報道発表

- **都市圏敷設ファイバーで世界最長、最高速の量子暗号鍵配送に成功**
  ～将来の極めて安全性の高い暗号鍵*1配送技術の実現へ向けて大きく前進～

- **平成20年3月26日**

独立行政法人情報通信研究機構（以下「NICT」という。理事長：宮原 秀夫。）は、量子力学の法則を使った新しい暗号技術（量子暗号*2）を、道路沿いに設置された光ファイバー回線を用いて、世界最長（97km）かつ最高速（従来比で100倍）で実現することに成功しました。

現在インターネット上で使われている暗号技術は、公開鍵暗号と呼ばれる方式で、コンピュータの能力が飛躍的に向上すると、解読される危険性をはらんでいます。ところが、量子暗号は将来どんなに科学技術が進歩しても、絶対に盗み見られない特徴を持っています。

最近、情報システムからの機密情報の流出が問題となっており、重要情報を一元管理するデータセンターと利用者の端末間で、秘匿性の高い通信ネットワークを構築しようとする動きが広がっています。今回の量子暗号方式は、そうしたネットワーク上での利用に適しています。

これまでの量子暗号の研究は、ほとんどが実験室内の理想的な環境で行われていましたが、今度の実験は前述のとおり、道路沿いに設置された光ファイバーを用いて（フィールド実験）実施しました。今回達成した性能は、これまでの実験室内での記録をさらに10倍上回るもので、将来の極めて安全性の高い暗号技術の実現に向けて大きく前進する成果となります。

【背景】

近年、インターネット上での安全な商取引や個人情報の保護、機密情報の流出防止など、情報の安全性確保に対する要求が高まっています。現在一般に使われている公開鍵暗号は、盗聴しようとしても暗号の解読に膨大な時間がかかることを利用しています。しかし、この方式は、将来、新しい解読法が発見されたり、コンピュータの能力が飛躍的に向上すると、解読される危険性を有しています。

そこで、将来的に技術が進歩しても絶対に破られることのない次世代暗号技術として、量子暗号が注目されています。量子暗号では、微弱な光が持つ粒子（光子）の物理的性質を暗号鍵として利用します。光ファイバーを使い、情報の送り手と受け手であらかじめ暗号鍵を共有して、この鍵を使って情報を暗号化します。共有作業の途中で誰かが鍵を盗むと光子の状態に必ず痕跡が残り、受け手が盗聴を必ず検知できる仕組みです。この鍵を共有するための技術を特に"量子暗号鍵配送"と呼びます。これによって、将来どんなに科学技術が進歩しても、絶対に盗み見られることのない安全な情報伝送を保証する暗号通信が可能になります。

【量子暗号の研究開発の現状】

絶対安全な量子暗号の実現には、光子を制御する高度な技術が要求されるため、インターネット上での実用化にはまだ至っていません。実際の敷設光ファイバーで、量子暗号鍵配送を実現するためには、時々刻々変動する条件のもとでも、送り手から受け手へ正確なタイミングで光子を安定に伝送し、雑音の影響を抑えて正確に光子を検出できなければなりません。

しかし、これまでの量子暗号システムのほとんどは、実験室内に設置したコイル巻き状の光ファイバーを用いて実験されており、それでもファイバー長が100 kmを超えると、絶対安全な鍵の生成速度は1秒当たり数10ビットまで下がってしまうのが現状でした。また、鍵の生成速度を無理に上げると、ごく限られた盗聴法に対してしか安全性を保証できなくなるという難点もありました。さらに、送り手と受け手のタイミング合わせも、数メートル以下の電気ケーブルに限定されるなど、実用化には遠い実験となっていました。

【本成果の概要】

今回の成果は、実際の敷設光ファイバーで97kmにわたり、絶対安全性を保証する「おとり信号付きBennett-Brassard 84*3」と呼ばれる暗号方式を用いて、世界最高の鍵生成速度（1秒当たり700ビット）を達成したものです。これは従来の室内実験に比べても10倍、敷設光ファイバー実験では100倍以上の向上に相当します。

大幅な性能改善を実現した技術は、以下の3つに集約できます。

（1）伝送途中での光子への擾乱をうまく相殺し、高い明瞭度で光子の暗号鍵を判定できる光回路（平面光回路量子干渉計）を開発したこと。

（2）従来より高速かつ極めて低雑音で光子を検出できる超伝導単一光子検出器*4を開発したこと。

（3）一本の光ファイバーの中で、光子の伝送を邪魔することなく、送り手と受け手で正確にタイミングを合わせる技術（量子波長分割多重伝送技術*5）を開発したこと。

これらの技術を集積し、現在最高の安全性を保証する量子暗号鍵配送方式を敷設光ファイバー上で世界最長かつ最高速に動作させることに成功しました。

【本成果の意義】

今回の成果は、政府や金融機関のネットワークで、機密性の高い通信を実現する基盤技術として期待されています。特に、最近では情報システムからの機密情報の流出が問題となっており、重要情報を一元管理するデータセンターと利用者の端末間で秘匿性の高い通信ネットワークを構築しようとする動きが広がっている中で、今回の量子暗号鍵配送方式を応用し、そうしたネットワーク上での鍵配送に役立つものと考えられます。

