[PRESS RELEASE](技術)　　2004-0139

2004 年 7 月 15 日

東京大学生産技術研究所ナノエレクトロニクス連携研究センター
株式会社富士通研究所

世界初、通信波長帯において単一光子発生に成功：量子暗号通信の実用化に向けて大きく前進

東京大学先端科学技術研究センター・生産技術研究所ナノエレクトロニクス連携研究センター（注 1）荒川泰彦教授グループと株式会社富士通研究所（注 2）は、単一光子（注 3）の発生・計測システムを開発し、世界で初めて、通信波長帯における単一光子の発生に成功しました。今回開発した技術により、究極の暗号通信手段と言われながら、従来、毎秒数 100 ビット（以下、bps）でしかデータ転送できなかった量子暗号通信（注 4）の速度を一挙に 400 倍以上高速化できる可能性が拓け、その成果は、量子暗号通信の実用化に向けた大きな前進と言えます。

本研究開発の一部は、文部科学省 IT プログラムとして実施されています。

本技術の成果の第一報は、7 月 15 日発行の JJAP(Japanese Journal of Applied Physics) Express Letter に掲載されます。さらに、本技術の内容の詳細は、7 月 26 日から米国アリゾナ州で開催される半導体物理国際会議（International Conference on the Physics of Semiconductors；ICPS-27)で発表します。

なお、本技術の研究開発の一部は、文部科学省の研究開発委託事業である「 IT プログラム～世界最先端 IT 国家実現重点研究開発プロジェクト～」の中の１課題である「光・電子デバイス技術の開発プロジェクト」によるものです。また、独立行政法人 物質・材料研究機構 ナノマテリアル研究所（注 5）の協力も得ています。

【開発の背景】

インターネット上での電子商取引の普及に伴い、より安全性の高い通信に対する需要が高まっています。その中でも量子暗号通信は、盗聴の可能性をゼロにできる極めて安全性の高い究極の暗号通信として、世界で研究開発が活発に進められています。

【課題】

量子暗号通信の実現には、1パルスに含まれる光子を1個に制限できる単一光子発生器が必要となります。しかし、実用的な光ファイバー通信に用いられる波長帯（1.3-1.55マイクロメートル）では単一光子発生技術が存在せず、従来の量子暗号通信の実験では、単一光子の代わりに通常のレーザー光源を用いざるを得ませんでした。

しかし、量子暗号通信にレーザー光源を用いる方法では、1パルスに2個以上の光子が入る可能性があり、盗聴の可能性をゼロにはできません。2個以上の光子が発生する確率を低くするためには光の強度を極めて弱くする必要があり、このために、レーザー光源を利用した量子暗号では、長距離での通信速度が数100bpsと、著しく遅い速度でしか実現できないという大きな問題がありました。

【開発した技術】

今回開発したのは、1.3から1.55マイクロメートルの実用的な通信波長帯で、単一光子を発生・計測する技術です。開発した技術の特長は、以下の通りです。

（１） 通信波長帯での単一光子発生技術（図1）

光学シミュレーションを用い、量子ドットと呼ばれるナノメートルサイズの構造から効率よく光子を発生できる半導体素子を設計しました。また、極めて小さな構造である量子ドットにダメージを与えない半導体プロセス技術を新たに開発しました。これにより、従来実現されていなかった通信波長帯での単一光子の発生が可能になりました。なお、使用した量子ドットは、独立行政法人 物質・材料研究機構 ナノマテリアル研究所の佐久間主幹研究員のグループと富士通研究所が共同で作製したものを用いています。

（２） 通信波長帯での単一光子計測技術（図2）

開発した半導体素子から出る光を効率よく集光し、量子ドットから放出された光だけを通信用光ファイバーに送る単一光子送信システムを設計・開発しました。また、光ファイバーを通過した光を2手に分け、2手に分けた光の受信のタイミングを正確に測定できる単一光子受信システムを設計・開発しました。2手に分けた光が同時計測されないことを確認することで、発生した光が単一光子であることを証明することが可能です。

【実験結果と効果】

今回開発したシステムを用いて実験を行ったところ、2手に分けた光が同時計測されることは、ノイズによる誤差の範囲でゼロであることが確認でき、通信波長帯で量子ドットから単一光子が発生していることを検証できました（図3）。

なお、今回、単一光子を検証した光の波長は1.3マイクロメートルですが、すでに、より一般的な通信波長である1.55マイクロメートルでの量子ドットからの発光も観測できています。

通信波長帯で単一光子の送信が確認できたことにより、送信側の発光強度を弱めなくても量子暗号通信が可能となります。この特長により、100キロメートル程度の伝送距離において、従来のレーザー光源を利用した量子暗号通信に比べ約400倍となる100kbpsの通信が可能となり、高度な情報セキュリティが必要とされる官公庁、金融、医療等の現場において、量子暗号通信技術が実用化される可能性が飛躍的に高まりました。

【今後】

今後、波長1.55マイクロメートルでの単一光子の伝送検証、単一光子の取り出し効率の向上などを図り、2007年頃の単一光子発生器実用化を目指した研究開発を推進していきます。また、量子ネットワーク実現に向け、量子中継技術や量子計算技術開発も進めていきます。

