

2025/6/30東京大学量子ソフトウェア寄付講座
第6回量子ソフトウェアワークショップ
最先端の量子技術 - 量子センサーから量子アルゴリズムまで -

SQAI
Center of Innovation for Sustainable Quantum AI



量子通信・量子暗号の現在および今後

慶應義塾大学
理工学研究科兼政策メディア研究科
慶應サステナブル量子AI研究センター

友野孝夫

自己紹介：友野孝夫, 博士 (工学)

IEEE Senior Member

現在の仕事：
量子機械学習、量子アルゴリズム
量子光学(CV-QKD)



1984年筑波大学卒業、1998年論文による博士(量子光学：慶應義塾大学)
大学卒業後、シャープ、富士ゼロックス、Samsung電子、TOPPAN Holdingsを経て
現在、慶應義塾大学理工学研究科特任教授
30年近く半導体(微細加工)およびフォトニクス分野で製品開発。ここ15年はコンピュータサイエンス

2018年頃から量子機械学習、光量子情報の研究に従事。

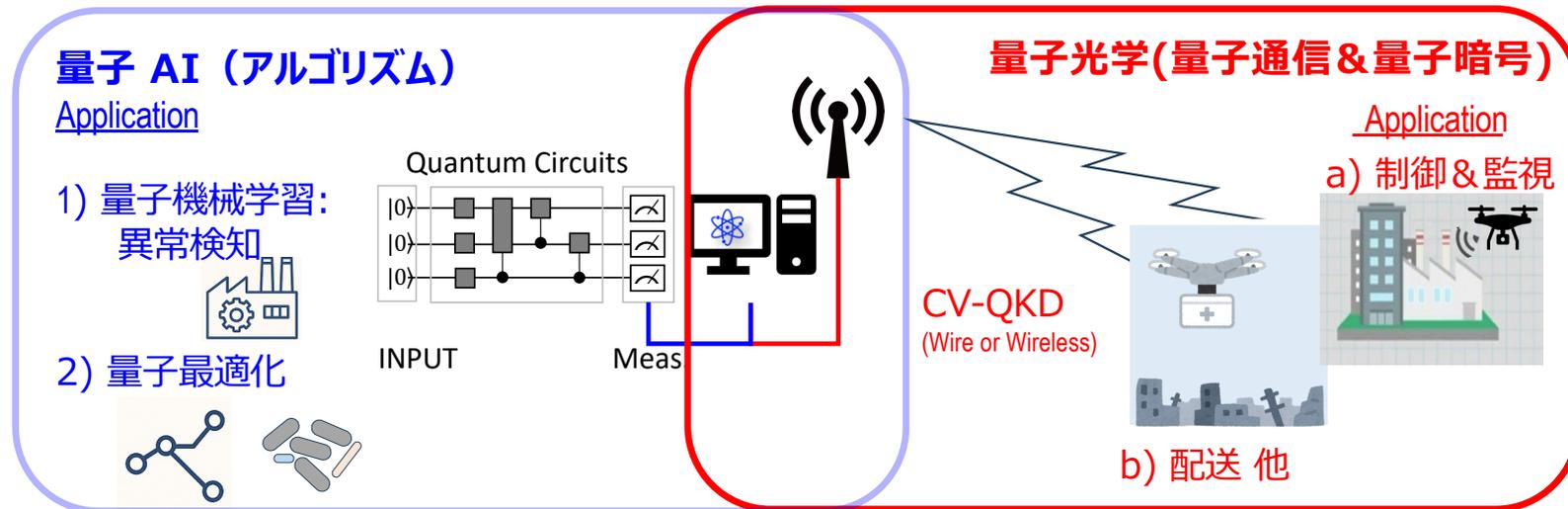
実績	全体	量子関係
査読付論文	31 (第一著者:17)	10 (第一著者:6)
招待講演	7	3
国内海外の委員	5 JSAI, IDW (国内)	3 QAIO, PQAI, IEEE QAI (海外)
公開特許	>150	(出願済: 2)
登録特許	>52 (日本) / >21 (世界)	
製品	半導体・微細加工製品 • TFTプリンタヘッド(A0地図向け) • μサイズのレンズシート(70' Prj.TV向け) • マイクロニードル(医薬品向け)	

Google Scholar:
Google Patents:
慶應義塾研究者情報データベース

https://scholar.google.com/citations?hl=ja&user=Mk7yMhEAAAAJ&view_op=list_works&sortby=pubdate
<https://patents.google.com/?inventor=Takao+Tomono&oq=Takao+Tomono>
https://k-ris.keio.ac.jp/html/100016852_ja.html

MY MOTIVATION

量子AIの社会実装を加速させるため、
量子優位性のメリットが明確に実感できる
アプリケーション (量子機械学習、量子最適化、量子暗号など)
の研究開発を目指しています。



量子が優位と考えられている分野：1)量子シミュレーション、2)暗号、3)組み合わせ最適化、4)機械学習、5)CAE

OUTLINE



1. バックグラウンド
2. 従来の暗号技術
3. 量子力学の基本性質
4. 量子暗号
5. 耐量子暗号
6. 研究開発動向
7. サマリー
8. 支えてくれているメンバー

1. バックグラウンド

NEWS

20250611

欧州で商用量子鍵配送ネットワークが開始された例

フランスOrange Business 社と東芝がフランスで初の商用量子セキュア通信ネットワークサービスを提供開始

https://www.global.toshiba/content/dam/toshiba/jp/company/digitalsolution/news/pdf/news_20250611.pdf

20250527

Googleの研究者がこれまで想定されていたよりも少ない量子ビット数で
ビットコインの暗号を解読できる可能性を示した

<https://finance.yahoo.co.jp/news/detail/d0cf81dc582ee60e38ae806ed23a77a7d11b903e/photo/view-001>

Project Eleven、量子コンピュータでビットコインの暗号
鍵を破った者に1BTC（約1,260万円）の賞金を提供
締切：2026年4月5日

<https://www.qdayprize.org>

The Competition is on:

Can You Break ECC with Quantum?