【今後の展開】

実用化にあたっては、暗号システムの動作をさらに安定化させ、鍵生成速度も現状から1,000倍程度向上させる必要があります。今回、そのために必要な技術課題が明確になり、数年以内に政府安全保障レベルの量子暗号鍵配送システムを実現するという目標が射程圏内に入ってきました。今後もNICTが中心となり、関係機関と連携して装置の小型化・低コスト化を進め、実用化に向けた研究開発を加速させていきます。

― 研究開発の背景 ―

今回の成果は、日本電気株式会社（以下「NEC」という。代表取締役社長:矢野 薫。）がNICTの委託研究「量子暗号の実用化のための研究開発-課題イ-1 都市圏量子暗号ネットワーク技術-」の一環として開発した量子暗号システムと、NICT及びNIST（National Institute of Standards and Technology、米国コロラド州。）が共同開発した高速かつ低雑音の超伝導単一光子検出器、さらに3機関共同で開発した量子波長分割多重伝送技術を用いて、NECとNISTが、NICTの有する敷設光ファイバー施設（JGN2）においてフィールド実験を行った結果です。

尚、上記委託研究は、NEC、日本電信電話株式会社(NTT)、三菱電機株式会社により研究開発が行われているテーマです。

＜ 広報　問い合わせ先　＞
情報通信研究機構　広報室
栗原 則幸
Tel:042-327-6923
Fax:042-327-7587

NEC　コーポレート・コミュニケーション部
大戸 和人
Tel:03-3798-6511 （直通）

＜ 本件に関する 問い合わせ先 ＞
情報通信研究機構
新世代ネットワーク研究センター
光波量子・ミリ波ICTグループ
佐々木 雅英
Tel:042－327-6524
Fax:042－327-6629

補足資料1

＜ 用語 解説 ＞

*1　暗号鍵

送り手と受け手の間で、情報を第3者に盗み見られないように暗号化する道具。

*2　量子暗号

微弱な光が持つ粒子（光子）の物理的性質を暗号鍵として利用。

*3　おとり信号付きBennett-Brassard 84

1982年にBennettとBrassardがはじめて提案した量子暗号鍵配送方式をBB84と呼ぶ。これは、光子を4種類の状態のどれかにランダムに変調して鍵を載せるもので、1990年代に絶対安全性の証明が与えられた。その後、送り手がさらに光子の元となる微弱光にランダムな強度変調を加えることで、装置の不完全性があっても、安全性を高められることがわかり、おとり信号付きBB84と呼ばれている。

*4 超伝導単一光子検出器

幅100ナノメートル（1ナノメートルは10億分の1メートル）ほどの窒化ニオブ超伝導体の細線に、光ファイバーから単一光子が入射すると、超伝導状態が壊れることを利用して光子を検出する。半導体検出器に比べ、極めて低雑音で、かつ光子の到来時間を正確に捉えることが可能。

*5 量子波長分割多重伝送技術

量子暗号鍵配送では、一本の光ファイバー中で光子の伝送を邪魔することなく、送り手と受け手で正確にタイミングを合わせる必要がある。そこで、タイミングを合わせるための光信号と鍵の載った光子信号を、波長を変えて多重化し、伝送し、受け手側で散乱光などの雑音を除去する技術。

