

2007年5月31日

(報道発表資料)

日本電信電話株式会社  
国立情報学研究所  
National Institute of Standards and Technology  
情報通信研究機構

## 世界最長、量子暗号鍵を200kmの光ファイバー上で配送することに成功 ～世界最速10GHzクロック周波数の超高速量子暗号システムで実現～

日本電信電話株式会社(以下 NTT、東京都千代田区、代表取締役社長:和田紀夫)、国立情報学研究所<sup>\*1</sup>(以下 NII、東京都千代田区、所長:坂内正夫)スタンフォード分室(室長:NII/スタンフォード大学教授 山本喜久)および、National Institute of Standards and Technology(以下 NIST、米国コロラド州)は共同で、世界最速10GHz(ギガは10億)クロック周波数<sup>\*2</sup>の量子暗号システムを開発し、単一光子レベルの光を用いた量子暗号鍵をこれまでで世界最長となる200kmの光ファイバー上で配送することに成功しました。

この成果は、NTT物性科学基礎研究所<sup>\*3</sup>(以下 NTTの研究所)とNIIスタンフォード分室が開発した差動位相シフト量子鍵配送システムと、NISTが開発した超伝導単一光子検出器を組み合わせることで実現したものです。NTTの研究所は、この研究を情報通信研究機構(以下 NICT、理事長代行:田中栄一)の委託研究「量子暗号の実用化のための研究開発(研究代表者:NTT都倉康弘)」の一環として実施しました。本成果は、盗聴が絶対に不可能な究極的に安全・安心な長距離通信ネットワークを実現するための重要な基本技術として期待されています。

今回の成果は、英国科学誌『Nature Photonics』(電子版、現地6月1日付)に掲載されます。

### 【開発の背景】

近年のインターネットの発展に伴い、ネット上での商取引や個人情報など、秘密のデータ送受信時でのセキュリティに対するニーズが高まっています。

現在一般に使われている公開鍵方式の暗号システムは、仮に第三者が情報を盗聴しても、現在のパソコンの能力では、暗号の解読に膨大な時間がかかるため、実質的に安全なものとして用いられていますが、将来、コンピュータの能力が飛躍的に向上すると、解読される可能性があります。

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。

量子暗号システム<sup>\*4</sup>は、情報を光の量子力学的な状態(量子状態)に乗せて運ぶため、「情報を読むと量子状態が壊れてしまう」という量子力学の法則によってその安全性が守られています。

具体的には、暗号鍵の情報を光の最小単位である光子の量子状態に乗せて伝送するため、途中で第三者が盗聴(観測)すると量子状態が壊れ、盗聴者は元の状態を再生することができず、盗聴の痕跡も残ります。

そのため受信側において盗聴を検知することができ、絶対安全な暗号通信システムとして期待されており、その安全性は、公開鍵暗号と異なり、将来どれだけ技術が進歩しても「量子力学」が正しい限り不変です。

これまでの量子鍵配送実験では、伝送距離は 100 km 程度、そのときの鍵生成率は最大 166bps にとどまっており、伝送距離と鍵生成率の向上が実用化に向けた課題となっています。

## 【実験のポイント】

### (1) 世界最速となる 10GHz クロック周波数の量子暗号システムの構築(図1)

今回の 10GHz クロック周波数量子暗号実験は、高速化に適した差動位相シフト量子鍵配送(Differential phase shift quantum key distribution: DPS-QKD)プロトコル<sup>※5</sup>を用いて、以下のように行いました。

送信側(アリス)は、波長 1.5  $\mu$ m のレーザと高速強度変調器を用いてクロック周波数 10GHz の短パルス列を発生させ、各パルスの位相を位相変調器によって 0 または  $\pi$  でランダムに変調したのち、減衰器を通してパルスあたりの平均光子数を 1 よりも十分小さい状態にして送信します。

光ファイバーを通ったパルス列は、受信側(ボブ)において、パルス間隔(100ps)と等しい遅延時間を持った干渉計に送られ、2 つの出力ポートに接続された超伝導単一光子検出器<sup>※6</sup>(Superconducting single photon detector: SSPD)(図2)のいずれかによって検出されます。