> Prize: 1 Bitcoin

> Deadline: April 5, 2026

> Competition: Break the biggest ECC key with Shor's algorithm.

Register now

or, [on the fence?](#)

情報セキュリティの重要性

情報セキュリティの新たな時代

デジタル社会における情報保護の重要性が増大
現代の重要インフラは暗号技術に依存

量子コンピュータの発展により従来の暗号が危機に

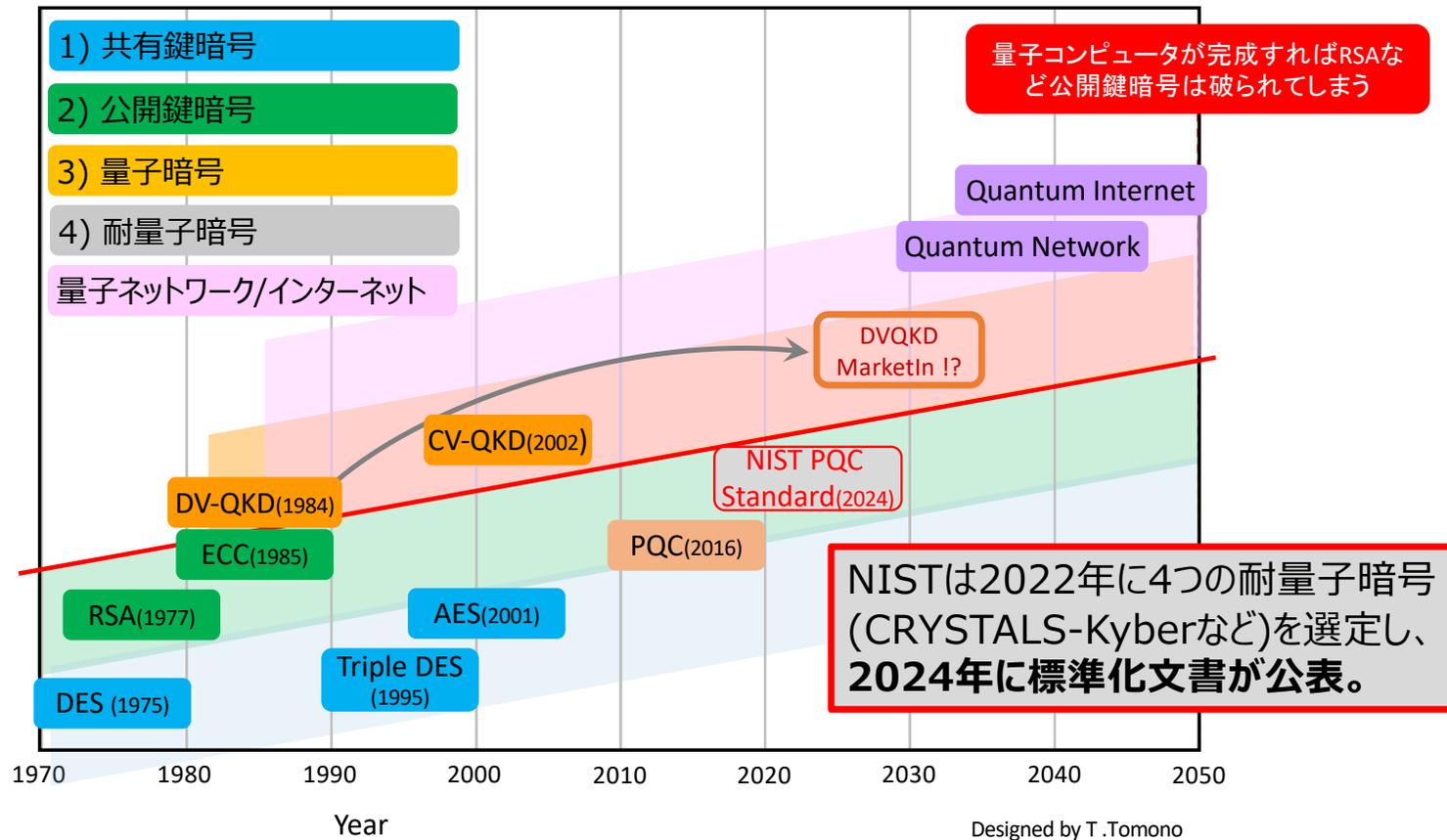
RSAや楕円暗号が将来的に破られる可能性



量子暗号は数学的困難性ではなく
物理法則に基づく新しい安全性の概念を提供します。

1. バックグラウンド

量子通信&量子暗号技術のロードマップ

