

資料 6

NECにおける量子暗号通信の取組み

2021/12/6

日本電気株式会社

技術シナジー創造本部

本部長 浅井 繁

\Orchestrating a brighter world

NEC creates the social values of safety, security, fairness and efficiency to promote a more sustainable world where everyone has the chance to reach their full potential.

1. 量子暗号通信技術の研究開発状況
2. NECの量子暗号通信技術への取組み
3. 戦略見直しにむけて

1. 量子暗号通信技術の研究開発状況

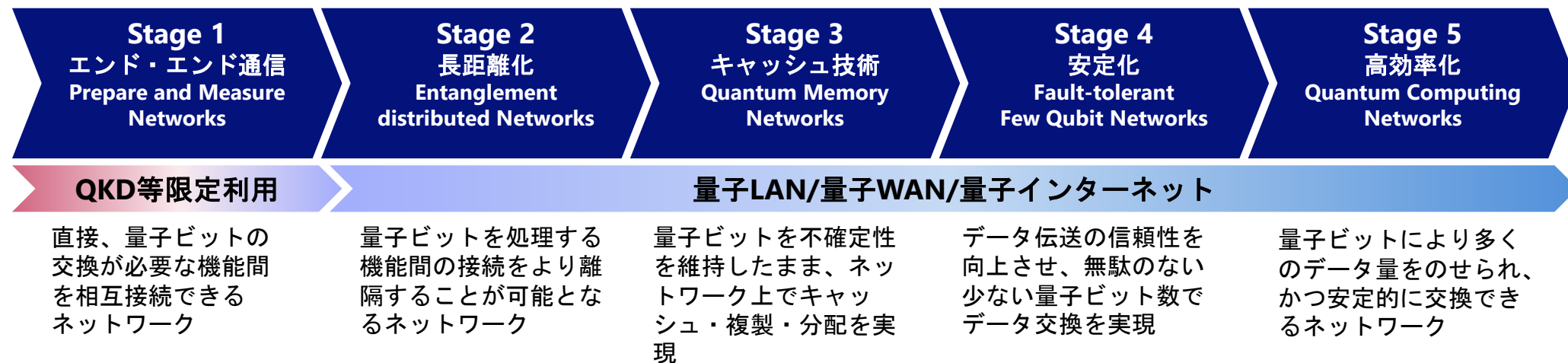
各国の量子暗号通信の戦略

量子暗号通信は、将来の量子インターネットの戦略的な位置づけ(EU/US)

- ◆ 量子鍵配送に関する技術要素が量子ネットワーク・量子インターネットにつながる
- ◆ 量子のままビット交換する技術として、QKDは量子ネットワークの第1ステップとされている

US研究範囲 2030達成目標

EU研究範囲 2028達成目標



Quantum internet: A vision for the road ahead, 2018を参考にNECにて作成 <https://science.sciencemag.org/content/362/6412/eaam9288>

