3.6.2　未来 ICT 研究所　量子 ICT 研究室

研究室長　　佐々木雅英　ほか 8 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事が予測される。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を産学官連携により戦略的に進めている。平成 24 年度は、より安定な量子鍵配送と新しいセキュリティ技術の実証、量子信号処理の利得増強の実証などの研究開発を実施した。

【平成 24 年度の成果】

(1) 量子暗号技術：より安定な量子鍵配送と新しいセキュリティ技術の実証

産学連携により、都市圏敷設光ファイバ環境に構築してある量子鍵配送テストベッド Tokyo QKD Network を用いて、量子鍵配送のデータを蓄積して安定動作試験を進め、装置変動や気象データとの相関解析により、特性変動の主要因を解明し動作の安定度を向上させた（図 1）。

暗号システムの実装では、装置の動作状況などを外部から観察・測定することにより情報にアクセスするサイドチャネル攻撃の存在が重要な問題となる。

種々のサイドチャネル攻撃の危険度を解析した結果、危険度の高い攻撃として、強い光を照射することで光子検出器を動作不能にしてしまう、いわゆる明光照射攻撃がまず挙げられることが分かった。そこで実際に明光照射攻撃実験を実施して問題点を分析し、有効な解決策（光子同時計数ユニットの追加）を開発して、その効果を実証した。産学連携により、安全性の定量的評価に必要な評価項目として、送信機の変調器特性の変動幅、復調干渉系の温度変化、半導体検出器のバイアス点変動、及び受信機に入り込む背景光の光量が重要であることを明らかにした。さらに、年度計画を上回る成果として、サイドチャネル攻撃の影響を低減できる量子もつれ鍵配送方式の基本設計を行うとともに、光源のスペクトル純度を向上させ将来の量子ネットワークの長距離のリレー機能実現に必要な 4 光子同時計数の計数率を従来比 30 倍以上に改善し世界記録を達成した(図 2)。

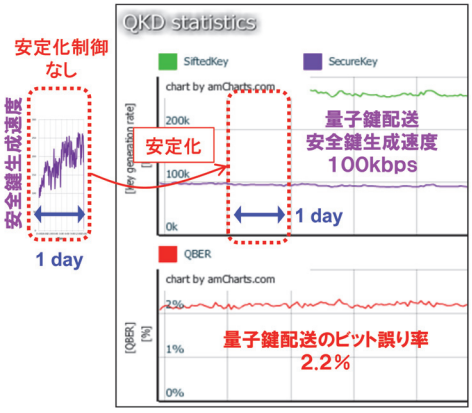

図 1　特性変動の主要因を解明し、安定度を向上させた動作を表示する量子鍵配送管理システムのモニタ画面

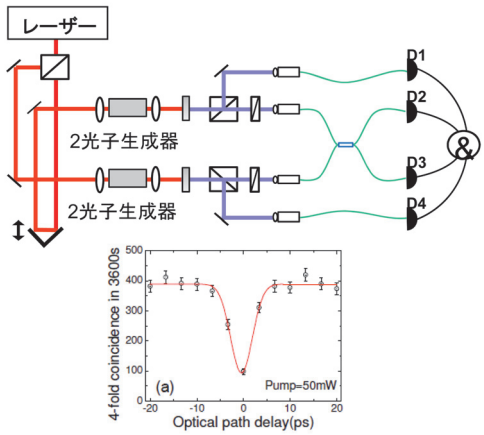

図 2　4 光子同時計数の計数率を従来比 30 倍以上に改善し世界記録を達成

量子鍵配送を用いたノード認証技術などの新たな応用の創出やセキュリティ機能拡張に向けた研究開発として、拠点間通信を制御するレイヤ 3 スイッチの上で、ペイロードとユーザ IP アドレスを量子鍵配送により暗号化し、さらに最新の現代暗号技術（ユニバーサルハッシュ関数）を組み合わせることで情報理論的に安全なメッセージ認証及びデータ秘匿化を同時に実行できる新しいセキュリティ技術を考案し、Tokyo QKD Network 上で実装した。さらに、年度計画を上回る成果として、量子鍵配送の秘密鍵をスマートフォンへ供給し、ネットワーク上の重要情報にアクセスする際のマルチユーザ認証やアクセス権限のマルチ階層化に利用して、データ保存時及び閲覧時の安全性を向上させる技術を開発した(図 3)。