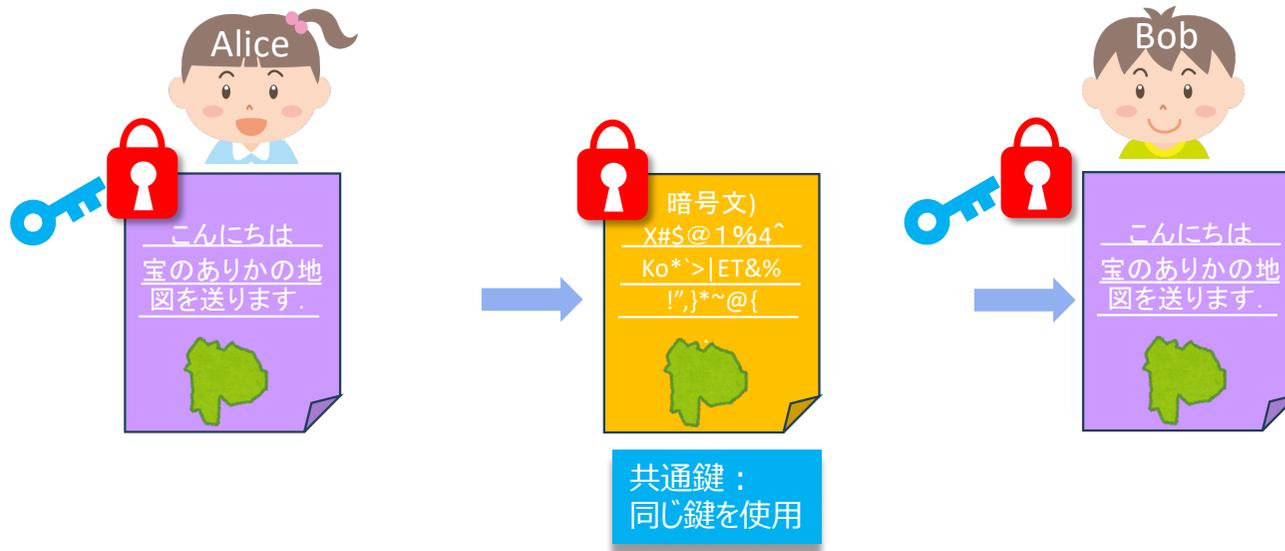


2. 従来の暗号技術

共通鍵暗号

送信者と受信者が同一の秘密鍵を共有し、その鍵で暗号化・復号を行う方式

例：AES, 3DES, Blowfish



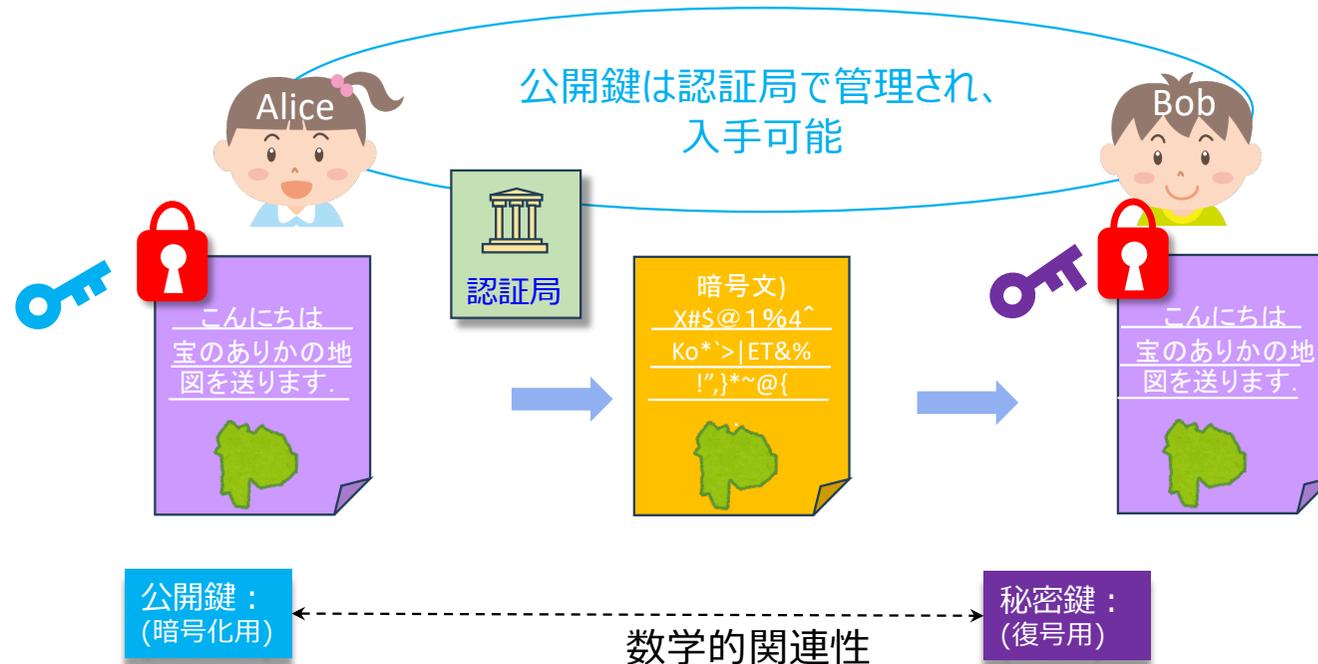
最大の課題： **鍵の安全な共有方法**

この鍵配送問題を安全に解決するための一つの回答が後で述べる量子鍵配送(QKD)です

2. 従来の暗号技術

公開鍵暗号

送信者と受信者が異なる鍵を使用
例：RSA, ECC, etc

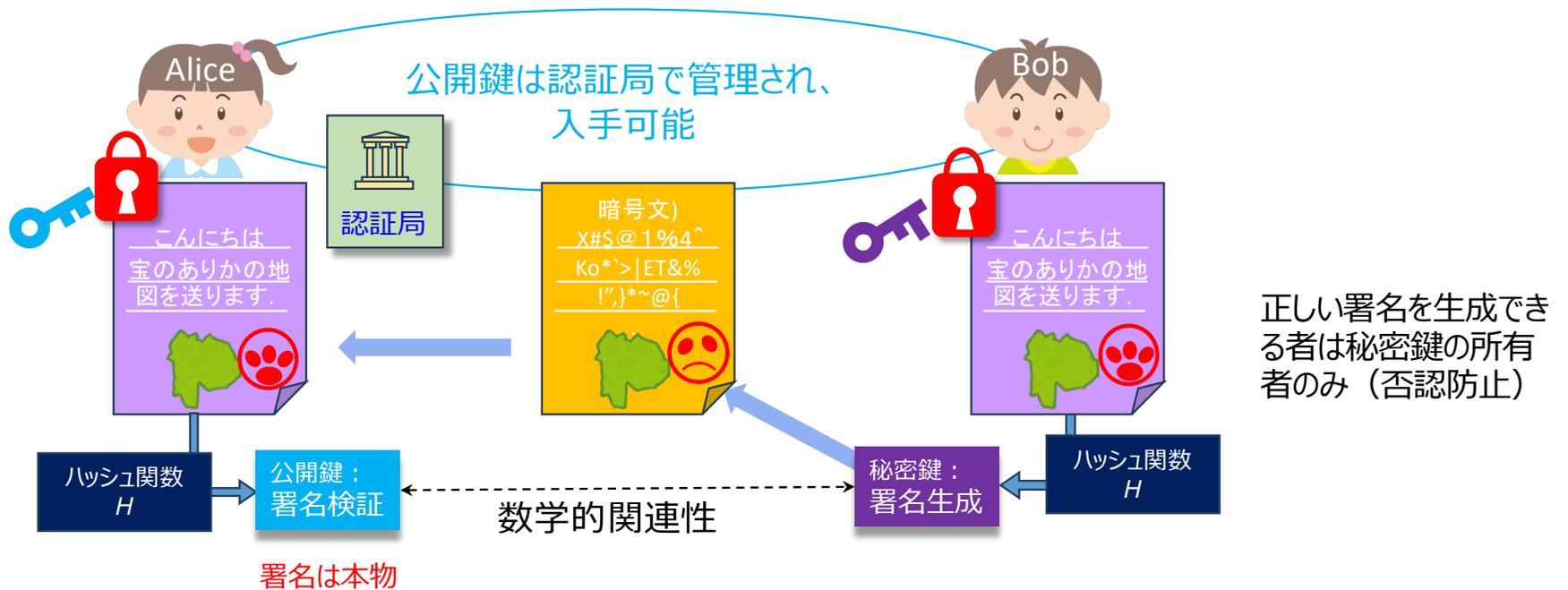


安全性の基盤：計算量的困難性 (大きな数の因数分解など)

2. 従来の暗号技術

デジタル署名