量子暗号通信の普及が期待される市場

- ◆ 量子暗号通信は、DX化が進む社会を安全・安心に担保するためのインフラ技術となる
- ◆ 社会を下支えするためには量子暗号通信網の普及が必須

安全保障



機密情報

認証情報

行政



個人情報

認証情報

製造業



設計情報

サプライチェーン改竄保護 認証情報

金融



取引・与信情報

認証情報

医療



遺伝子情報

創薬開発情報

量子暗号通信

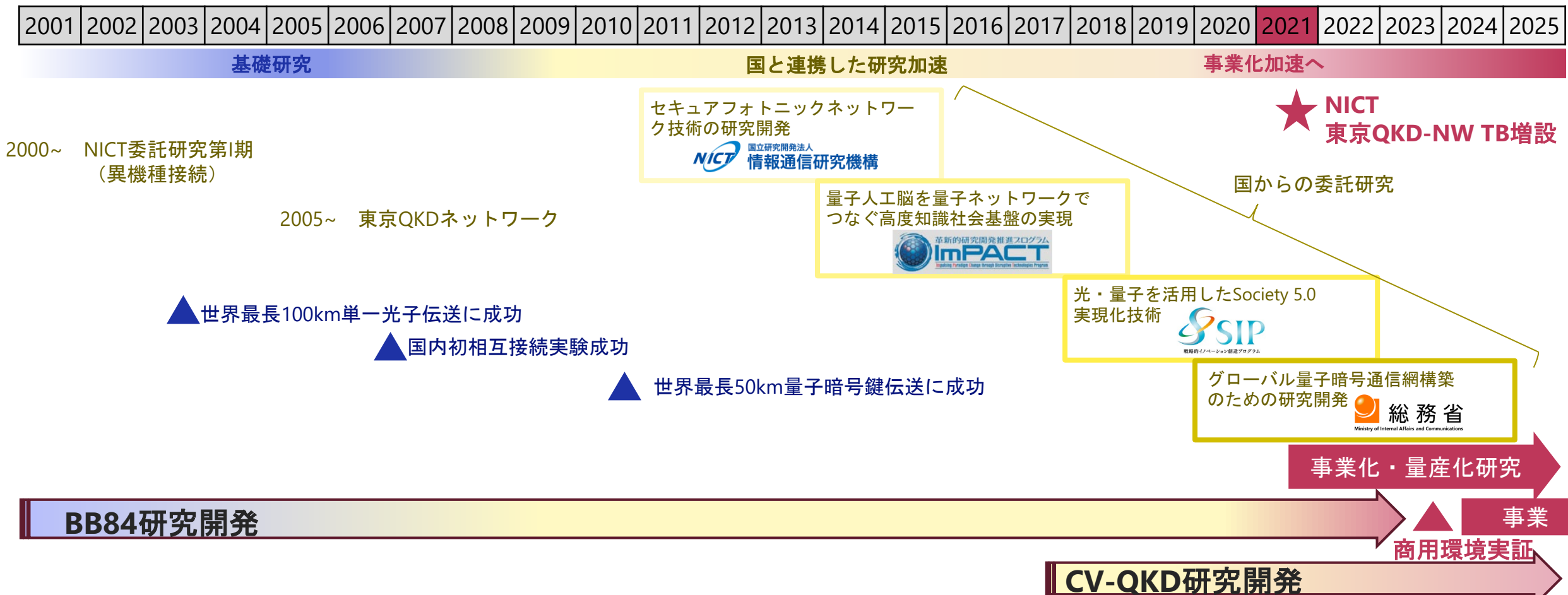
BB84: バックボーン網

CV-QKD: アクセス網

2. NECの量子暗号通信技術への取組み

NECの量子暗号研究の取組み

国内に主要研究拠点を有する唯一の企業として、20年間にわたり日本の量子暗号通信技術開発を牽引
FY2023の商用環境稼働を目指し、技術実証から量産化研究フェーズにシフト中

