宇宙物理・数理科学研究室　　Astrophysics & Mathematical Sciences

量子鍵配送（E91プロトコル）

情報ゼミ（3年）文献報告レポート　B22-088　三村歩

1.調査の動機

企業間量子暗号ネットワーク及び運用試験の概要

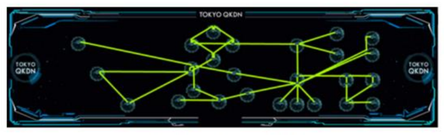


図 テストベッドのネットワーク監視画面

NICTでは、2010年に安全な鍵供給を可能とする量子鍵配送ネットワークとして東京圏にQKDネットワーク【東京QKDネットワーク】を形成、運用を続けてきました。さらに、重要情報を安全に長期保管し利活用する仕組みとして、東京QKDネットワーク上に秘密分散技術を組み込んだ量子セキュアクラウドを開発し、以降、現在に至るまで運用しながら様々な技術実証やアプリケーションの開発を行ってきました。

今回、様々な社会課題の解決に向け、複数の企業拠点を結んで東京QKDネットワークを拡張するとともに、量子インスパイアードコンピュータと呼ばれる計算エンジンも組み込み、安全に試験利用できる環境を企業間量子暗号ネットワークテストベッドとして整備しました。これらの試験環境を複数の企業で連携し活用していくための運用試験を開始します。運用試験を通じて、企業が活用する際の課題及び多くの企業が連携活用する際の課題を抽出するとともに、従来インフラとの親和性/責任分界点のバランスなどの設計についても検証を行います。

●量子鍵配送とはなんなんだ？

参照:https://www.nict.go.jp/press/2023/12/18-1.html

２－１．現代の通信の安全性

RSA暗号　　→　　公開鍵暗号方式

$A^{ed} \equiv A(mod\ n)$　A…送りたいデータ

e, nの値を公開鍵に

$ed = (p-1)(q-1)v + 1$　v…任意の整数

nを秘密鍵に

$e = pq$　　p, q…素数

２－２　公開鍵暗号の限界？

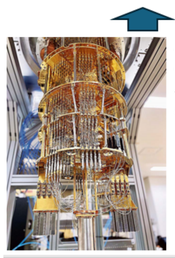
参照:https://dempa-digital.com/article/506461

秘密鍵dを求めるにはpとqが必要

⇒公開鍵nを素因数分解する必要がある

現代のRSA暗号の公開鍵は2048bit=617桁が一般的

⇒解読に膨大な時間がかかる



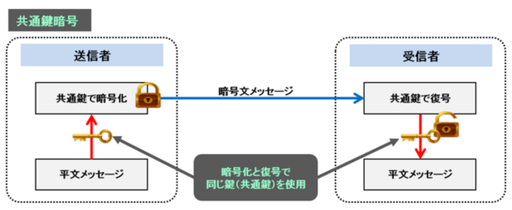
量子コンピューターであれば、現実的な時間で解決できる……!?

RSA暗号も絶対安全とはいえない。
そこで量子暗号が登場する

3.量子通信とは？

https://jprs.jp/glossary/index.php?ID=0227

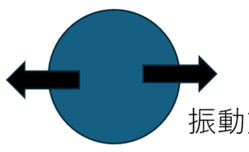
・共通鍵暗号方式
・暗号・復号はワンタイムパッドを用いて行う
・従来の共通鍵の配送問題を克服するために、鍵共有に量子もつれを利用したE91プロトコルを採用
・絶対に盗聴を検知することができる



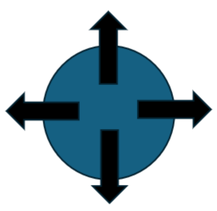
４－１.光子の性質(1)