デジタル署名：公開鍵暗号の暗号化のアイデアを逆方向に利用
Bobが自分の秘密鍵で文書に対する署名、AliceがBobの公開鍵で署名検証



安全性の基盤：**計算量的困難性** (大きな数の因数分解など)

従来暗号の問題点

鍵配送問題（共通鍵を安全に共有する難しさ）

数学的困難性に基づく安全性（公開鍵にとって、絶対的安全性はない）

量子コンピュータによる解読リスク（ショアのアルゴリズム:1994年）

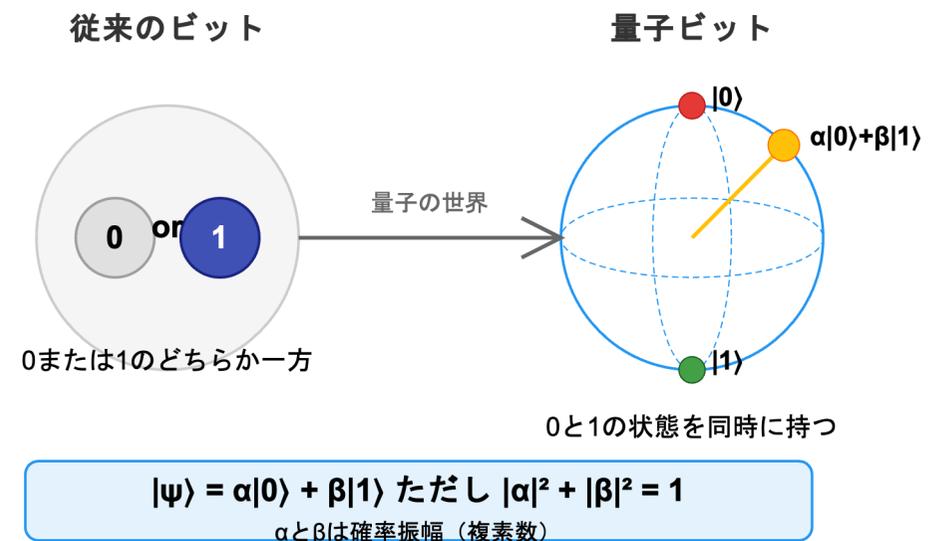
量子コンピュータで公開鍵暗号が解読可能に

- Shorのアルゴリズム： RSAなどの公開鍵暗号を効率的に解読
- Groverのアルゴリズム：**共通鍵暗号に対する総当たり攻撃を平方根時間で高速化**
(鍵長128ビットなら約 2^{64} 回の計算で破れる)

