

3.1.4 新世代ネットワーク研究センター 量子 ICT グループ

グループリーダー 佐々木雅英 ほか7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。

量子暗号通信は、送受信者間で絶対安全な鍵を共有するための量子鍵配送技術がキーになる。単一光子、或いは特殊な結びつきをもった一対の光子である量子もつれ状態で鍵を送信する技術の研究を行っている。

量子情報通信は、量子力学を用いて現在の光通信の様々な性能限界を乗り越え、大容量かつ安全な通信を実現するための新世代ネットワーク技術として期待されている。ネットワーク上のさまざまな場所で量子もつれによる結びつきを共有する事が出来れば、超並列計算や盗聴不可能な暗号通信、さらには低電力・大容量通信実現の道が拓かれる。

【平成22年度の成果】

(1) 量子暗号通信：量子暗号ネットワークの試験運用を開始

量子暗号は、理論上どのような技術でも盗聴できない究極の暗号技術である。その方法はまず、送り手と受け手に量子鍵配送装置を用意し、光回線を介して盗聴を完全に排除した絶対安全な秘密鍵を共有する。次に、一度使用した鍵は二度と使わないワンタイムパッド方式で送りたい情報を暗号化する（図1）。量子鍵配送は極めて高度な技術で、実用化には多くの課題があり、これまでのアメリカ国防総省や欧州連合のプロジェクトでは、データ量の少ない音声データの暗号化が限界で、伝送距離も敷設ファイバで数10km程度が限界だった。我が国では2001年からNICTの産学官連携プロジェクトにより、都市圏で完全秘匿テレビ会議が実現できる世界最高速の量子鍵配送技術の研究開発に取り組んできた。

平成22年度は、上記プロジェクトの10年目に当たる。量子ICTグループは、この間の自主研究の成果を基にNICT委託研究の受託機関である日本電気株式会社、三菱電機株式会社、日本電信電話株式会社と共に、NICTのテストベッドJGN2plus上の4つの拠点に量子鍵配送装置を設置し、10kmから最長90kmまで複数の回線パターンからなる量子暗号ネットワーク（Tokyo QKD Network）を構築し、様々な盗聴攻撃の検知実験、及び完全秘匿なテレビ会議システムの試験運用を行った（図1）。未来ICT研究センターのナノICTグループとともに開発した超伝導光子検出器を量子鍵配送装置に組み込むことで、45kmの光ファイバ回線で每秒約10万ビットと、実環境では世界最高速の秘密鍵生成速度を達成した。また、併せて、国際標準化に向け、ヨーロッパの研究機関（東芝欧州研究所、ID Quantique、オーストリア工学研究所、量子情報・量子光学研究所、ウィーン大学）のシステムとの相互接続実験も行い、最新のアプリケーションインターフェースを開発した。

関連の成果は、NHKニュース、ワールドビジネスサテライトなどのテレビ、毎日新聞、日本経済新聞など14紙の新聞、日経サイエンス（11月号）、Nature Photonics（1月号）などの4つの専門誌ニュース欄、及び39のウェブサイトで紹介された。

今後、さらに技術改善を進めるとともに試験運用を継続して、国家レベルの機密通信、電力・ガス・水道網などの重要インフラを監視する通信保護や、金融機関の秘匿通信等に順次適用できるよう取り組んでいく。

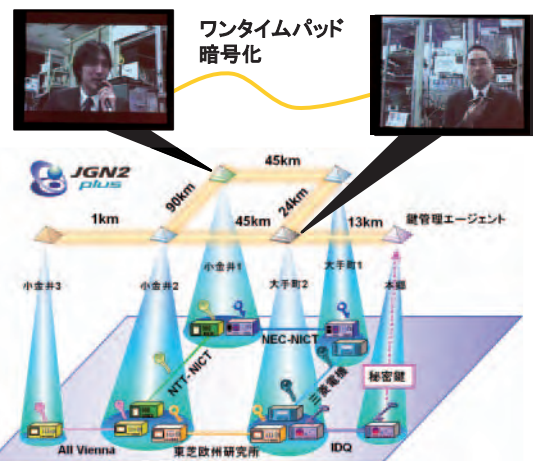


図1 量子暗号ネットワーク (Tokyo QKD Network) と盗聴不可能なテレビ会議システム

(2) 量子情報通信：将来のネットワークノード内で光信号を量子的に制御する基礎技術を開発 ～連続量量子ビットを世界で初めて実現～

従来のデジタル情報は0か1のどちらかの状態しかとることができないが、量子情報技術では0と1だけでなく“0でもあり同時に1でもある”重ね合わせ状態もとることができる（図2上部）。この新しいデジタル信号は量子ビットと呼ばれ、従来不可能だった超並列計算を可能にする。これまで光の量子ビットには、光の粒子としての特性である光子の偏光が利用されていたが、光ファイバ伝送に適した信号形態ではないため応用用途が限られていた。