青い丸は量子のひとつ、偏光状態の光子である。
黒い矢印は、光子の振動方向を表す。


振動方向:垂直

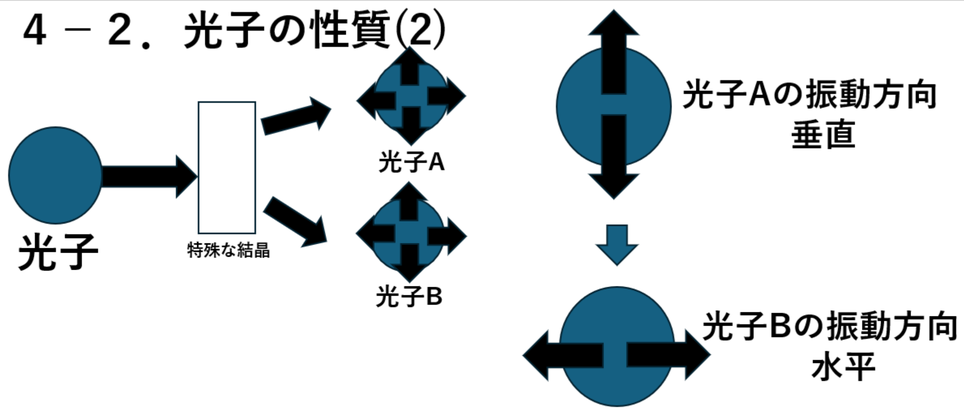

振動方向:水平

光子を特殊なフィルターを通すと、ろ過されるように同じ進行方向の光子が飛び出てくる。



光子には、「観測するまで垂直か水平に振動しているかわからない」という状態をとることができる。
これが重ね合わせ（量子的）という。

４－２．光子の性質(2)



・このとき、光子Aの振動方向がわかると、光子Bの振動方向もわかる。
この関係性のことを量子もつれという。

５－１　E91プロトコル~絶対に盗聴されない鍵共有

●ベル状態になっている光子のペアを用意して、送信者Aliceと受信者Bobにそれぞれ配分

●光子の振動方向を「０」と「１」に対応させる。

・ベル状態…特殊な量子もつれ。片方が「水平に振動」と観測されたとき、もう片方も同じ「水平に振動」とわかる。

５－２．AliceとBobは測定方法を共有せずに、ある角度から光子を観測

●選択角度は二つが共通のもの、一つは互いに異なるものを利用する。

●同一の角度で測定された光子に対応したビットは共通鍵の作成に利用

●異なる角度で測定された光子は盗聴検知に利用する

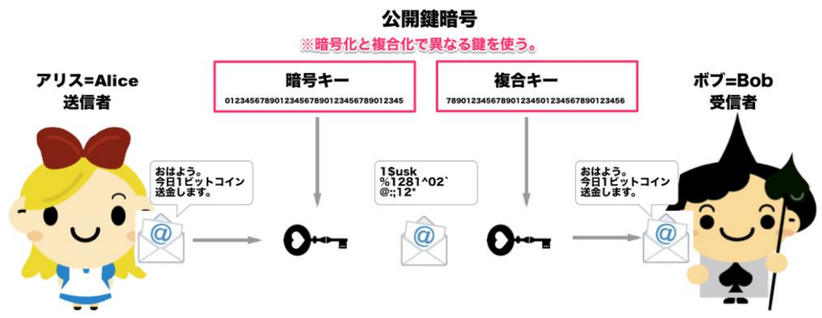
５－３．盗聴検知の原理

ベルの不等式を利用して盗聴を検知する。

↑
↑
$-2 \leq C \leq 2$

異なる角度で観測された光子をもとにCを算出
↓
・ベルの不等式が破れると量子もつれが存在する
・ベルの不等式が破れなくなると量子もつれになっていない光子が混ざっていることを示す

５－４．　５－１から５－３を実行することで、絶対安全に共通鍵を作成することができる。



参照:https://salestechnologylab.com/ビットコインとブロックチェーンの-暗号技術-初心者入門-deb5a12e009b

参考文献:福田伊佐央　『もつれる粒子』　Newton2024年10月号　p14-p43
「量子鍵配送E91による通信プロトコルの提案とノイズ・盗聴者下における性能評価」.2024年10月24日https://aqua.sfc.wide.ad.jp/publications/chanou_bthesis.pdf.