量子コンピュータが実現するとRSA等は破られ、共通鍵も十分長い鍵が必要

量子の重ね合わせ

- 従来のビット： **0または1**のどちらか一方
- 量子ビット： **0と1の両方の状態を同時に持つ**
- 数学的には： $a|0\rangle + \beta|1\rangle$
- a と β は確率振幅 ($|a|^2 + |\beta|^2 = 1$)

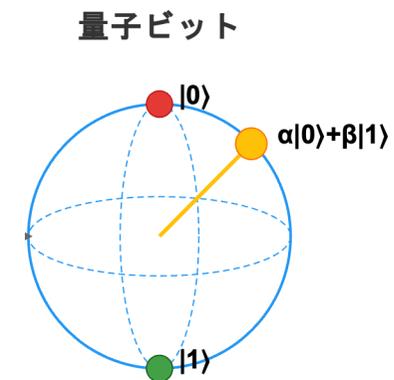


1つの量子ビットが**複数の可能性を同時に表現**できる

観測効果

量子状態の観測と波束の収縮

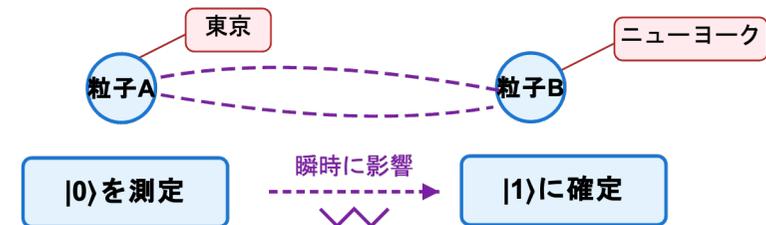
- 観測前：重ね合わせ状態（0と1の混合）
- 観測すると：状態が一つに確定（0か1）
- 確率的に結果が決まる（ $|\alpha|^2$ と $|\beta|^2$ の確率）
- この現象を「波束の収縮」と呼ぶ



観測行為自体が量子状態を変化させる→ この性質が**盗聴検知**に利用される

離れた粒子間の不思議な相関関係

- 2つ以上の粒子が**量子的に相関**した状態
- 一方の粒子を測定すると、**他方の状態も瞬時に決定**
- 距離に関係なく**瞬時に影響**
(アインシュタインが“不気味な遠隔作用”と呼んだ)



応用：
量子鍵配送
量子テレポーション
量子コンピュータ

量子もつれは**量子鍵配送**や**量子通信**の基礎となる現象

物理法則に基づく絶対的安全性

◆ 非クローン定理：

盗聴者が量子状態にある光子を完全にコピーすることは不可能

◆ 観測による状態変化：

盗聴者が測定を試みると状態が変化して痕跡（エラー）を残す

◆ 量子もつれ：

「盗聴者がいない場合に限り**遠隔地でも安全に同じ鍵を共有できる**
(盗聴があると相関が乱れる)

古典暗号:計算量的困難性に基づく安全性 vs. **量子暗号:物理法則**に基づく安全性

量子鍵配送(QKD概要)

