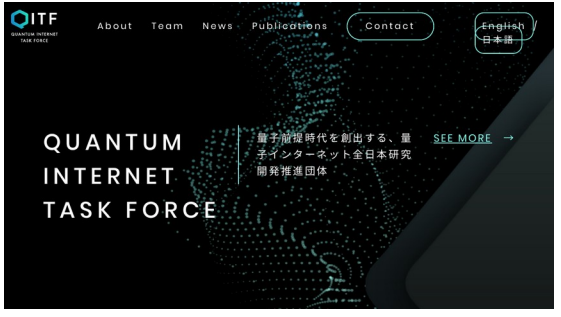
# 量子暗号通信とその安全性

東京大学大学院工学系研究科物理工学専攻
佐々木 寿彦

日本銀行金融研究所
情報セキュリティ・セミナー
2022-02-22

# 自己紹介

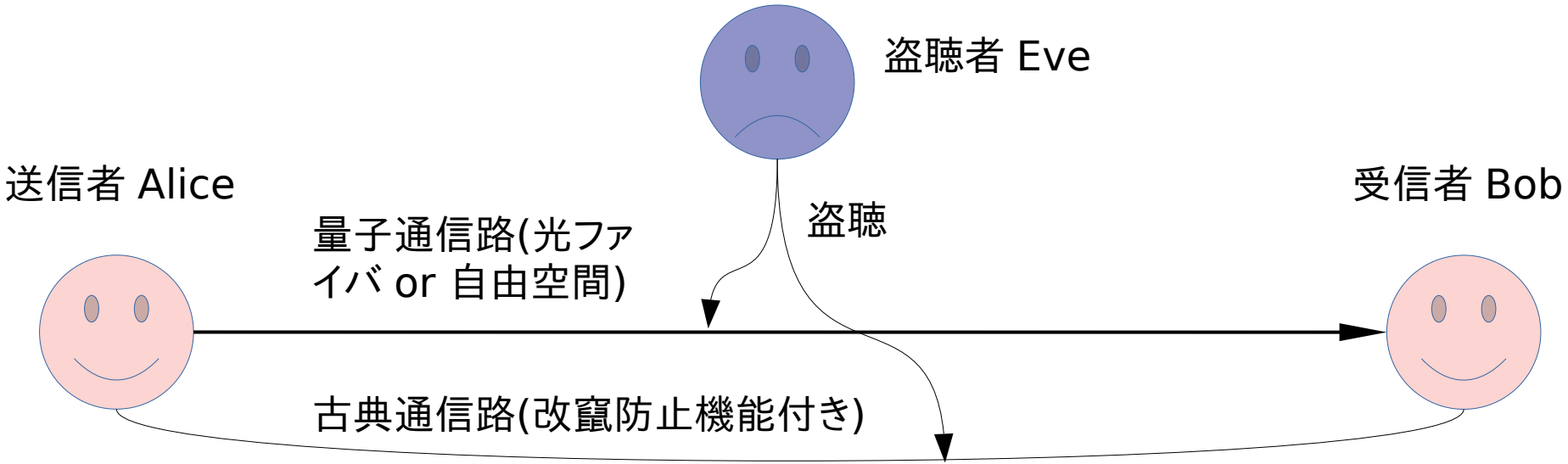
- 2012年に東京大学で博士(理学)を取得
- ポスドク、助教をへて2020年から現所属(東大工学系)の講師
- 研究内容
  - 量子基礎論: 特に量子論の物理的特徴付け
  - 量子鍵配送理論: 量子鍵配送の安全性証明
  - 量子インターネット: 責任分解点の調整、各領域の摺り合わせ
- 量子ICTフォーラム量子鍵配送技術推進委員会委員、量子インターネットタスクフォースボードメンバー

