

3.6.2 未来 ICT 研究所 量子 ICT 研究室

室長 佐々木雅英 ほか 12 名

量子情報通信技術の研究開発

【概要】

現在の情報通信技術は 19 世紀に確立された物理法則に基づいており、すでに光ファイバの電力密度限界や最新技術による暗号解読の危機が指摘されるなど、今後も次々と物理的限界を迎えることが予測される。このような限界を打破するため、究極の物理法則「量子力学」に基づいて、絶対安全な量子暗号通信（量子暗号技術）や従来理論の容量限界を打破する量子情報通信の研究開発（量子ノード技術）を自ら研究と産学官連携により戦略的に進めている。平成 26 年度は、量子暗号技術の研究開発で量子鍵配送システムの高信頼性動作実証に成功するとともに鍵管理アーキテクチャとアプリケーションの拡張を達成した。また、量子ノード技術の研究開発では、量子光源の性能改善により光量子回路を使った量子通信プロトコルを実証し、更に新しい量子通信プロトコル設計の指針となる量子通信レート原理限界の導出に成功した。

【平成 26 年度の成果】

(1) 量子暗号技術：量子鍵配送システム高信頼性動作実証と鍵管理アーキテクチャ・アプリケーションの拡張

新世代通信網テストベッド JGN-X にて小金井-大手町間での量子鍵配送システムの連続運転試験を実施した。平成 25 年度開発のアクティブ安定化回路を実装したデコイ BB84 プロトコルを、連続 34 日間のメンテナンスフリー動作を実現した。1 日あたり 25.8 Gbits（総鍵配信量は 878 Gbits）、平均通信速度は 300 kbps であり、量子暗号における 1 日あたりの暗号鍵配信量の世界最高値を達成した（図 1）。さらに都市圏敷設ファイバでの量子鍵配送安定性評価を進め、実運用時に予想される様々な外乱による性能揺らぎを評価し、それら装置が有する不完全性を相殺するための最新の理論を構築し、安全性評価基準項目の選定に着手した。

従来、離れたサイト間での情報交換が必要だった量子鍵配送装置の機器較正（光源揺らぎチェック）を 1 つのサイトで完結し、かつネットワークの冗長性も同時に担保する方法を新規に提案、試作を行った。さらに、量子鍵配送システムの冗長性を利用したシステムの自己診断機能アーキテクチャを確立するなど、システムの完成度を大幅に向上し、実用化に大きく前進した（図 1）。また、コヒーレント光・ホモダイン検波を用いた実装技術についても、鍵配送高速化、システム自動復帰機能付加等、実用上重要な新機能を実現した。

量子鍵配送システムへのサービス停止攻撃（いわゆる DoS 攻撃）に対して量子鍵配送用経路を複数本用意することにより対応する方法を開発した。経路上の異常検知とルート切替機能を従来のネットワーク管理機能に追加し、量子鍵配送通信路への攻撃検知の中央監視技術を確立、さらにリレー経路制御技術を開発した。

(2) 量子ノード技術：光量子回路による量子通信プロトコル実証と新プロトコル設計指針の導出

光量子回路の開発では、通信波長帯において波長幅 110 nm 以上の量子光源（超広帯域スキューズド光源）と、超広帯域・高感度光子数識別器を組み込んだ系を構築し、超広帯域スキューズド光の光子統計とモー

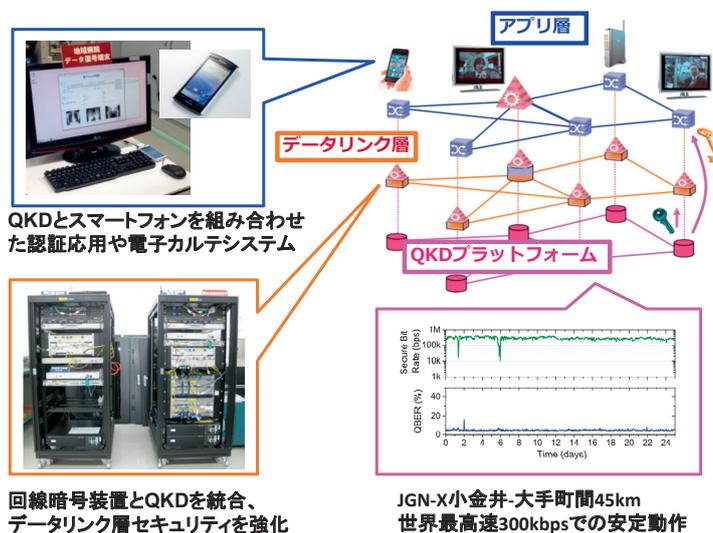


図 1 量子鍵配送システムのフィールド試験で 1 日あたりの暗号鍵配信量の世界最高値を達成（右）、鍵管理アーキテクチャのアプリケーションの拡張（スマートフォン、回線暗号装置等との統合）を実施（左）

分布の直接測定に世界で初めて成功した。また高速量子もつれ光源の光子回路への導入、さらに量子通信プロトコルの実証に取り組んだ。光源の高速化と、前年度までの光子検出器の改良により、量子通信の基本プロトコルの1つである「量子もつれ交換」プロトコルについて、通信波長帯で従来の1,000倍以上の高速動作で実証することに成功した。