補足資料2

＜ 実験の概要 ＞

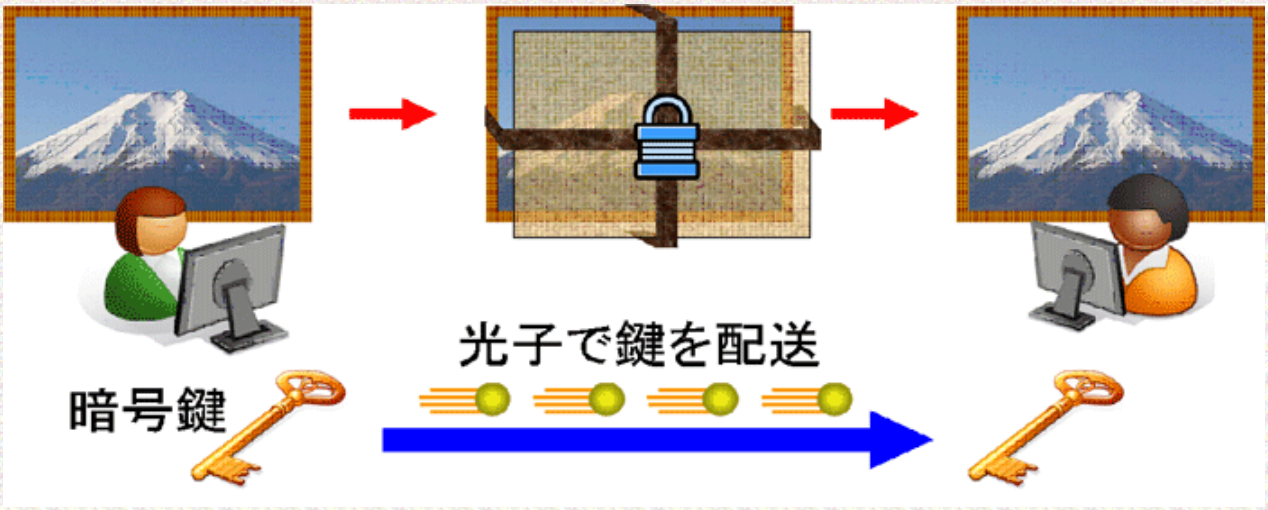

図1：量子暗号鍵配送のイメージ

量子暗号鍵配送のイメージを図1に示し、今回のフィールド実験の概要を図2に示します。NICTが有する敷設光ファイバー施設（JGN2）のけいはんなオープンラボ内に量子暗号の送受信装置を設置し、奈良のNTT大安寺局舎との間の複数本の光ファイバーを用いて、光子を3往復させ、97kmの伝送を行っています。送り手側では、繰り返し周波数625 MHzで微弱光を変調し、800ピコ秒（1ピコ秒は1兆分の1秒）はなれたパルスの対に光子が1個だけ存在するように調整しています。

