\Orchestrating a brighter world **NEC**



本研究開発は、総務省の

「ICT重点技術の研究開発プロジェクト(JPMI00316)」と 「グローバル量子暗号通信網構築のための研究開発(JPJ008957)」 並びに、内閣府の戦略的イノベーション創造プログラム(SIP) <u>「光・量子を活用したSociety5.0 実現化技術」</u> によって実施した成果を含む

NECにおける離散量並びに連続量量子鍵配送の実験の紹介

2024年7月17日 日本電気株式会社 アドバンストネットワーク研究所 川上哲生

Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、 誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

本発表の目次

- 1. 量子鍵配送(QKD)の概要とNECのQKD研究開発の 取り組み
- 2. NECにおける離散量(DV)-QKD実験の紹介
- 3. NECにおける連続量(CV)-QKD実験の紹介





1.量子鍵配送(QKD)の概要とNECのQKD研究開発の取り組み

量子暗号とは?

量子暗号では、解読不可能なワンタイムパッド暗号に**量子鍵配送(QKD)**で共有した 乱数列を供給して絶対安全な通信を実現する



離散量(DV)と連続量(CV)の二つのQKD方式

QKDは量子状態受信方法によってDVとCVの2種類に大別される NECは**DV/CV双方QKD技術の適材適所で柔軟なQKDネットワーク構築を目指す**



NECのこれまでのQKD研究

NECは20年間にわたり研究を継続し、国内に主要研究拠点を持つ唯一の企業として総務省・情報通信研究機構(NICT)とともにQKD技術開発を牽引





2. NECにおける離散量(DV)-QKD実験の紹介

代表的DV-QKDプロトコルである偏波変調BB84の概要1

◆ 送信者Alice

■暗号鍵と基底の2ビットをランダムに選択し、偏波変調光をBobに伝送



▶ 受信者Bob

9

■ 基底1ビットをランダムに選択し、伝送光の偏波を読み取る



代表的DV-QKDプロトコルである偏波変調BB84の概要2



NECのtime bin変調デコイBB84装置

NECではより実用性を高めたtime bin変調デコイBB84装置の研究開発を行い 製品実用化を完了させている



NECのtime bin変調デコイBB84装置の光学ブロック図

time bin変調実装の概要1

光子パルスの時間&位相差に情報を載せるtime bin変調BB84により、ファイ バ伝送時偏波変動の影響を最小にしてシステム安定性を向上



time bin変調実装の概要2

光子パルスの時間&位相差に情報を載せるtime bin変調BB84により、ファイ バ伝送時偏波変動の影響を最小にしてシステム安定性を向上



13 © NEC Corporation 2024 量子ICTフォーラム第31回量子鍵配送技術推進委員会

\Orchestrating a brighter world NEC

デコイ変調実装の概要1

ランダムに送信パルス強度比を変えて光源の多光子発生確率を見積もり、理想的な単一光子発生器ではない光源に用いた際の安全性を確保



デコイ変調実装の概要2

ランダムに送信パルス強度比を変えて光源の多光子発生確率を見積もり、理想的な単一光子発生器ではない光源に用いた際の安全性を確保



BB84装置による社会実装の取り組み

BB84装置による社会実装を通じ、必要な場所に適切に安全に秘密鍵を提供するためのQKD周辺の様々な技術についても研究開発を実施





3. NECにおける連続量(CV)-QKD実験の紹介

連続量量子鍵配送(CV-QKD: Continuous Variable QKD)とは

CV-QKDはコヒーレント検波により量子光の直交振幅を読み出すQKD方式 CV-QKDにより小型・低コスト・波長多重可能な装置の実現が期待される



CV-QKD研究トレンドの遷移

QKD光とLO光の位相同期方法でこれまでのCV-QKD研究トレンド遷移を分類 広域QKDネットワーク実現を目指し、 NECはDSP CV-QKDの研究に注力している



DSP-CV-QKDによる広域QKDネットワークの実現

小型低コストで波長多重可能なDSP-CV-QKDにより、既存光ネットワークをフル活 用して広域QKDネットワークを実現する



NECのDSP-CV-QKD系の概要

既存光NWを活用した広域QKDネットワーク実現に向け、DSP-CV-QKD系を構築して既存信号光とCV-QKD光の最適な共存方法について研究を行っている







NECのDSP-CV-QKD系の最近の研究

DSP-CV-QKD光と高出力大容量信号光のガードバンド無し波長多重を行い、 既存光信号の運用に影響の無いCV-QKD導入が可能である見込みを得た



QKD波長への混入光強度の伝送距離特性

QKD波長混入光強度が距離に対して単調減少せず、 混入光成分のうち非線形光成分が支配的である事を確認した



波長多重伝送系における過剰雑音の特性評価

QKD波長への混入光のうち支配的なのは自発ラマン散乱光である事、 過剰雑音においても自発ラマン散乱光による雑音が支配的である事を確認した



高密度波長多重下でのCV-QKD秘密鍵生成率見積もり

27

ガードバンドレス波長多重下において0~75 kmで秘密鍵生成可能な事と、 秘密鍵生成率の距離特性は自発ラマン散乱光特性に基づき決まる事を明らかにした



発表のまとめ

◆ 離散量量子鍵配送(DV-QKD)装置と
連続量量子鍵配送(CV-QKD)装置のそれぞれについて
NECでの実装方法について概要説明を行った。



弊社のDV-QKD装置

◆弊社NECはDV/CV双方のQKD技術を有しており、 DV-QKDは製品実用化が完了し、

CV-QKDは既光NW活用した広域QKDネットワーク実現のための研究中である。

双方の方式の適材適所で柔軟で広域なQKDネットワーク構築を目指す

Orchestrating a brighter world