# 概要

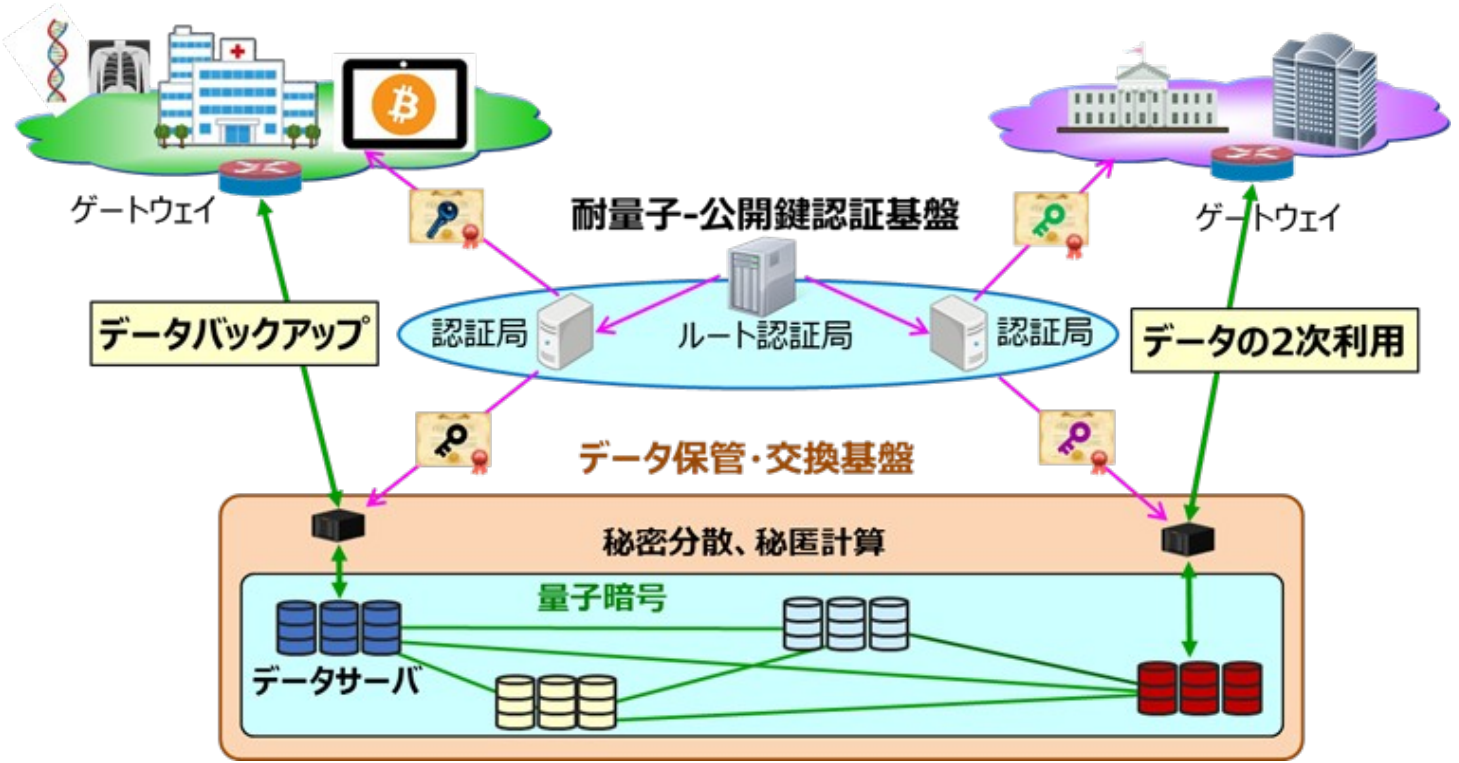
- 量子鍵配送(QKD)の概観、補足
- QKDの意義
- 最近の研究(連続量QKDの意義と現状)
- 考察(私見)

# 量子鍵配送(QKD)




- 遠隔2者間で長期的に安全な乱数(共通鍵)を共有するのが目的
- 共通鍵を使って安全な通信ができる。(One-time pad)

# 量子セキュアクラウド




情報通信研究機構(NICT) 量子ICT協創センター
https://www.nict.go.jp/qictcc/

# QKDの標準化

- デジュール標準:
  - 政府調達(大学やインフラ企業での1500万以上の買い物含む)は従う必要のある標準(WTO-TBT協定)
  - ITU-T:
    - SG13 Network: Y.3800,Y.3801,Y3802,Y3803,Y3804,Y3805,Y3806
      - アーキテクチャ・制御の基本構造
    - SG17 Security: X.1702,X.1710,X.1712,X.1714
      - 乱数、フレームワーク、鍵管理
  - ISO/IEC JTC1 SC27
    - ISO/IEC CD 23837-1/2(審議中)
      - 検査基準、評価方法

# 概要

- 量子鍵配送(QKD)の概観、補足
- QKDの意義
- 最近の研究(連続量QKDの意義と現状)
- 考察(私見)