暗号鍵はその結果に基づいて生成されます。

### (2) 世界最長 200 km の光ファイバー(伝送損失 42 dB)での量子鍵配送(図3)

超高感度かつ高時間分解能特性を有する超伝導単一光子検出器を用いることで、世界最長となる 200km 長の光ファイバー(伝送損失 42 dB に相当)を通して、12bps の生成率で安全な暗号鍵を配送することに成功しました。

この記録は、光ファイバーを用いた単一光子レベルの量子暗号鍵配送実験としては、従来の記録(107km)を大きく上回るものです(約 2 倍)。

### (3) 100 km の光ファイバー伝送における鍵生成率の飛躍的な向上

伝送距離 105 km において、17kbps の安全鍵生成率を実現しました。

これは、100km における光ファイバー上の安全鍵生成率の世界記録(166bps)を 100 倍以上、上回るものです。

量子暗号システムでは、暗号の安全性を確保するためには、暗号化においてデータのビット数と同数の鍵ビット数を用いる必要があります。今回の鍵生成率の飛躍的な向上により、大量のデータを長距離ネットワークでも安全・安心に送ることを可能とするものです。

#### 【今後の展開】

今回の結果を、長距離での実用的な量子暗号システムを構築するための大きな一歩として、今後は長距離量子暗号を100km超の光ファイバーネットワーク上で実現することを目指し、研究開発を進めます。

また、さらに200kmを超える長距離の量子暗号を実現するため、量子状態の中継技術の基礎研究も行っていきます。

<本研究の一部は、科学技術振興機構戦略的創造研究推進事業(CREST)「通信波長帯量子もつれ光子とその応用システム(研究代表者:大阪大学教授 井上恭)」および戦略的創造研究推進事業発展研究(SORST)「光を用いた量子情報システムの研究(研究代表者:スタンフォード大学教授 山本喜久)」、NIST Quantum Information Initiative および DTO の援助を受けて行われました。>

(ネイチャーフォトリクス誌からの要請により、報道解禁日時は日本時間6月2日午前2時とさせていただきます。)

- ・図 1:10GHz クロック周波数の量子暗号システム
- ・図 2:超伝導単一光子検出器(SSPD)
- ・図 3:伝送損失／光ファイバー長と安全鍵生成率

< 本件に関する問い合わせ先 >  
N T T 先 端 技 術 総 合 研 究 所  
（ 物 性 科 学 基 礎 研 究 所 ）  
企 画 部 広 報 担 当  
岸 根 、 飯 塚  
T E L : 0 4 6 - 2 4 0 - 5 1 5 2  
<http://www.ntt.co.jp/sclab/contact>

国 立 情 報 学 研 究 所  
企 画 推 進 本 部 広 報 普 及 チ ー ム  
小 野 、 早 川  
T E L : 0 3 - 4 2 1 2 - 2 1 3 5  
E - M a i l : k o u h o u @ n i i . a c . j p

情 報 通 信 研 究 機 構  
連 携 研 究 部 門 委 託 研 究 グ ル ー プ  
天 野 、 千 葉  
T E L : 0 4 2 - 3 2 7 - 6 0 1 1

総 合 企 画 部 広 報 室  
栗 原  
T E L : 0 4 2 - 3 2 7 - 6 9 2 3

## 【用語解説】

### ※1 国立情報学研究所 <http://www.nii.ac.jp/>

情報学という新しい研究分野での「未来価値創成」を目指すわが国唯一の学術総合研究所として、ネットワーク、ソフトウェア、コンテンツなどの情報関連分野の新しい理論・方法論から応用展開までの研究開発を総合的に推進しています。

### ※2 クロック周波数

送信側と受信側での時間同期のテンポを表す指標であり、1秒間に何個の時間スロットが同期されているかを示す。

### ※3 NTT 物性科学基礎研究所 <http://www.brl.ntt.co.jp/>

ネットワーク、情報処理技術における処理能力、セキュリティの壁を越える新原理・新概念の創出をミッションとし、イノベーションにつながる基礎技術の開拓による中長期的な事業貢献を目指すとともに、科学技術への貢献も視野に入れ、研究開発を行っています。

