

- **単一光子源量子暗号システムで世界最長の80kmの原理検証実験に成功**  
BB84プロトコルを使用した量子暗号システムの安全性を強化
- 平成19年1月15日

三菱電機株式会社(執行役社長:下村 節宏、以下「三菱電機」)ならびに北海道大学(総長:中村 睦男、以下「北大」)は、BB84プロトコル※1を使用した量子暗号システムとして、単一光子源を組み込んだ高精度な量子暗号通信装置を共同開発し、世界最長の80kmの量子暗号原理検証実験に成功しました。

この研究は、三菱電機は情報通信研究機構(理事長:長尾 真、以下「NICT」)の委託研究「量子暗号の実用化のための研究開発」の一部として、北大は科学技術振興機構(理事長:沖村 憲樹、以下「JST」)の戦略的創造研究推進事業(CREST)「量子情報処理システムの実現を目指した新技術の創出」領域の一環として実施しました。

※1 BB84: C.H.BennettとC. Brassardが1984年に提案した量子暗号プロトコル

## 【開発の背景と概要】

「現代暗号」と呼ばれる現在の暗号技術(暗号アルゴリズム)は、解読するために膨大な計算量(時間)が必要であることを安全性の根拠にしており、超高速処理が可能な量子コンピューター等が出現した場合には、この安全性が脅かされると指摘されています。

これに対して「量子暗号」は、盗聴されたことを検知できるという「現代暗号」には無い特長があることから、絶対に解読されない究極の暗号として実用化が期待されています。しかし、これまでの量子暗号通信システムのほとんどが、光源としてパルスレーザーを弱めた擬似的な単一光子源を用いているため、同じ情報を運ぶ光子が同時に2個以上発生する確率が無視できず、そのうちの1個を取り出して情報を盗聴され、暗号を解読される可能性があることが判明しています。

今回、同時に2個以上の光子が発生する確率を1万分の1以下に抑えた「単一光子源」を北大が開発し、三菱電機がこの「単一光子源」を組み込んだ高精度な「量子暗号通信装置」を開発して、共同で「単一光子源を実装した量子暗号システム」として世界最長の80kmの原理検証実験に成功しました。

## 【主な開発成果】

1. **同時に2個以上の光子が発生する確率が1万分の1以下の「単一光子源」を開発**(北大・JST)  
従来「擬似単一光子源」として多く用いられている微弱なパルスレーザー光源は、同一時刻に複数個の光子が発生する確率が無視できず、そのうちの1個を取り出されると、盗聴されたことを検知できずに、暗号が解読される可能性があります。今回北大電子科学研究所竹内繁樹助教授らは、非線形光学効果を利用した「単一光子源」を開発し、2個以上の光子が発生する確率が1万分の1以下という通常の微弱パルスレーザー光源では実現できない精度を達成しました。
2. **精度と安定性に優れた「量子暗号通信装置」を開発**(三菱電機・NICT)  
従来三菱電機は光子源に取り扱いの容易なパルスレーザーを用いていましたが、今回北大の開発した単一光子源を組み込み、伝令信号と呼ばれる電気信号と時間精度の高いクロック信号を併用することによって、単一光子検出の精度と安定性に優れた「量子暗号通信装置」を開発しました。
3. **安全性の厳密な定量評価方法を開発し、世界最長の80kmの通信を確認**(三菱電機・北大・NICT・JST)  
これまで単一光子源を利用する量子暗号システムの評価は、単一光子源の特性に依存するため定量的に評価できていませんでしたが、今回、光子生成プロセスまで踏み込んで漏洩情報量を定量的に見積もる方法を開発しました。また、単一光子源による世界最長の80kmの原理検証実験(単一光子干渉実験)を行い、この評価方法を用いて80kmで安全に通信できることを確認しました。

## 【今後の展開】

今後は今回開発した技術をベースに、装置の小型化および高速化に取り組み、5年後を目標に単一光子源を用いた量子暗号装置の実用化を目指します。

**【開発内容の詳細】**

従来の微弱なパルスレーザー光源を用いた盗聴可能性の残る方式に比べ、今回の単一光子源を用いた方式は2光子発生確率が1万分の1以下という光源の完全性によって安全性が保障されます。世界最長となる80kmの量子暗号原理検証実験の成功により、共同開発した単一光子源を組み込んだ量子暗号通信装置の有効性も実証されました。

**表1. 単一光子に関する比較**

項目	今回(北大・JST)	従来(MagiQ社)	従来(三菱電機・NICT)
光子源	単一光子源	単一光子源	微弱レーザー光源
光子源の駆動方式	パルス光駆動	連続光駆動	パルス駆動
光源の完全さ 光子の生成 2光子発生確率 (盗聴の原因)	完全 1個ずつ生成可能 0.0001以下	完全 1個ずつ生成可能 不明	不完全 2個出ることがある 0.005
光子源の規則性	規則的(O)	ランダム(X)	規則的(O)
量子リピーターとの接続性 (距離の延伸)	可	不可	不可
量子暗号プロトコル	BB84※2	BB84	BB84
通信距離	80km※2	76km	96km