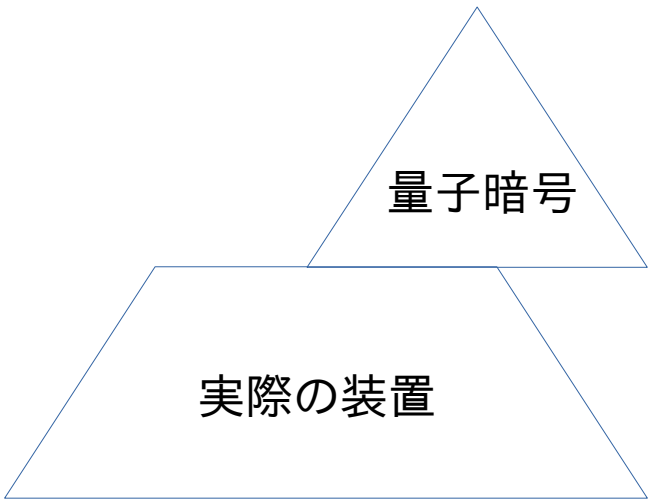
# QKDの意義は?

- QKDを使えば
  - 長期的に安全な鍵を共有できる。
  - 長期的に安全なデータ送受信を可能にする。(One-time pad)
    - 専門的に言えば、情報理論的安全性を保証できる
    - 保証するには前提条件が存在する

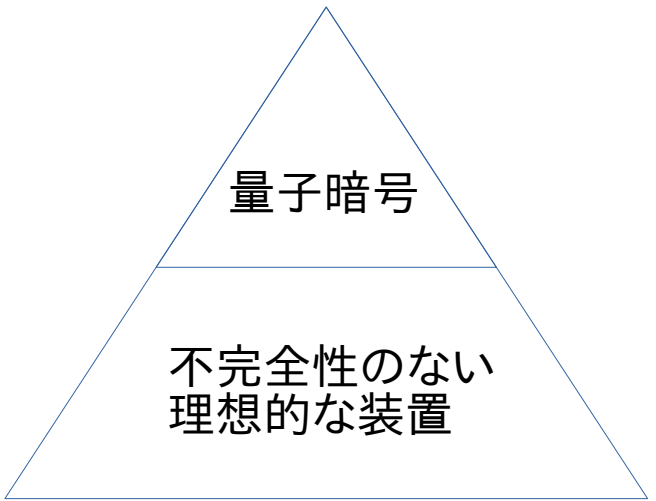
# 前提条件

- 前提条件
  - 装置が想定通り動いている
  - 通信可能な古典通信路が使える
  - (平時は)ノイズや信号減衰が激しすぎない量子通信路が使える
  - (ユーザー認証とメッセージ認証が使える(後半で解説))

