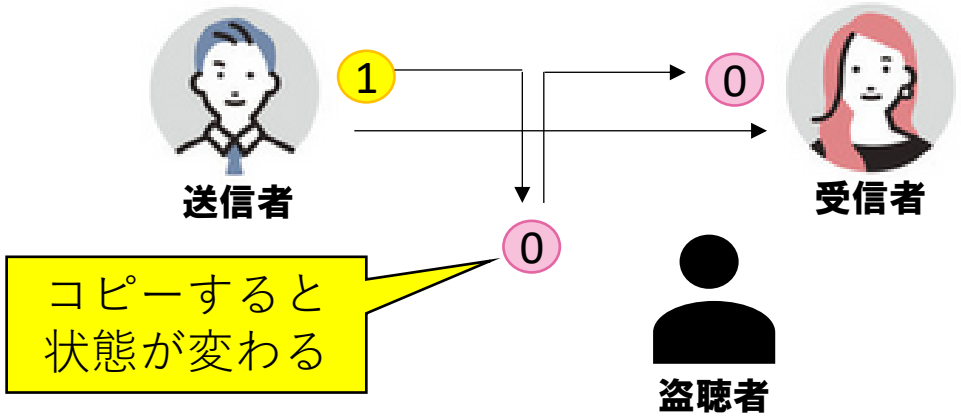
“光子”の特殊なふるまい（分割できない、コピーできない）を利用し、「盗聴」を検出する。

