3.6.2　未来 ICT 研究所　量子 ICT 研究室

室長　　佐々木雅英　ほか 11 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 27 年度は、量子暗号技術の研究開発で量子鍵配送プラットフォームに盗聴・異常検知及び自動回避機能を実装するとともに、量子暗号ネットワークテストベッド“Tokyo QKD Network”上で量子鍵配送システムの長期安定動作を実証、ユーザ環境での評価試験を開始した。量子ノード技術の研究開発では、量子ノード基本プロトコルである「量子もつれ交換」の速度を一気に 1,000 倍に改善することに成功した。

【平成 27 年度の成果】

（1）　量子暗号技術：量子鍵配送システムの長期安定動作実証とユーザ環境での評価、システム高機能化

NICT 自主研究及び委託研究を通じた産学官連携により、新世代通信網テストベッド JGN-X 及びその他の回線を活用して NICT が構築した都市圏量子ネットワークテストベッド“Tokyo QKD Network”を構築し、各参画機関の量子暗号装置の長期安定動作実証、相互接続試験を実施した（図 1 上）。また、盗聴検知・リルーティング等の新しいネットワーク機能の実証試験等も実施した（図 1 下）。

量子鍵配送（QKD）装置から共通鍵暗号（AES）装置へ暗号鍵を高頻度（最大 1 秒ごと）で供給し、データレイヤ上の重要通信を直接、高速暗号化（100 M ～ 1 Gbps）する統合型暗号化システム（QKD-AES ハイブリッドシステム）を開発した。このシステムを、Tokyo QKD Network 上の小金井−府中をつなぐ敷設ファイバに導入し、長期安定性評価を実施、1 カ月以上の安定動作を実現した。さらに、実用化に向けた評価実験として、都内の NEC のサイバーセキュリティ対策の中核拠点「サイバーセキュリティ・ファクトリー」内で、平成 27 年 7 月に長期安定性試験を開始し、順調にデータを蓄積している。また、システムの干渉計光路長、偏光及び検出同期を能動的に安定させ、かつサイドチャネル攻撃対策を組み込んだ「第三世代」と呼ばれる QKD 装置を開発した。このシステムには重要部品の故障モニターと自動スタート機能も導入し、Tokyo QKD Network の小金井−大手町間敷設ファイバで長期安定動作を実証した。さらにこのシステムを、仙台市の東芝ライフサイエンス解析センターと東北大学東北メディカル・メガバンク機構をつなぐゲノム解析データの暗号通信へ導入し、こちらもユーザ環境での実証試験を平成 27 年 8 月に開始した。これらのユーザ環境での運用試験のデータ蓄積は、実用化へ前進するための重要な実績となった。

一方、将来の実運用上の重要課題を把握するための産業界等への聞き取り調査を進め、その結果に基

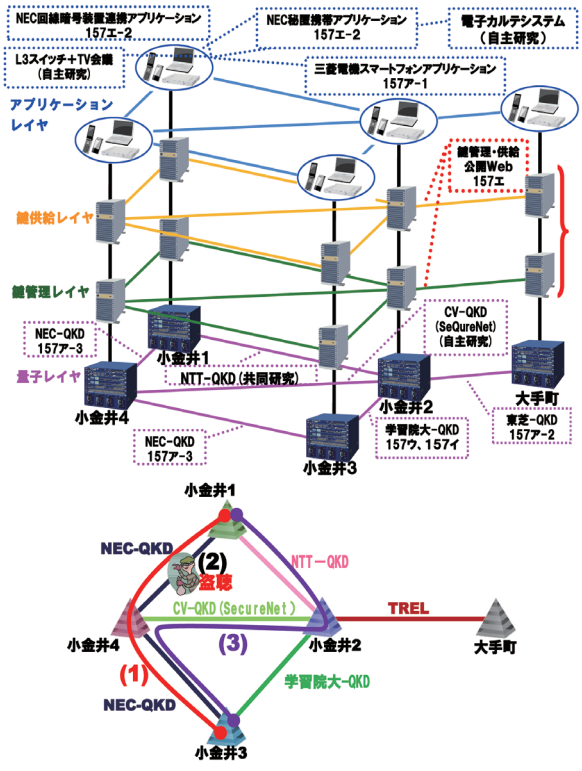


図 1　NICT 自主及び委託研究により構築された Tokyo QKD Network（上）と、盗聴検知自動リルーティング機能の概要（下）

づき、サービス停止（DoS）攻撃への耐性向上とバックアップ回線の確保に向けた盗聴検知・自動リルーティングや通信路上での異常診断機能を備えた鍵管理及び多様なアプリを実現する鍵供給インタフェースのアーキテクチャを開発した。これらの機能は Tokyo QKD Network 上でのフィールド実証試験を開始している。