# 装置のモデル化




こちらは最近にかけて精力的に研究されている

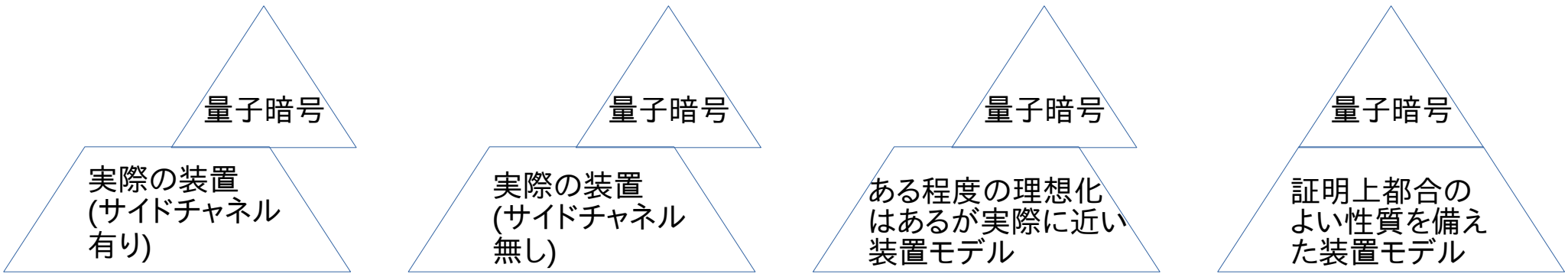



2010年くらいからできるようになってきた

# 装置のモデル化

想定外のことが起きにくい

証明しやすい
性能高い




玉木先生の最
後の話

性能低下を少なくしつつ
なるべく近づけておきたい

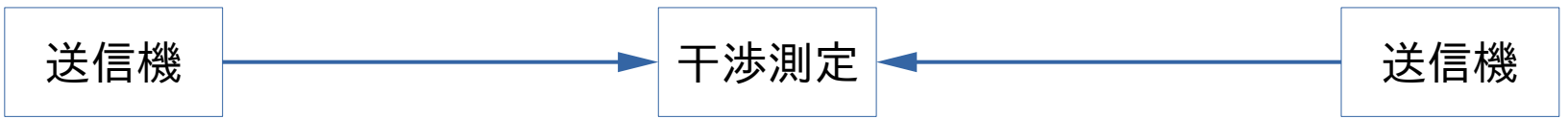
# 概要

- 量子鍵配送(QKD)の概観、補足
- QKDの意義
- 最近の研究(連続量(CV)-QKDの意義と現状)
  - QKDの分類とCV-QKDの位置づけ
  - 最近の研究結果
- 考察(私見)

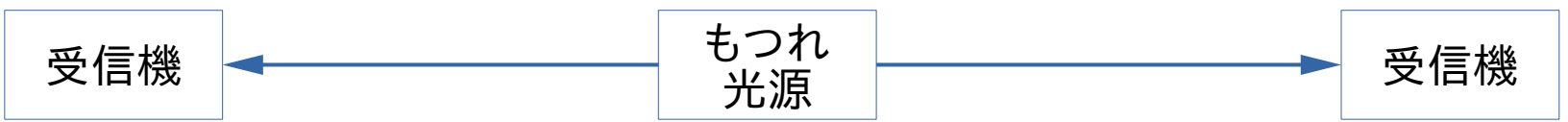
# 送受信器構成による分類

- Prepare-Measure型


- Measurement-Device-Independent型




- Entanglement-based型



# 検出装置によるQKDの分類

- 典型的な微弱光検出装置
  - on-off光子検出
    - 光子がきたかどうかを出力する
    - DV-QKD(離散量QKD)と呼ばれる
  - ホモダイン(ヘテロダイン)検出
    - 光の電磁波としての振幅を出力する
    - CV-QKD(連続量QKD)と呼ばれる