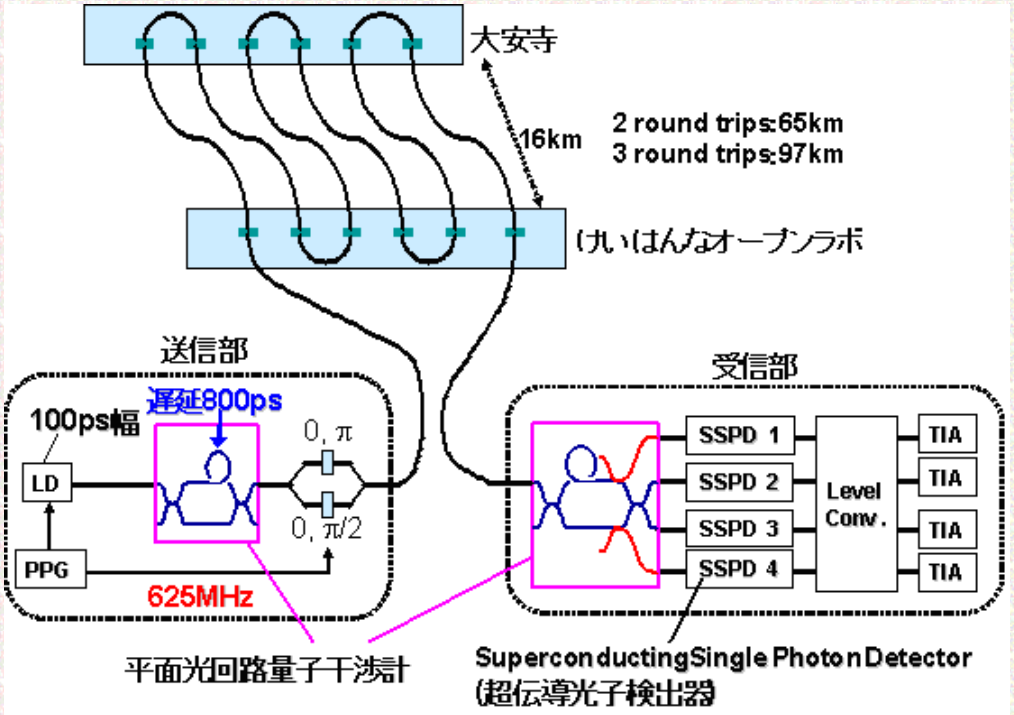

図2　超伝導単一光子検出器と平面光回路量子干渉計を組み込んだ量子暗号鍵配送システム

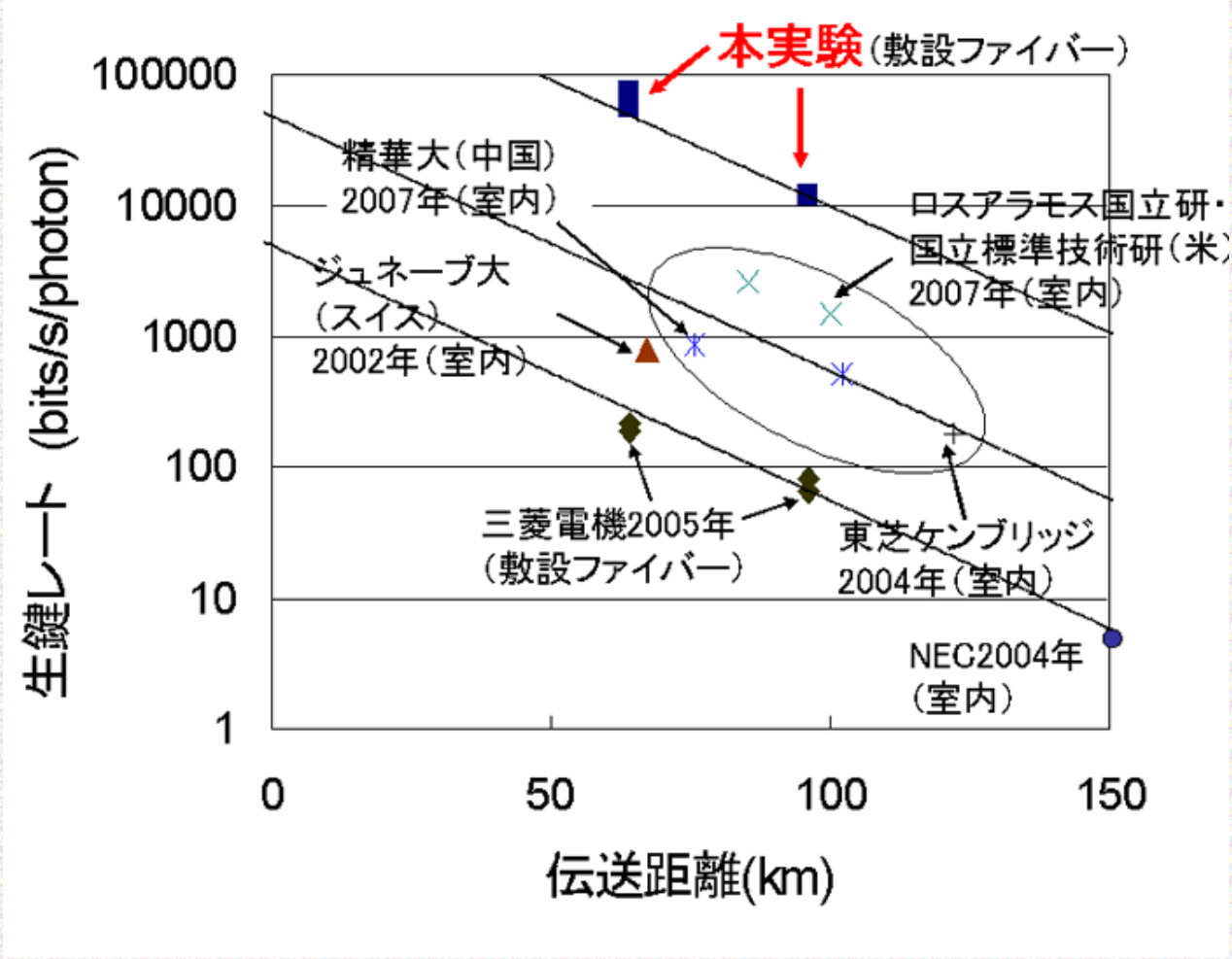

図3　伝送距離60km以上の実験における光子当たりの生鍵生成速度の比較

図3では、これまで伝送距離60km以上で行われた量子暗号鍵配送実験の主なものを比較しています。縦軸は秘密鍵を生成する前の種になる「生鍵」の生成速度を表します（実験条件や処理方式の違いによる比較補正を公正に扱うため、あえて生鍵で比較してあります）。従来のフィールド100km圏では100倍の改善、室内実験まで入れても10倍の改善を達成しています。

補足資料3

＜ 成果に関連した学会発表 ＞

会議名：The Optical Fiber Communication Conference and Exposition (OFC)
光ファイバー通信国際会議
San Diego, California, USA, 2008年2月24-28日

著者：Akihiro Tanaka1, Mikio Fujiwara2, Sae Woo Nam3, Yoshihiro Nambu1, Seigo Takahashi1, Wakako Maeda1, Ken-ichiro Yoshino1, Shigehito Miki2, Burm Baek3, Wang Zhen2, Akio Tajima1, Masahide Sasaki2, and Akihisa Tomita2
1 NEC Corporation
2 National Institute of Information and Communications Technology
3 National Institute of Standard and Technologies

講演タイトル：″Ultra fast quantum key distribution over a 97-km installed telecom fibre with wavelength division multiplexing clock synchronization″
セッション名・講演番号：OWJ – QKD and 100 Gbps Pres., no. OWJ2
Wednesday, February 27, 2008.