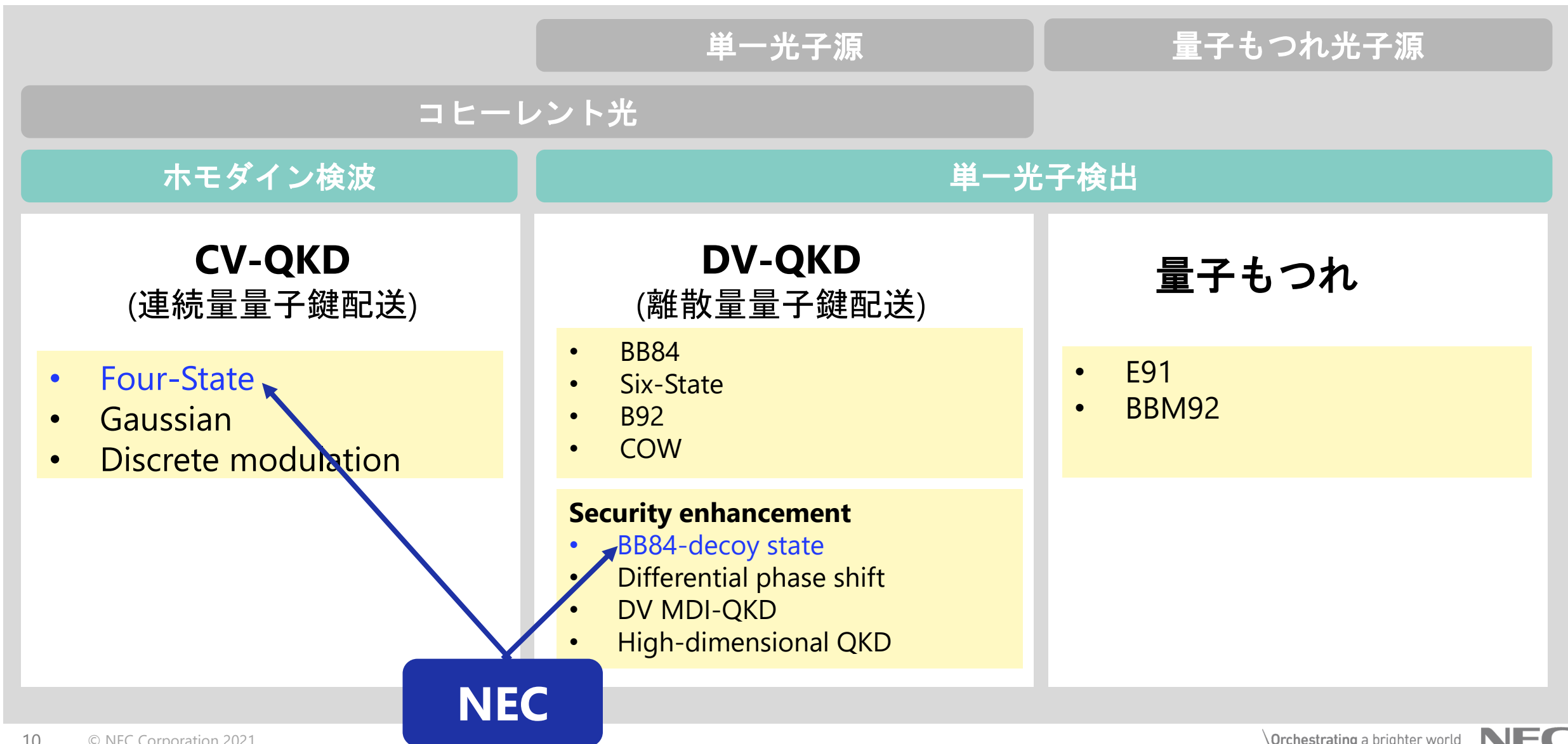


NECの研究開発体制

ハードからソフトまで一気通貫した研究開発・製造体制を国内に構築



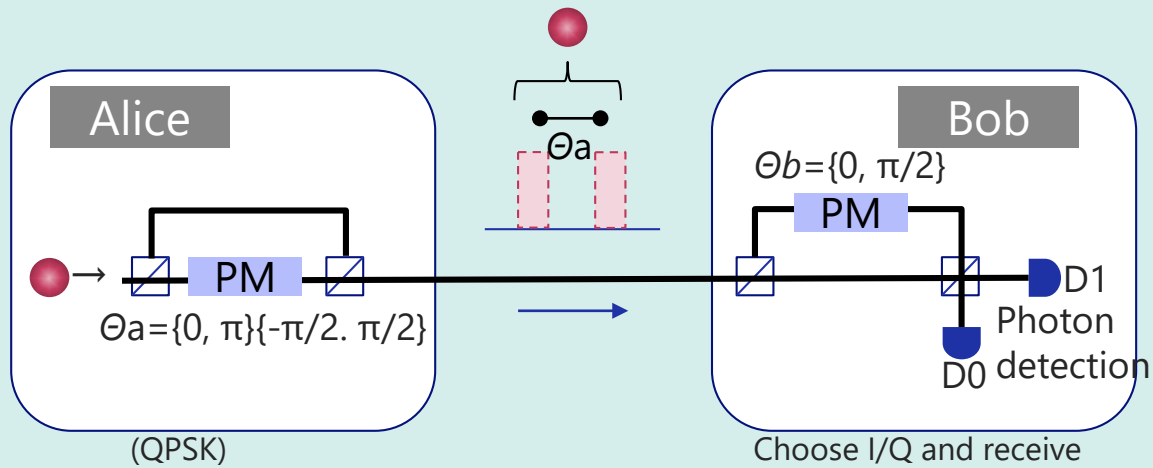