### ※4 量子暗号システム

量子鍵配送によって暗号鍵を生成したのち、その鍵を用いて暗号化したデータを別の古典チャネルによって送ります

### ※5 差動位相シフト量子鍵配送プロトコル:

NTT 研究所とスタンフォード大学が開発した量子暗号プロトコル。従来の光パルスを折り返す Plug&Play 方式に比べ、一方向の伝送が可能であり、セットアップがシンプルかつ鍵生成効率が高いなどの特長がある。

### ※6 超伝導単一光子検出器(SSPD):

光ファイバーに結合された窒化ニオブ超伝導体の細線(図 2(a)、(b))に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、光子を低雑音、高時間分解能(60ps)(図 2(c))で検出することが可能。

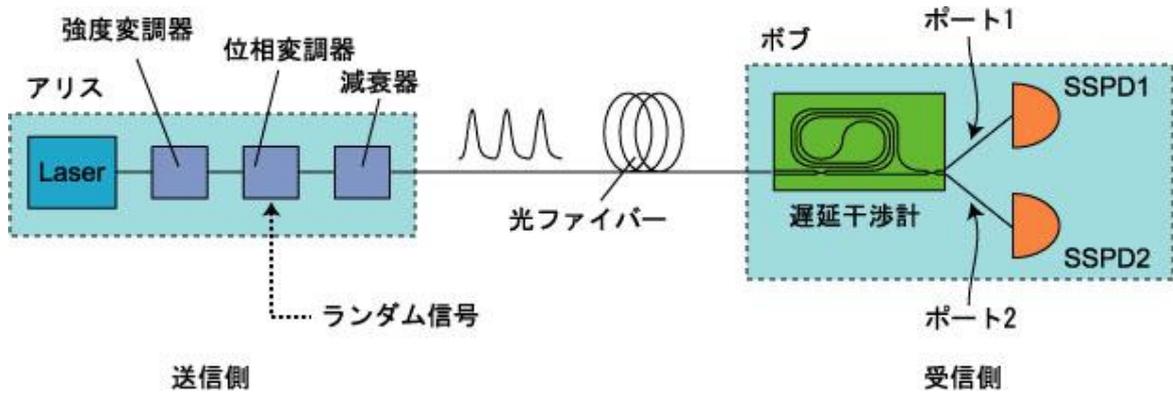


図 1: 10GHz クロック周波数の量子暗号システム。

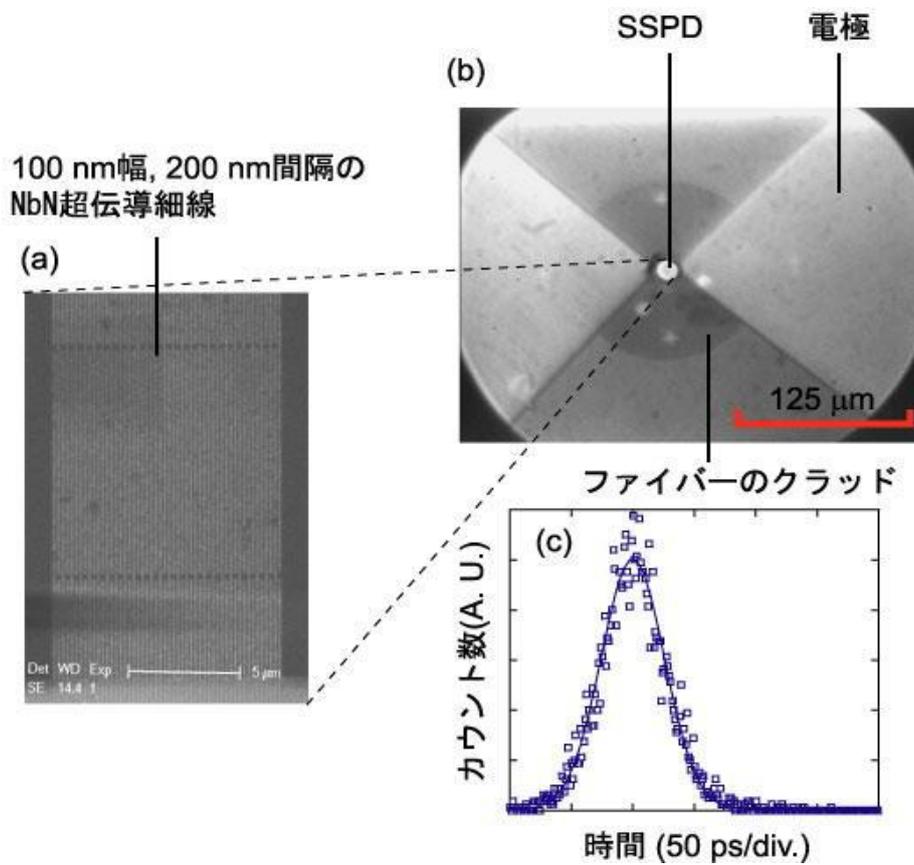


図 2: 超伝導単一光子検出器 (SSPD) 画像提供: NIST

- (a) 走査電子顕微鏡による SSPD の拡大図
- (b) 光学顕微鏡による SSPD と光ファイバーの結合
- (c) SSPD の時間分解特性

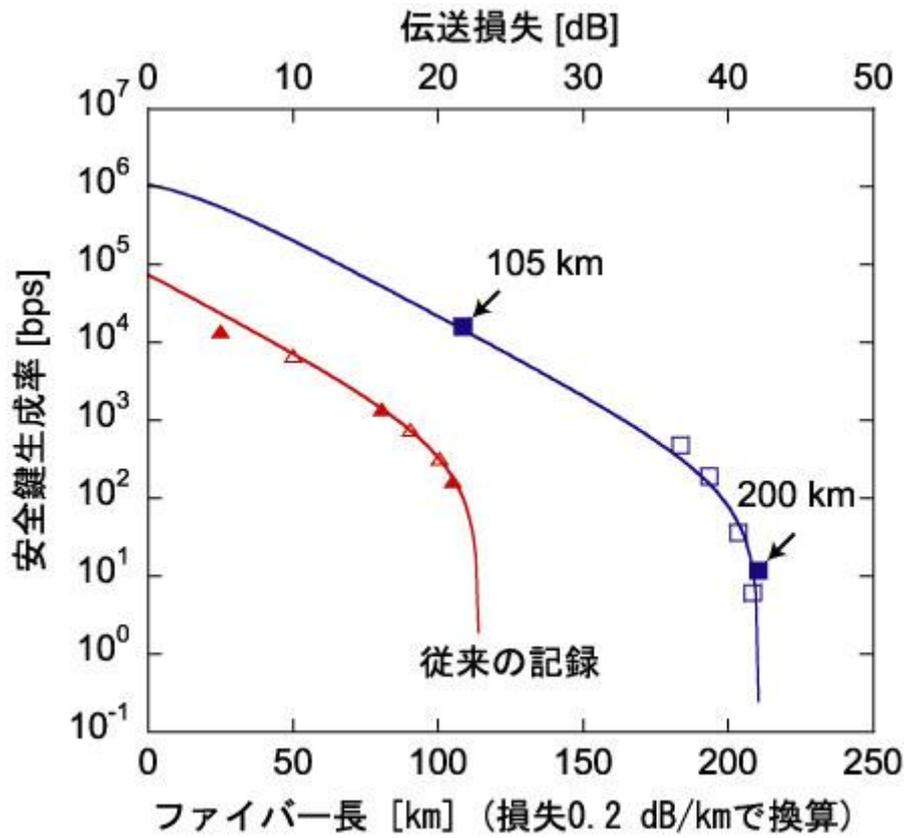


図 3: 伝送損失／光ファイバー長と安全鍵生成率

■, □: 今回の結果

▲, △: 100 km における安全鍵生成率の従来記録

(塗りつぶしはファイバー伝送実験結果、

白抜きは光減衰器での模擬伝送実験結果)