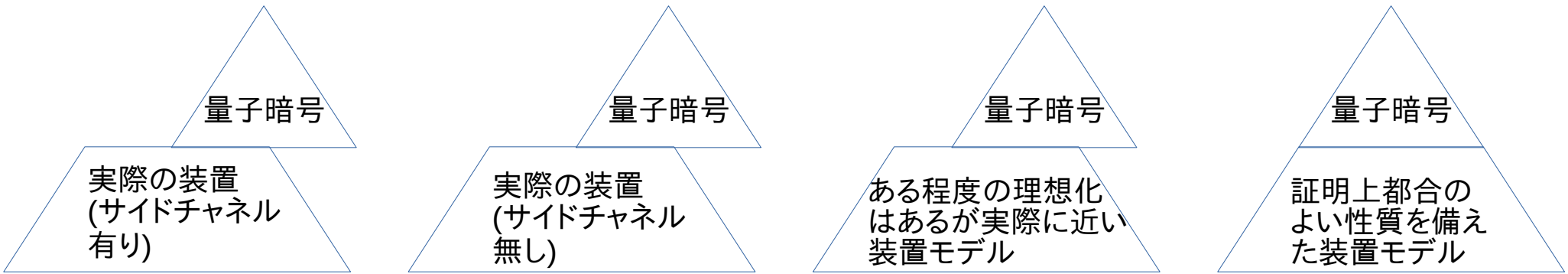
# CV-QKDの立ち位置

- 長所
  - 導入しやすい!
    - 既存通信と相乗りしやすい
    - 導入コストが安い
- 短所
  - 安全性を証明するのが難しい

# 装置のモデル化

想定外のことが起きにくい

証明しやすい
性能高い




玉木先生の最
後の話

DV-QKD

CV-QKD

本研究の話

# 概要

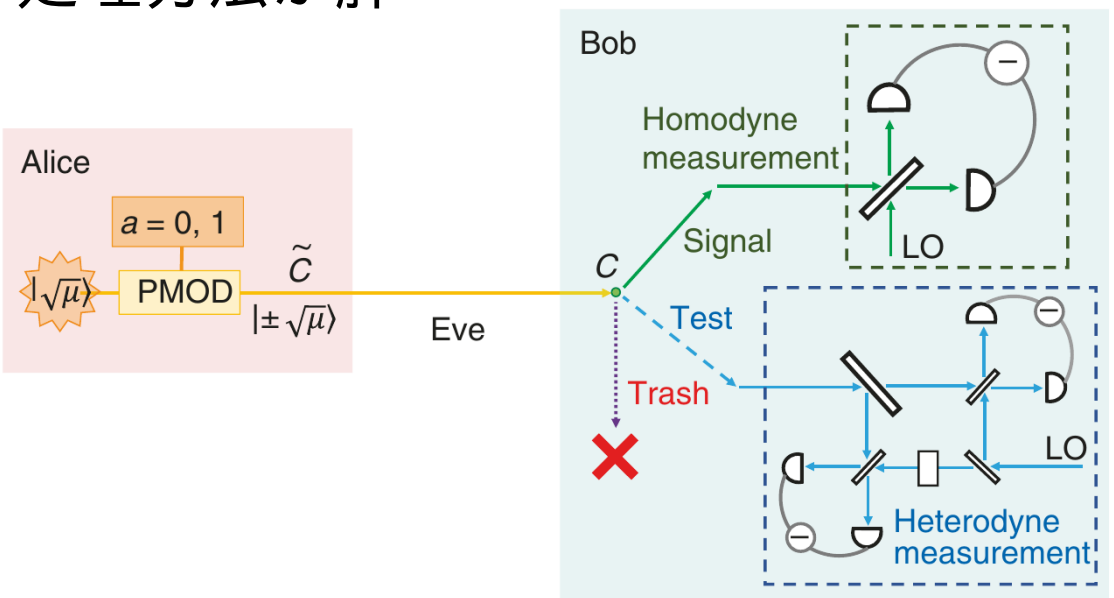
- 量子鍵配送(QKD)の概観、補足
- QKDの意義
- 最近の研究(連続量(CV)-QKDの意義と現状)
  - QKDの分類とCV-QKDの位置づけ
  - 最近の研究結果
- 考察(私見)

# CV-QKDの既存研究

- 既存研究
  - 特定の攻撃モデルだけに対する安全性を考える
  - 無限時間極限で想定される性能のみを考える
    - 有限時間、つまり現実の安全性を保証しない
  - 装置に厳格な連続値変調を要求する
    - 離散変調で近似すると証明が破綻する