NECが研究中のQKD(量子鍵配送)技術



2つのQKD技術の特徴

DV-QKD(BB84)

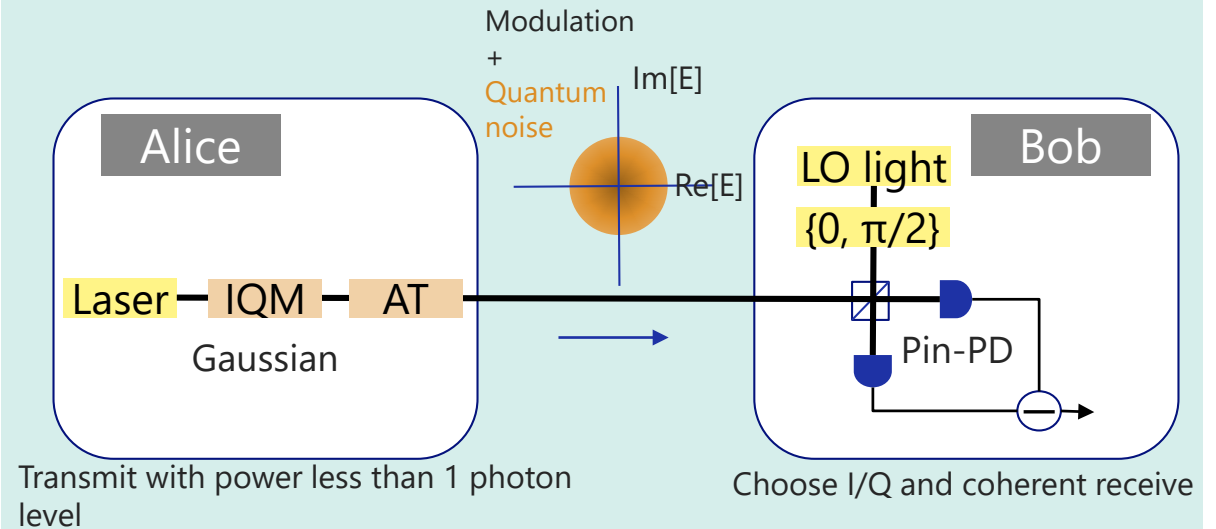
単一光子に対して、暗号鍵の論理ビットに対応するように位相変調を付与して装置間で送受する。