※2 三菱電機がNICTとの委託研究の一部で実施

図1は単一光子源を組み込んだ量子暗号通信装置の構成と仕組みを表す図です。左端の単一光子源から出た単一光子が光学装置を経由して光子検出装置へ送信されます。量子暗号送信装置と受信装置は、飛んできた光子を乱数情報に従いBB84プロトコルで量子変調および量子復調します。光子検出装置では、送られてきた光子をビット列に変換して出力します。このビット列をデータ処理することで送信者と受信者は安全に秘密データを共有することができます。

単一光子源は、単一光子を送信する際、単一光子と同時に伝令信号と呼ばれる電気制御信号を送信します。受信装置では、伝令信号を受信することで単一光子が送られてくる時刻を把握し、光子検出器の検出タイミングを制御します。さらに伝令信号と同期した時間精度の高いクロック信号も利用することにより、受信側での高精度かつ安定的な光子検出に成功し、通信距離80kmの原理検証実験に成功しました。

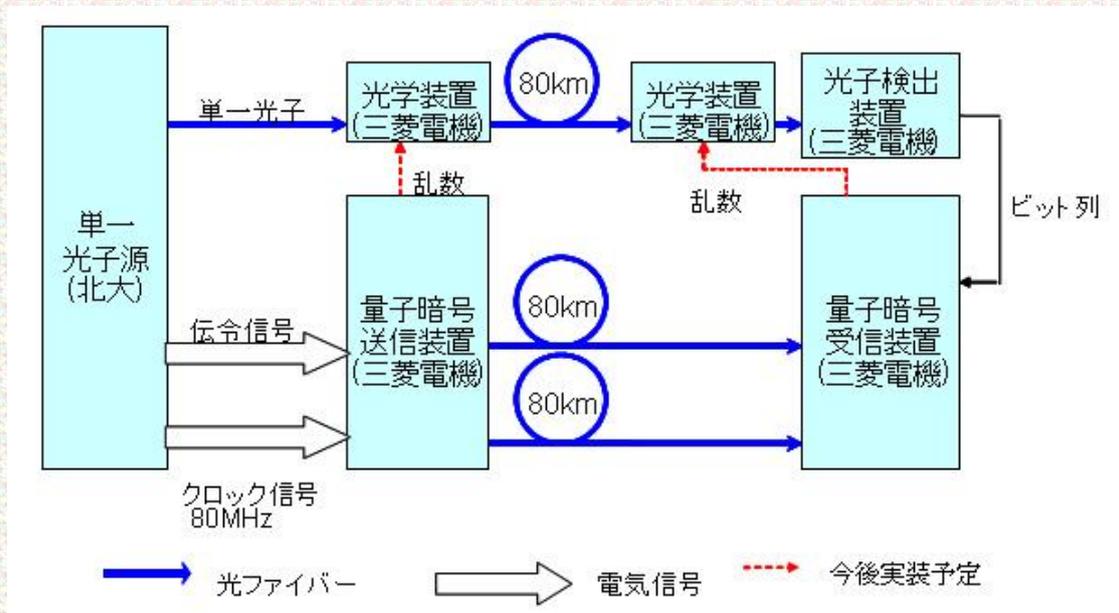


図1. 単一光子源を組み込んだ量子暗号通信装置

< お問い合わせ先 >

**三菱電機株式会社**

< 報道関係からのお問い合わせ >

広報部

〒100-8310 東京都千代田区丸の内二丁目7番3号

電話: 03-3218-2333 FAX: 03-3218-2431

< 開発内容に関するお問い合わせ >

情報技術総合研究所 計画部 業務グループ

〒247-8501 神奈川県鎌倉市大船5-1-1

FAX: 0467-41-2142

[http://www.mitsubishielectric.co.jp/corporate/randd/inquiry/index\\_it.html](http://www.mitsubishielectric.co.jp/corporate/randd/inquiry/index_it.html)

**北海道大学**

電子科学研究所 庶務係

〒060-0812 北海道札幌市北区北12条西6丁目

電話: 011-706-3195 FAX: 011-706-4977

**独立行政法人情報通信研究機構 (NICT)**

〒184-0012 東京都小金井市貫井北町四丁目2番1号

<広報 お問い合わせ>  
NICT総合企画部 広報室  
栗原則幸、大野由樹子  
電話:042-327-6923 FAX:042-327-7587

<委託研究に関する問合せ先>  
NICT連携研究部門 委託研究グループ  
天野滋  
電話:042-327-6011 FAX:042-327-5604

**独立行政法人科学技術振興機構**  
広報・ポータル部 広報室  
〒102-8666 東京都千代田区四番町5-3  
電話:03-5214-8404 FAX:03-5214-8432

---