# 提案するCV-QKDプロトコル

- 装置概要
  - 装置的にはほぼ従来通り
  - データ処理方法が肝

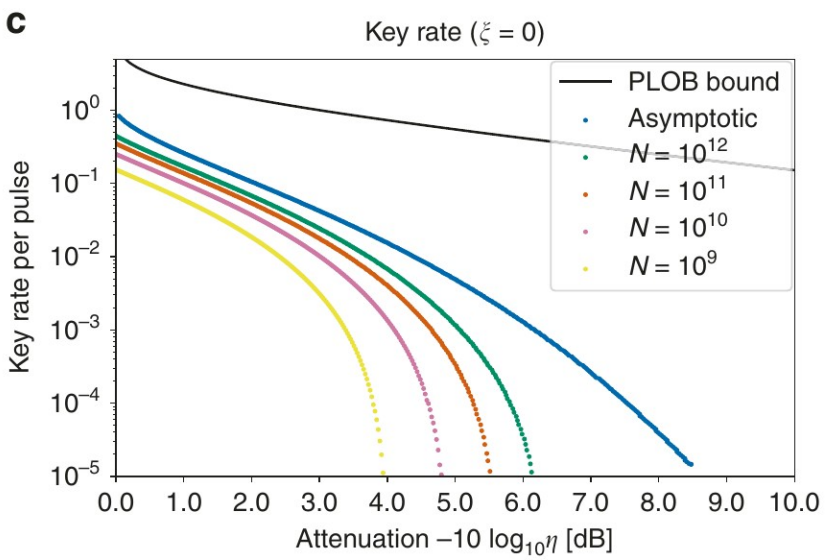


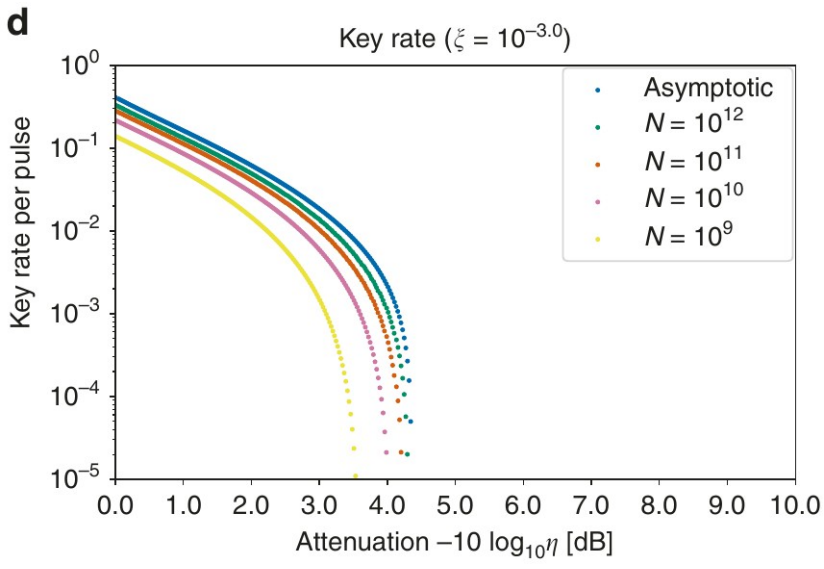



T. Matsuura, K. Maeda, T. Sasaki, M. Koashi, Nature communication **12**, 252 (2021)

# 性能

- 減衰率(~距離)に対するパルスあたり鍵レート
  - 想定する通信路モデルでの計算(左はノイズ無、右はノイズ有)
  - 結果の解釈: 現実的な時間で鍵がとれる。性能は改善の余地がある。



# CV-QKDまとめ

- 離散変調CV-QKDの有限時間での安全性を初めて証明した。
- 今後は性能をあげる
  - 今回は現実的設定で証明をつけるのが主目的だった
- 先端研究レベルではDV-QKDと比較可能なレベルまできた

# 概要

- 量子鍵配送(QKD)の概観、補足
- QKDの意義
- 最近の研究(連続量(CV)-QKDの意義と現状)
- 考察(私見)

# 考察(私見)

- 結局QKDをどう捉えたらよいのか?
  - Q&A形式の話をします
  - 私が妥当と思う想定や価値判断に依存します

# 耐量子計算機暗号とどちらが良い？

- 耐量子計算機暗号(PQC)
  - 量子計算機を使っても解読する方法が知られていない難しい問題を使った暗号
- その難しい問題が破られるかもしれないといっているが杞憂ではないのか？
  - どういう事態を心配しているのか？

# 情報理論的安全性 vs 計算量的安全性

- 情報理論的安全性
  - 盗聴者の能力に制約をつけなくても安全
  - 長期安全: 安全性が時間の経過で低下しない
- 計算量的安全性
  - 解読に必要な計算量が現実的でないと信じられているので安全
  - 現在主に使われている
  - アルゴリズムや計算機の進展により安全性が低下していく
  - 耐量子計算機暗号でも同様

# 計算量的安全性の安全性の低下

- 本質的脅威は解読アルゴリズムの進展とバックドア
  - DES(共通鍵暗号)は20年くらいで実際に解かれた
  - RSA(公開鍵暗号)は量子計算機ができれば解読可能
  - Dual_EC_DRBG（乱数生成）はNSAにバックドアを埋め込まれた
- 鍵長選択の問題
  - 実装コストの問題があるので無闇に鍵長を長くはしない
  - 計算量的安全性の暗号は更新していくのが大前提
  - 昔使われていたRSA512は古典計算機で充分解読できる

# Store & Decrypt 攻撃

- Store & Decrypt 攻撃
  - 通信路を流れるデータを保持しておいて後で解読する
  - 計算量的安全性には脅威
  - 情報機関はデータ保持を(多分)すでに行っている
  - 陳腐化するデータにこの攻撃を行っても意味がない
    - 陳腐化しなさそうなデータの例は、DNA情報。洩れると子孫の情報も部分的に洩れることになるため。

# 耐量子計算機暗号とどちらが良い？

- まとめると
  - QKD: 長期安全な秘匿性を提供
  - PQC: 保証は短期(30年くらい？)だが、今のインフラに乗る。提供できる機能が多い。
- そもそもユースケースが違う。適材適所
- QKDとユースケースが近いと思われるのは Trusted Courier
  - 鍵を人の手で運ぶ手法
  - 情報理論的安全性を提供
  - 運ぶ人の信用にすべてがかかっている
  - 鍵の更新頻度が低くなりがち