特徴：

- 量子力学の原理を利用して**安全な鍵を共有**する技術
- 鍵そのものではなく、**鍵の配送方法**が量子的

安全性：

- 第三者に盗聴されていないことを検知しつつ、共通の乱数鍵を生成可能なため、送信者と受信者の間で**秘密鍵を安全に確立**

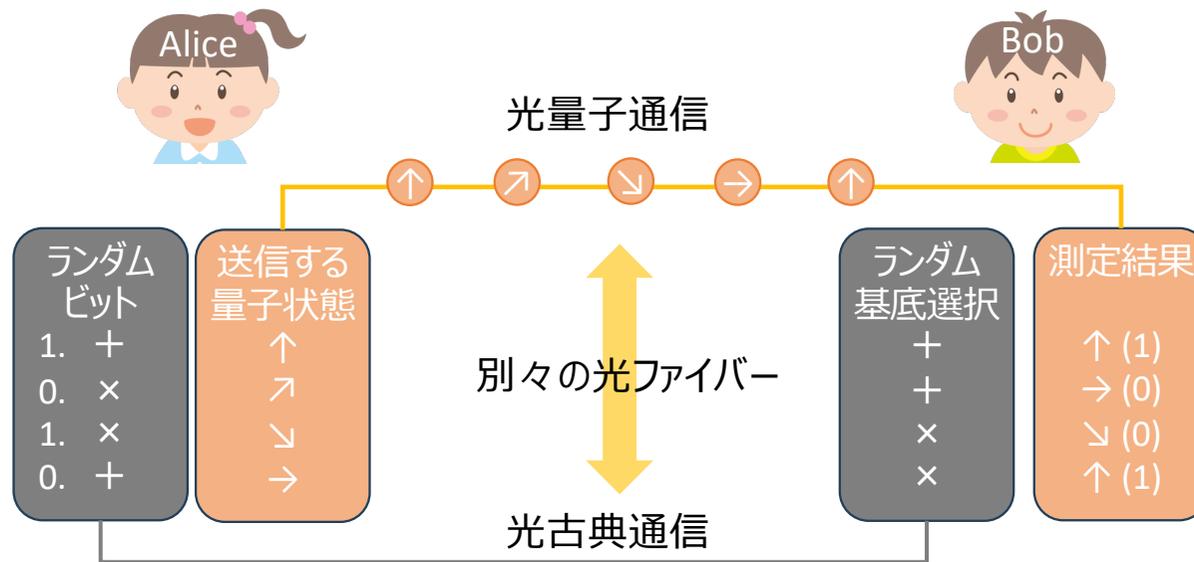
唯一実用段階に達している量子暗号技術
盗聴の有無を確実に検知できる

離散変数QKD vs. 連続変数QKD

項目	離散変数QKD (DV-QKD)	連続変数QKD (CV-QKD)
方式の概要	単一光子の離散的な状態（例：偏光の上下/左右）で情報を送る方式	レーザー光の振幅や位相といった連続量を用いて情報を送る方式
特徴	1984年提案されたBB84プロトコル以降長年研究され実用化が進んでいる技術	2002年提案された新方式(GG02プロトコル)で既存の光通信技術との親和性が高い技術
利点	長距離伝送に強いが装置が複雑	市販のレーザーと検出器で実装可能
欠点	単一光子検出器が必要.	長距離が厳しい上損失に弱い.
現状	フィールド実証・商用化が開始される段階	研究中の段階

4. 量子暗号

量子鍵配送(DV-QKD):BB84仕組み



$$|\psi\rangle = \frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}$$

- + 基底: $|0\rangle = \rightarrow$
- + 基底: $|1\rangle = \uparrow$
- × 基底: $|+\rangle = \nearrow$
- × 基底: $|-\rangle = \searrow$

ビット	アリス基底	ボブ基底	一致 (?)	測定結果	最終鍵ビット	判定
1	+	+	✓	1	1	鍵成立
0	×	+	✗	0	--	破棄
1	×	×	✓	0	0	盗聴検知
0	+	×	✗	1	--	破棄

基底が一致したビットのみ使用

量子鍵配送(DV-QKD):盗聴検知

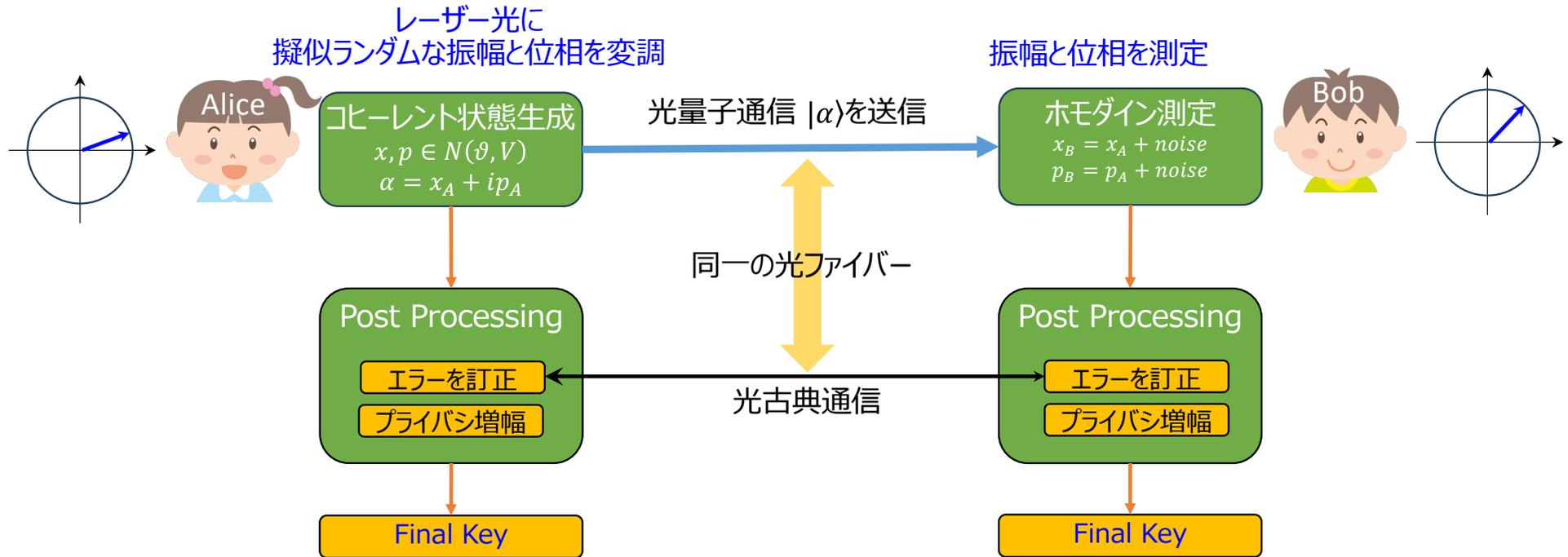
- 盗聴者（イブ）は送信に使用された**基底を知らない**
- 誤った基底で測定すると**ランダムな結果**になる
- 測定すると**元の量子状態が変化**する
- **誤り率**の上昇で盗聴を検知できる