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



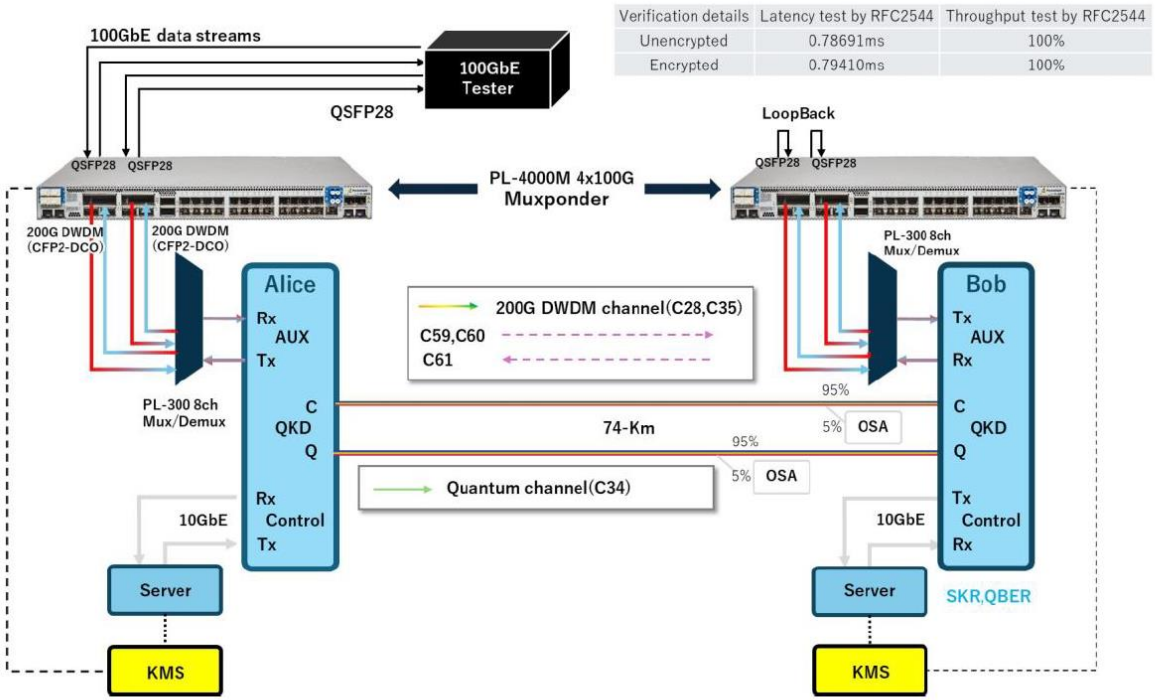
量子暗号通信の実証実験をやってみました！

- 実証実験で、QKDシステムと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。

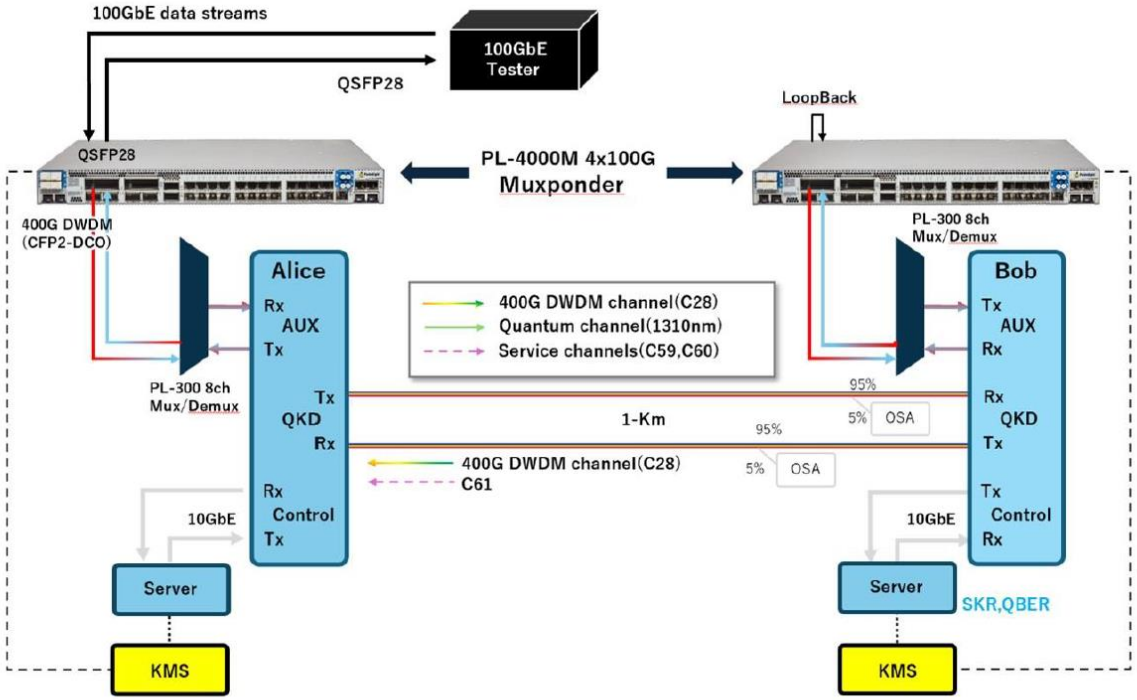
DWDMリンク上でQKDの実用化に向けた実証実験に成功

- 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



Verification details	Latency test by RFC2544	Throughput test by RFC2544
Unencrypted	0.78691ms	100%
Encrypted	0.79410ms	100%

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

◆国産量子コンピュータ

- 1号機 理化学研究所(64量子ビット)
- 2号機 富士通(64量子ビット)
- 3号機 大阪大学(64量子ビット)

◆量子コンピュータ関連のサービス

- AWS - Amazon Braket
- 理化学研究所 –
  「量子計算クラウドサービス」
- Azure Quantum –
  量子クラウド コンピューティング サービス
- エクイニクス&Oxford Quantum Circuits –
  「 32量子ビットコンピュータ「OQC Toshiko 」

◆量子技術を学べる場所

・NICT Quantum Camp※2024年度の応募は締め切り

- 量子ICTの人材育成を効果的・効率的に進める量子ICT人材育成プログラム
- 社会人も参加可能

・Q-Quest※2024年度第２回9月初旬申し込み

- 量子技術リテラシー人材の育成と、オープンイノベーションの創発を目的とした人材育成プログラム(9月12日説明会)
- 社会人も参加可能

Thank you

ご清聴ありがとうございました

www.packetlight.jp/

packetlight@iland6.com