# 認証について

- QKDは中間者攻撃で簡単に破れるとネットで聞きました!
  - ユーザー認証もするので中間者攻撃できません。
    - Wegman-Carter認証という情報理論的安全性をもつ認証が使える。全体として文句なしに情報理論的安全性をもつことになる。
      - ただし、初期鍵を安全に運ぶ必要がある。
    - 認証部分は計算量的安全性をもつ暗号を使うという選択肢も存在する。
      - 計算量的安全性をもつ暗号が、後で破れるとしても、今破られていなければ、長期の秘匿性は傷つかない。

# 安全性証明の歴史

- いつも安全性が示されたって言っていて、前は何だったの？
  - 最初のQKD(BB84)の提案は1984年
  - 方式は多種多様なものがある
  - 当時の基準でBB84に証明がついたのが2000年の少し前くらい
  - この辺で安全性基準の見直しが行われた
  - 現在の基準で証明がついてきたのが2010年くらい
  - デバイスの不完全性に対する対策が整備されてきたのが最近

# 性能比較

- ずっと性能(鍵生成レート)のよいものをみかけました!
  - 性能は通信距離に依存します。非常に近距離だと高い性能がでます。
  - ちゃんとした安全性解析をしない方が性能が高くなります。
    - 一定の認証手続きができるはずなので、それに通っていればよいと思います。

# NSAの評価1/2

- NSA(とかGCHQ)が推奨しないって言ってます。
  - https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

1. QKDは秘匿性しか提供しない。秘匿性も耐量子計算機暗号使えばよい。
   - 他と組み合わせれば良い。意図的に長期安全性を無視している。
2. 特別なハードウェアが必要。updateも難しい。
   - 必要ならやるしかない。組み込みのセキュリティ製品はいくらでもある。
3. 多くの場合でTrusted relayが必要。コストもかかるし、リスクもある。
   - インフラ側が要所を守ってくれることにある程度の信頼は必要。

# NSAの評価2/2

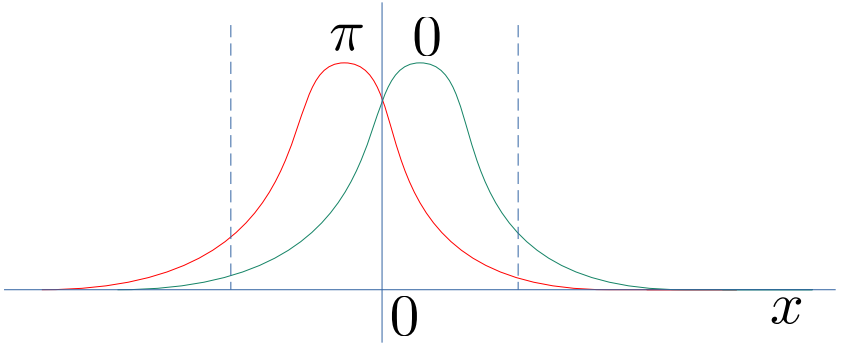
4. QKDを安全にするのは難しい。ノイズにも弱い。商用QKDに対する攻撃手法も存在する。
   - 実用的ノイズ環境で運用できることは実証済み。既知サイドチャネル攻撃に対する対策は存在する。安全性が保証できなくなるのと、攻撃が成立するには大きなギャップがある。
5. 盗聴者の存在(ノイズ)に敏感だからDoSに弱い。
   - ノイズ増やすくらいならケーブル切ればよいし、それなら古典通信でも対策不能。衛星通信の話だとしたら、むしろモード選択性が高いのでジャミングに強い。

# まとめ

- QKDを使うと、データ通信の秘匿性を長期で守ることができる
- 導入のための実績は積み上がっている
  - 理論・技術の整備
  - フィールドテスト、導入実績
  - 標準化
- 導入すべきかはユースケース依存なので、相談して下さい。(例えば、量子ICTフォーラム)

# 動作の仕組み

- 送信信号は位相0かπの弱いレーザー光
- ホモダイン測定
  - これで通信する。
  - 出力は実数値 x (-∞ < x < ∞)
  - 入力がきまっていてもある程度は揺らぐ。
  - どちらかわかりずらいところは使わない



# 動作の仕組み

- ヘテロダイン測定
  - これで盗聴を監視する。
  - 出力は実数値の組 (x,p) (-∞ < x,p < ∞)
  - 入力がきまっていてもある程度は揺らぐ。