新量子プロトコルとその実現に必要な基盤技術の開発では、量子中継を用いない光通信路における最も一般的な量子暗号・量子通信の理論モデルにおいて、いかなるプロトコルでも超えられない鍵生成レート・量子通信レートの原理限界を導出することに成功した。これは量子情報理論における15年以上の未解決問題の解決に向けて大きく前進させ、また今後の量子暗号プロトコルの設計においても重要な指針を与える成果である(図2)。

高純度量子光源の開発では、シリコンリング共振器を用いた量子もつれ光源を開発した。長距離伝送に適した時間位置変調信号での量子もつれ相関を、シリコンリング共振器方式としては世界で初めて確認し、さらに明瞭度92%超を達成した。また将来の超伝導素子の量子回路応用を見据え、無冷媒冷凍機の小型化を進め、従来比40%の小型化に成功した。さらに、本小型冷凍機に高感度超伝導光子検出器を実装し、差動位相シフト量子鍵配送装置の検出器として鍵生成実験を実施した。伝送損失30 dB(透過率0.1%)の敷設ファイバ伝送路を用いた実験において、1か月を越える正常動作を確認し、極めて安定に動作することを証明した。伝送損失30 dBを超える敷設ファイバにおける長期鍵生成成功は世界で初めての成果である。また、NICTが開発した高繰り返し光周波数コムレーザ(2.5 GHz)を用いた、通信波長帯における量子もつれ光源の高速化を実現した。量子もつれ光の純度を損なうことなく、従来光源の30倍以上の高速化に成功した。

与えられた光送信電力の下で最大容量の通信を実現する技術としての量子デコーダの設計理論と基本回路技術の研究開発では、光空間通信での実証に向けたプロトタイプ設計とテストベッド構築を完了した。基本動作試験を行い、様々な気象条件下での大気による信号擾乱の特性の観測に成功した。さらにその特性を説明する理論モデルの構築にも成功した。

次世代の量子鍵配送システムの開発では、NICT独自開発の有無線統合量子リンク(光空間-ファイバ統合型の量子もつれ鍵配送装置)において、時間位置変調信号の時間間隔を昨年度までの2.5 nsから0.8 nsとし、信号稠密化を実現した。さらに、開発した有無線統合量子リンク上に、量子もつれを用いた、現在主流のプロトコルBB84よりも高いサイドチャネル攻撃耐性を持つ変形E91プロトコルを実装した。検出器の高感度化により有無線統合リンクとしては世界最長のファイバ伝送距離(20 km)において、安全鍵生成が可能な量子もつれ相関を確認した。

光子や原子の極限的測定技術の開発と計測応用への実証では、インジウムイオンの波長230 nmの遷移を用いた量子論理分光法を開発し、イオン光時計への実装を実施した。更に高精度化を目指し波長159 nmの遷移を用いた次世代手法である真空紫外射影測定法の開発に着手し、基盤要素技術である真空紫外光源の開発に成功した。

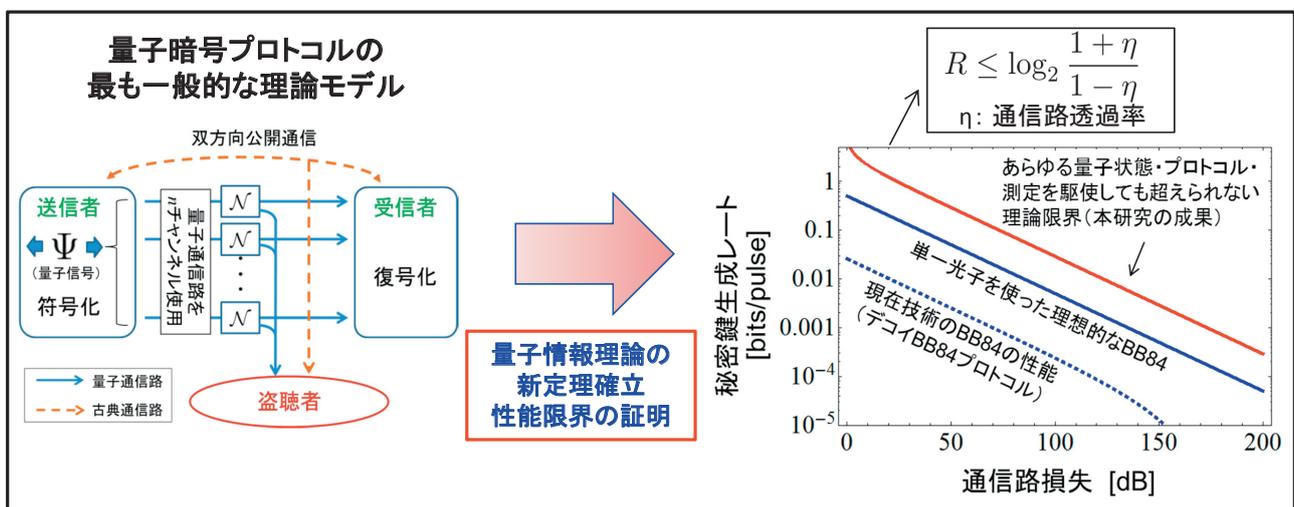


図2 鍵生成レート・量子通信レート原理限界の導出の概要。今後の量子暗号プロトコルの設計に重要な指針を与える成果。