平成22年度は、光ファイバ伝送で使われている光の波動性を利用した光波信号で量子ビットを構成することに世界で初めて成功した（図2下部）。光ネットワークの中継地点の装置（ノード）に量子ICTを導入する際の重要な基盤技術となる。量子ビット自体は損失に弱く長距離伝送が難しいが、光ネットワークのノード内において局発光として利用することで従来の伝送容量の限界であるシャノン限界を超える通信が可能になる。多数の量子ビットをノードで用意し、光波信号と干渉させながら情報を復号する量子デコーダを開発できれば究極の容量限界であるホレボー限界が実現できる。

本成果は、物理学の専門誌としても最も権威がある「Physical Review Letters」に掲載された。さらに、アメリカの光学学会の月刊誌「Optics and Photonics News」の12月号において、2010年の光学分野における主要成果“Optics in 2010”の1つに選ばれ、雑誌の表紙を飾った（図3）。表紙の図は、量子ビットの表現法であるポアンカレ球である。従来の偏光量子ビットは、2次元の系のためポアンカレ球上の位置ですべての性質が表現できるのに対し、光波量子ビットは連続値を取る無限次元系であるため、各点には連続量の波動関数（カラーのとんがり帽子のような分布関数）が付随している。

(3) 成果展開：イオンの冷却技術を光周波数標準へ

量子情報通信の基礎技術として開発していたカルシウムイオン冷却技術を高度化するとともに、小規模量子計算を利用した量子論理分光法に基づく次世代光周波数標準システムとして、インジウムイオン-カルシウムイオン複合系の共同冷却技術を開発した（図4）。今後、光・時空標準グループと協力し、新しい光周波数標準の実現へ向けて、さらに精度改善とシステム化を行う。

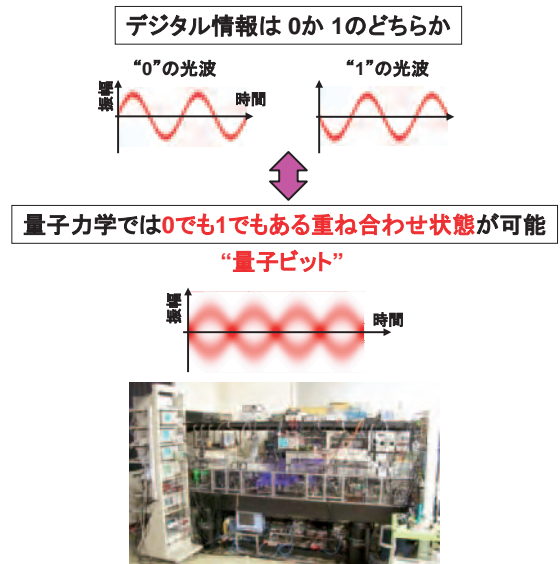


図2 上部：従来のデジタル情報と量子ビットの違い
下部：光波信号で量子ビットを生成する実験装置の写真
スクイーズド光と光子検出器からなる量子信号処理回路を用いて光波信号で量子ビットを生成する。



図3 Optics and Photonics News 誌12月号の表紙

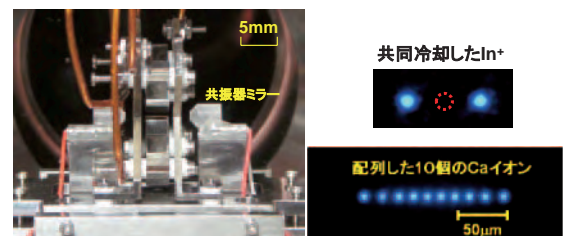


図4 冷却イオン制御系（左）と冷却されたカルシウムイオンやインジウムイオン