量子力学の原理により、盗聴者は必ず量子状態を乱す
エラー率の上昇で**盗聴を検知**できる

理論上の検知確率：**100%**

実環境では光ファイバーの損失などで多少エラーが出るので、実測エラー率が理論想定より大きければ盗聴の疑いがある、と判断する。

量子鍵配送(CV-QKD): GG02仕組み



量子鍵配送(CV-QKD):盗聴検知

- Eveの介入は必ずチャンネルのノイズ・損失を変化
- Bobが受け取る信号の変動が大きくなる(Entropy増大)
- 盗聴が入るとAliceとBobのデータの相関が下がり、BobとEve（盗聴者）のデータの関連性が上がってしまいます
- 観測される余分なノイズが理論限界以上なら盗聴の可能性ありと判断する

理論上の検知確率：**100%**

量子力学の原理により、盗聴者は必ず量子状態を乱す。
したがってエラー率・ノイズの増加から盗聴を検知できる

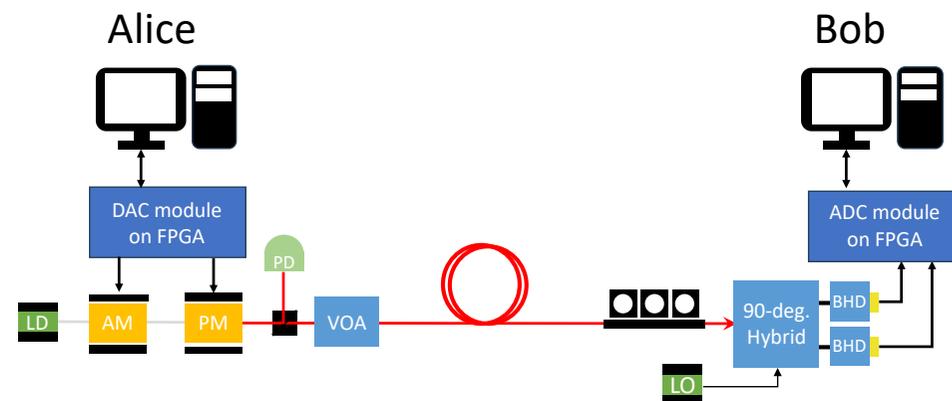
我々の研究

現状：

CV-QKDプロトコルの再現実験を実施。
特に、通信路の誤りに対するLDPCコードを用いた誤り訂正手法を検証中。

HEART2025(5/26-28/2025)にて
FPGA(Xilinx RFSoc 4x2)を対象にスループット
(最大0.89 Mbps) とのバランスを最適化。
最大で**ARMコアの9.36倍の高速化**を達成

<https://doi.org/10.1145/3728179.3728183>



概要

耐量子暗号(PQC)とは 量子コンピュータでも解読が困難な古典的な暗号

従来型計算機上で動作し、数学的問題の困難さを利用する新しい暗号

項目	内容	コメント
きっかけ	素因数分解/離散対数の高速解法	量子コンピュータが実用化されると、Shorのアルゴリズム等によってRSAとECCでは多項式時間で破られる（1994年:Shor）
緊急性	Harvest Now, Decrypt Later (時限爆弾) のリスク	現在の暗号通信を収集し、後で解読(医療記録、知的財産、政府情報などの長期間秘匿情報)
標準化	NIST国際標準策定プロジェクト (2016年～提案募集) 2024年に4方式を選定	目的・量子コンピュータが現れても安全な暗号 ・国際的なデジタル通信（政府、金融、IoTなど）を守る。

① 耐量子暗号の方式

格子暗号 ¹⁾ :	多次元格子の困難問題に基づく 格子（高次元格子上的ベクトル問題）により困難さを実現
コード系暗号 ²⁾ :	符号理論に基づく暗号 (古くからあるMcEliece暗号)
多変数多項式暗号 ³⁾ :	多変数方程式を解く困難さに基づく Rainbow署名(但し脆弱性が指摘され標準化は落選)
ハッシュベース暗号 ⁴⁾ :	ハッシュ関数の安全性に基づく

1). [doi:10.1109/CCWC.2019.8666459](https://doi.org/10.1109/CCWC.2019.8666459). ISBN 978-1-7281-0554-3

2). [doi:10.1007/978-3-642-12929-2_6](https://doi.org/10.1007/978-3-642-12929-2_6)

3). [doi:10.1007/11496137_12](https://doi.org/10.1007/11496137_12). ISBN 978-3-540-26223-7

4). [doi:10.1007/978-3-642-25405-5_8](https://doi.org/10.1007/978-3-642-25405-5_8)

5. 耐量子暗号

NISTで2024年に標準化された耐量子暗号

名称	目的	方式	特徴	FIPS
CRYSTALS–Kyber (ML-KEM)	鍵交換	格子	鍵の長さが短く、当事者間での鍵交換が容易	FIPS203
CRYSTAL-Dilithium (ML-DSA)	デジタル署名	格子	主要なデジタル署名標準	FIPS204
Sphincs+ (SLH-DSA)	デジタル署名	ハッシュ関数	パラメータによって、署名長の短さと署名生成速度の速さのどちらかを優先するか選択可能	FIPS205
FALCON (FN-DSA)	デジタル署名	格子	CRYSTAL-Dilithiumと比較して公開鍵長と署名長が短い	FIPS206