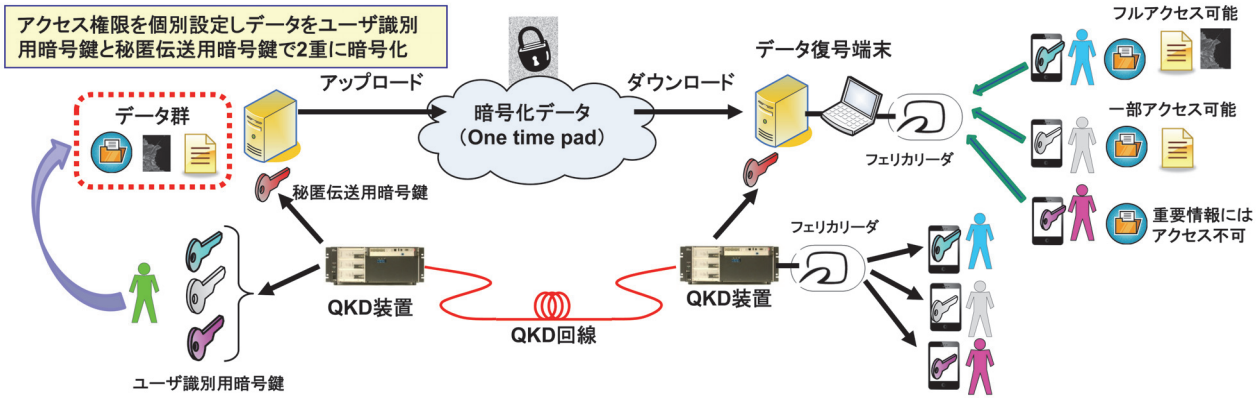

図 3　量子鍵配送（QKD）の秘密鍵をスマートフォンへ供給し、データ保存時及び閲覧時の安全性を向上させる技術を開発

(2) 量子ノード技術：量子信号処理の利得増強の実証

量子デコーダの基盤技術として、量子信号処理回路と超伝導単一光子検出器とを組み合わせた通信波長帯の受信回路を構築した。特に、小型化に向けた開発を前倒しで進め、将来有望と考えられるシリコン導波路基板による回路構築を実現した。さらに、リング型導波路の非線形効果も新たに活用することにより、量子信号処理における利得増強に有用な量子相関（2 光子同時計数）の検出に成功して、年度計画を上回る成果を達成した（図 4）。

量子信号処理の利得増強のため、量子重ね合わせ状態を用いた量子テレポーテーションにより利得 3 倍の信号増幅転送技術の開発に成功した。産学連携により量子中継の要素技術として、半導体素子を用いてスピン－光子量子もつれ状態を生成することに世界で初めて成功し国際的著名誌 Nature で発表した。

導波路型スクィーズド光源を高品質化するとともに、その特性を高精度で検出するためのホモダイン検出器の最適化手法を確立した（図 5）。

光子数識別能力を持つ超伝導転移端センサの高感度化を行い、20 光子までの広範囲で明瞭な光子数識別に成功し、スクィーズド光との低損失結合技術を開発した（図 6）。

極限計測技術において、インジウムイオン時計遷移の読出し法として従来の相関測定技術よりも簡便なマクロ振動励起法を独自に考案し予備実験に成功するとともに、真空紫外光出力の従来比 3 倍の高出力化と独自手法による周波数安定化実装に成功した。

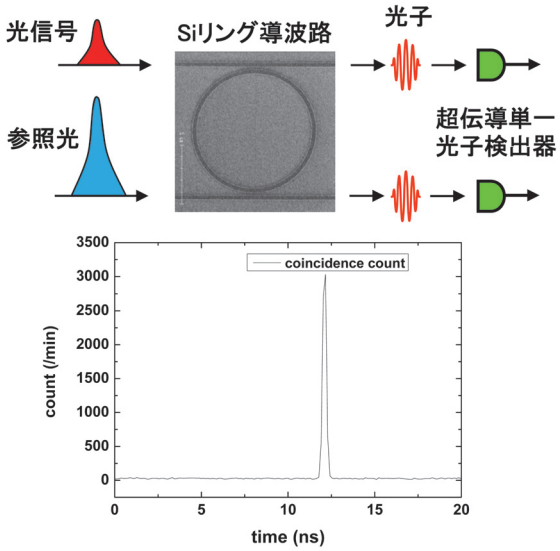

図 4　リング型導波路での 2 光子同時計数の検出に成功

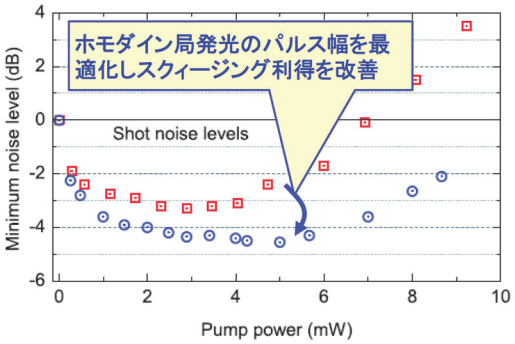

図 5　ホモダイン検出器の最適化手法を確立

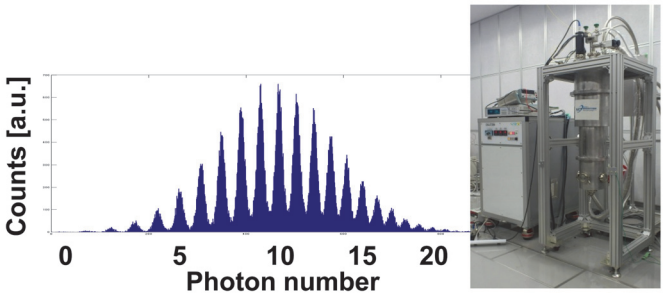

図 6　超伝導転移端センサにより 20 光子までの光子数識別に成功