量子暗号技術の中の要素技術である乱数生成技術及びワンタイムパッド暗号化を切り出し、ドローンの飛行制御通信の安全性を強化する技術を開発した。さらに、量子鍵配送プラットフォームで複数の地上局に暗号鍵を配送し、地上局間で安全に飛行制御を引き継ぐセキュア制御通信技術の実証実験に成功した（図 2）。量子暗号関連技術の早期実用化に道筋をつける重要成果となった。

また、9 月に東京の一橋講堂において 2 つの国際会議 The 4th International Conference on Updating Quantum Cryptography and Communications（UQCC2015）、及び 5th International Conference on Quantum Cryptography（QCrypt2015）を主催し、日本の産学官連携の研究開発成果の発信や世界の最先端研究開発成果の共有、実用化に向けた展望と課題についての討論などを行った。両会議の参加者はそれぞれ 300 人を超え、当該分野の会議としては最大規模のものとなった。

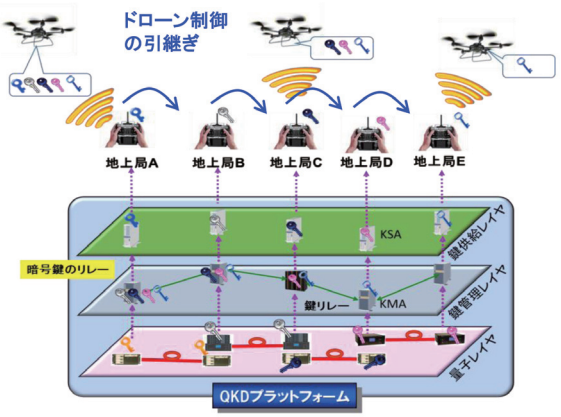


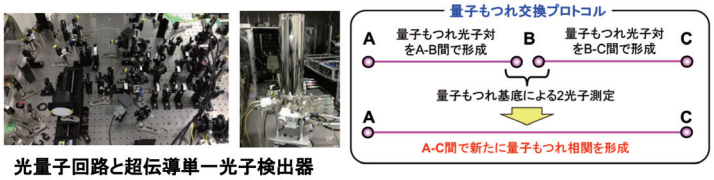
図 2　QKD プラットフォームで複数の地上局に暗号鍵を配送し、地上局間で安全に飛行制御を引き継ぐセキュア制御通信技術の実証実験概要

（2）　量子ノード技術：量子ノード基本プロトコルの実証と超高速化

平成 26 年度までに開発を進めてきた高速量子光源と低雑音高効率の超伝導単一光子検出器を用いて光量子回路を構成し、量子ノード技術の基本プロトコルである「量子もつれ交換」プロトコルを構築、通信波長帯において従来の 1,000 倍以上の高速動作の実証に成功した（図 3）。また、量子光源の特性を評価する一般的な手法である Hong-Ou-Mandel 干渉を周波数分解して測定する技術を開発し、独立した 2 つの量子光源から生成された光子間の量子干渉後の相関スペクトルの観測に初めて成功した。これにより量子光源の特性改善の重要技術を確立した。一方、量子光源において量子もつれの性質を壊す複数光子対生成の影響を定量的に予測し得る新しい理論を確立し、上記実験結果の定量的なモデリングを行うことにも成功した。

また、理論的にイオン光周波数標準に最も優れたイオンとされる、インジウムイオン（In^+）を用いた標準技術確立に取り組んだ。カルシウムイオン（CA^+）のレーザー冷却を介して In^+ を冷却する共同冷却法を用いた光周波数標準（光時計）動作の確認に成功し、NICT 時空標準研究室への技術移転を完了した。

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量子デコーダ技術のフィールド実証に向けて、NICT– 電気通信大学間（約 8 km）を結ぶ光空間通信テストベッドを構築し、微弱光信号のフィールド伝送試験を実施、空間通信路における大気の影響などの解析に取り組んだ。



光量子回路と超伝導単一光子検出器

年度	研究機関	一秒当たりの量子もつれ交換成功率	干渉の明瞭度
2005	ジュネーヴ大学	0.004	80%
2009	NTT	0.038	64%
2012	産総研	0.016	75%
2013	日本大学	0.08	92%
2015	**NICT・電通大**	**108**	**78%**

従来の1,000倍以上の高効率化を実現

図 3　量子もつれ交換プロトコルの概要と成果
（左上）光量子回路と検出器の外観、（右上）量子もつれ交換の概念、（下）本研究成果と過去の成果の比較