実用上の課題

課題	内容
処理速度・鍵サイズ	PQCアルゴリズムはRSA等に比べ公開鍵や暗号文が大きく、計算も重くなる傾向有り。通信量の増大し、CPU負荷が増し、 計算コスト が増大する。CRYSTALS-Kyberの暗号文サイズはRSAより大きい
Crypto Agility	新たな脅威やアルゴリズム改良に対応できる柔軟性が求められる。
既存資産への影響	現在運用中のシステムで暗号アルゴリズムを更新する 移行コスト や、既存データ（暗号化データ）の 再暗号化 の必要
ハードウェア対応	組込み機器やTLSアクセラレータなど ハードウェア実装 の場合、PQC対応品へのリプレイスが必要になる。 2030年問題 に間に合うか、といった課題が有り。
信頼性の検証	十分な安全性検証と業界標準化 NIST以外にも欧州の標準化機関や日本のCRYPTRECでの検討 世界的にPQCの信頼性評価と実装ガイドライン作りが進められている

性能面の懸念(鍵サイズ・計算コスト増)、既存システムへの適用(移行コスト、再暗号化)、標準化と相互運用性の確立

移行状況

国/機関

-  アメリカ (NIST, NSA)
-  カナダ政府通信保安局 (CSE)
-  日本 (総務省、NICT、情報処理推進機構)

業界

-  IT (Google, IBM, Microsoft)
-  金融 (Mastercard)
-  通信 (Cloudflare)
-  半導体・組込み (NXP, Infineon, Renesas)

取り組み内容

PQC標準化の中心的存在。NSAは「国家安全システムで2035年までにPQC導入を完了せよ」と通達。

ECDSA, EdDSA, RSAは**2035年以降利用禁止**。

商用ソフトにPQ暗号導入を推進。

IPAがPQCガイドライン策定。NICTがPQCのLOTUS研究開発

導入事例・動き

GoogleはChromeにPQC (ハイブリッドKyber) を試験導入。
IBMはTLSライブラリに組み込み。

トランザクション保護のためにPQC移行テストを実施。

Post-Quantum TLS (Hybrid Kyber+X25519) を展開中。

小型デバイス向けの軽量PQCチップを開発。

6. 研究開発動向

国別



中国

- 国家プロジェクトとして大規模量子ネットワーク構築



欧州

- 国際共同で量子インターネット研究



米国

- 最先端の研究を主導し、PQC標準化を主導



日本

- NICT中心に官民で実証実験を実施中で有り。

• (中国) 北京-上海量子通信幹線 (中国、2,000km超)
https://spc.jst.go.jp/news/171001/topic_1_06.html
• (中国) 地上衛星間量子通信ネットワーク(中国:4,600km超)
<https://www.nature.com/articles/s41586-020-03093-8>: <https://36kr.jp/113312/>
• (中国) 墨子J衛星(2016年) 7,600kmの量子もつれ配送、大陸間の量子暗号通信を実現
<https://uchubiz.com/article/new53555/>

(日本) 東芝QKD: 世界各地で商用のテストベッド
<https://www.global.toshiba/jp/company/digitalsolution/news/2023/0705.html>
• (日本) TOKYO QKDネットワーク (日本)
<https://www.nict.go.jp/press/2023/12/18-1.html>
• (日本) 盗聴不能な衛星暗号通信網を構築へ、スカパーJSATが実証中
<https://xtech.nikkei.com/atcl/nxt/column/18/02438/120500030/>

応用分野



金融システム

取引の安全性確保
長期機密データの保護



医療データ

患者情報の保護
遠隔医療の安全性



政府・軍事

機密通信の保護
国家安全保障



重要インフラ

電力網、通信網の保護
制御システムの安全確保

- 量子暗号は物理法則に基づき、理論上破られない（究極の安全性）
- 量子鍵配送（QKD）において
 - DV-QKDは商用システムあり、CV-QKDは研究開発中
- 耐量子暗号（PQC）は現在の暗号技術の延長線上で導入進む。
現在：従来暗号+PQC、将来：量子暗号+PQC
- 量子コンピュータの進展でこれら技術の重要性増大
- 課題は残るが量子通信インフラ構築が進行中
- 量子暗号とPQCは将来のデジタル社会を支える基盤技術になる

将来量子ネットワークが実現しても、一部では引き続きPQCも使われ、
量子技術と計算論的技術の両輪でセキュリティを守る形になるでしょう

支えてくれている方々に感謝します

CV-QKDの研究はCOI-NEXT (Grant No. JPMJPF2221)の支援を受けて実施しています。
量子AIの研究はCOI-NEXT (Grant No. JPMJPF2221)およびNEDOサイバーフィジカル事業(Grant No. JPNP23003)の支援を受けて実施しています。

他に複数のプロジェクトが今後進行する予定です。



量子AI：異常検知メンバー

辻村和也(Toppan Holdings) データサイエンス
松本匡哉(Toppan Holdings) 工場IT管理
嶋崎優絵(Toppan Holdings) 工場IT管理

量子AI：量子最適化メンバー

外林俊介(blueqat research) : 量子アルゴリズム
湊雄一郎(blueqat Inc.) : 量子アルゴリズム

CV-QKD メンバー

Wei Kaijie (慶應義塾大学)	FPGA, アーキテクチャ
Devanshu Garg (blueqat Inc.)	量子光学, 量子機械学習
永井隆太郎(SCSK Corp.)	量子光学, 量子機械学習
坂下達哉(東京大学)	スパコン, アーキテクチャ
天野英晴(東京大学)	FPGA, アーキテクチャ

強力な支援者

藤堂眞治(東京大学)	SQAI Project Leader
田中宗 (慶應義塾大学)	SQAI 慶應 Leader

敬称は略させていただきます



ご清聴ありがとうございました。

連絡先：
神奈川県川崎市新川崎7
慶應義塾大学新川崎タウンキャンパス K204B
takao.tomono@ieee.org