光子検出用の高感度デバイスが必要なため高コストだが、距離の延伸化で中継数を削減

CV-QKD

微弱光波に対し、受信側が暗号鍵の論理ビットに対応した信号レベルで受信できるように、送信側でIQ変調と減衰を付与して装置間で送受する。

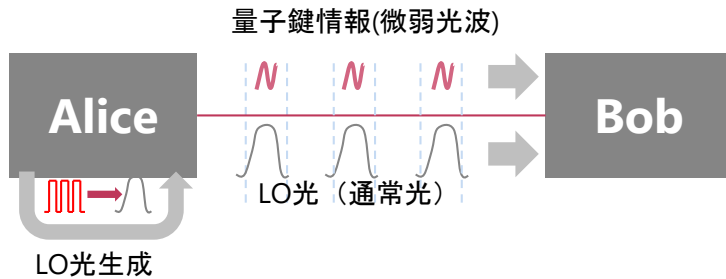


一般的な光通信デバイスが活用可能で、既存の光ファイバー通信との共存(同時利用)が可能

CV-QKD研究計画

セルフホモダイン方式

- ✓ 実現が比較的容易
- ✓ LO光への攻撃の可能性がある

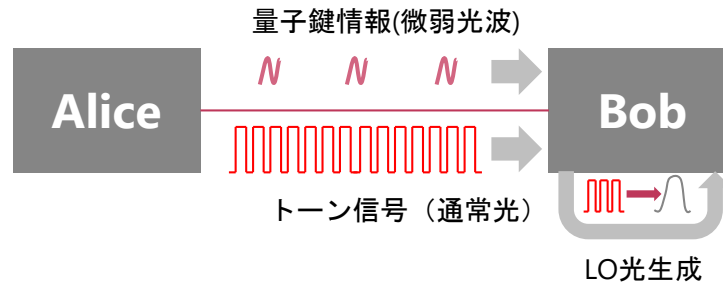


- ◆ 1つの光パルスを2つに分岐し、一方を信号光、もう一方をLO光とする方式。
- ◆ ビームスプリッターを使用して簡単に実現することができ、実績が多い。
- ◆ LO光が伝送路を通るため、LO光への攻撃の可能性があることや長距離化が難しいといった安全性・性能面での課題がある。

Current R&D

リアルLO方式

- ✓ セキュリティ課題への改善
- ✓ 量子信号への雑音低減技術開発要



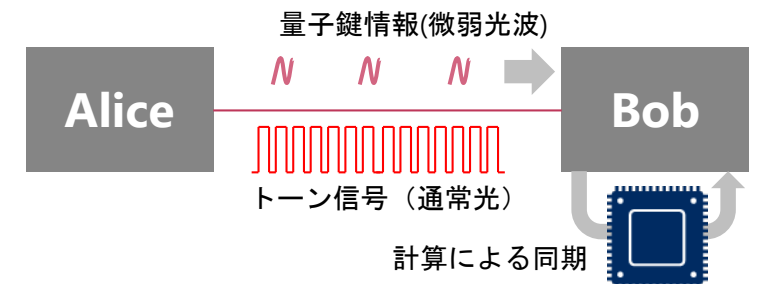
- ◆ Bob内にLO光を発生するためのレーザ光源を用意する方式。
- ◆ Aliceから信号光とは別に強い光（トーン信号）を送信し、Bobではトーン信号を元にLO光を生成する
- ◆ リアルLOではセルフホモダインの短所を軽減することができるが、量子信号への雑音を抑えつつトーン信号を送信する技術の開発や、狭線幅のレーザ光源が必要となるためコストが増加するといった課題がある。

SIP 2期

Current R&D

Digital coherent

- ✓ セキュリティ課題の解決
- ✓ 方式実現のための研究開発が必要



- ◆ BobはAliceの光源とは同期していないLO光を用いて測定を行い、測定結果に対してデジタル信号処理を行うことで直交振幅を測定する方式。
- ◆ 光の同期を行わないため光学系はシンプルであり、LO光への攻撃も回避できる
- ◆ 非常に重い信号処理が必要となることや、量子光は微弱であるため通常のデジコヒで行うパラメータ推定方法が使用できず、新規技術開発が必要となることが課題である

グローバル量子

3. 普及に向けた取り組みの分析

普及に向けた取り組みの分析

弊社が考える課題と対策

- ◆ 量子暗号通信の導入のハードルを低減
 - 商用化に不可欠な東京-大阪間や全国QKD網整備、安全保障分野での利用加速
量産化(調達拡大)による低コスト化と初期投資・運用コスト負担の軽減措置
- ◆ アプリケーション/ソリューション拡大を推進
 - 早期利用を促進し、新たなアプリケーション等のアイデア創出を加速
国際的な知財活用策の検討
- ◆ 実装安全性の獲得とデバイスや装置等の国内生産体制構築促進
 - セキュア開発手法の確立と評価・認証制度による安全性の確保
経済安全保障を考慮したサプライチェーン確立/低コスト化のための促進策

\Orchestrating a brighter world

NEC