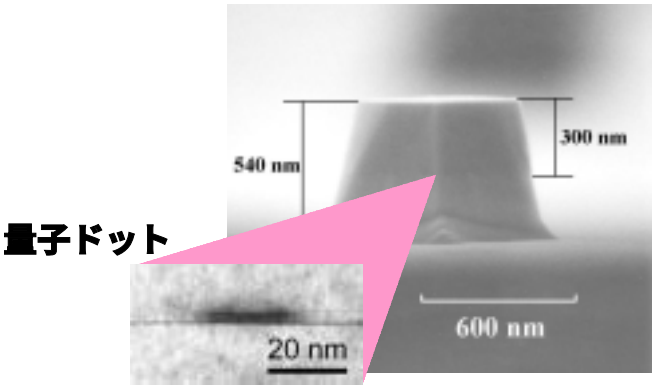

図1 単一光子を発生させた半導体素子

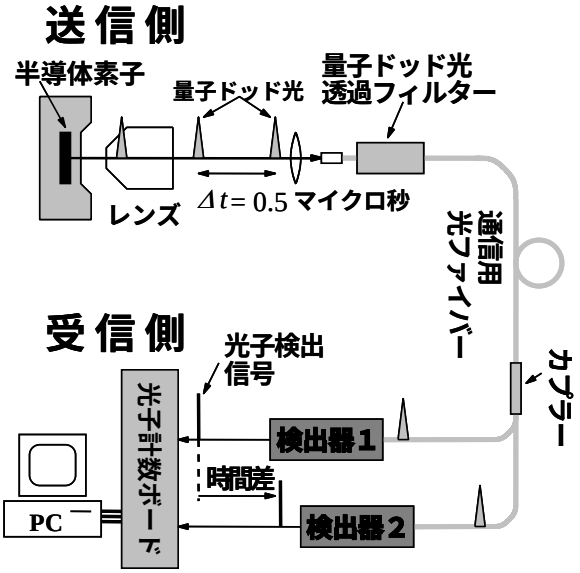

図2 単一光子計測システムの概要

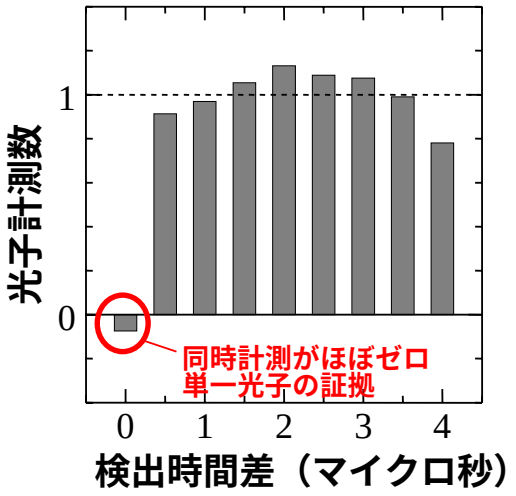

図3 単一光子計測の実験結果

【技術に関する問い合わせ先】
東京大学先端科学技術研究センター・生産技術研究所
ナノエレクトロニクス連携研究センター
教授 荒川 泰彦
電話：03-5452-6245（直通）

株式会社富士通研究所
ナノテクノロジー研究センター
電話：046-250-8234（直通）
e-mail：nano-qc@labs.fujitsu.com

以 上

（注1） ナノエレクトロニクス連携研究センター：センター長 荒川泰彦、所在地 東京都目黒区。
（注2） 株式会社富士通研究所：社長 村野和雄、本社 川崎市中原区。
（注3） 単一光子：光は粒子性を持っており、単一光子は光の粒子1個を意味する。これ以上分割して光子の持つ情報をコピーすることができない。
（注4） 量子暗号通信：量子力学を利用して、解読に必要な秘密鍵を通信者間で安全に共有できる通信技術。実用化に最も近い方式がBB84と呼ばれる方式で、単一光子に鍵情報をのせて伝送する。
（注5） 独立行政法人 物質・材料研究機構 ナノマテリアル研究所：所長 青野正和、所在地 茨城県つくば市。

【報道関係お問い合わせ先】
富士通株式会社
広報IR室　岡田、佐藤（英）
電話：03-6252-2174（直通）
e-mail：pr@fujitsu.com

補足資料

公開鍵暗号(RSA 等)をはじめとするインターネットで広く普及している暗号は、「解読に必要な計算時間が非常に長いので解読は困難である」という計算機の能力を前提とした“条件付き安全性”で保証されています。一般には、10～40 年先まで破られることは無いと予測された上で、暗号の強度が定められています。

しかしながら、いつ効率的な計算手法が開発されるかもしれませんし、数十年経っても解読されたくない情報の伝達はそもそも明確な安全性が保証されていないことになります。

量子暗号通信は情報伝達の安全性を長期にわたり守ることができる新しい通信技術で、官公庁、金融、医療等の高度なセキュリティが必要とされる現場での利用が期待されます。実現するには様々な技術課題を解決しなければなりませんが、特に重要なのは単一光子発生器です。

レーザーを用いた量子暗号は、長距離での通信速度の低下が顕著で、one time pad で必要な長い秘密鍵を送ることが難しくなります。単一光子を用いれば速度の劣化が抑えられ大幅な速度向上が期待されます。(下図参照)

我々は、単一光子発生器の実現を目指して量子ドットデバイスの研究開発を行っています。今回は1.3マイクロメートル帯での単一光子観測（用語説明参照）に世界で初めて成功しました。 今後は更に伝送効率のよい1.55マイクロメートル帯での単一光子伝送実験や実用化に向けた改良を進めます。（今回使用した量子ドットは既に1.55マイクロメートル帯での発光も確認されています。）

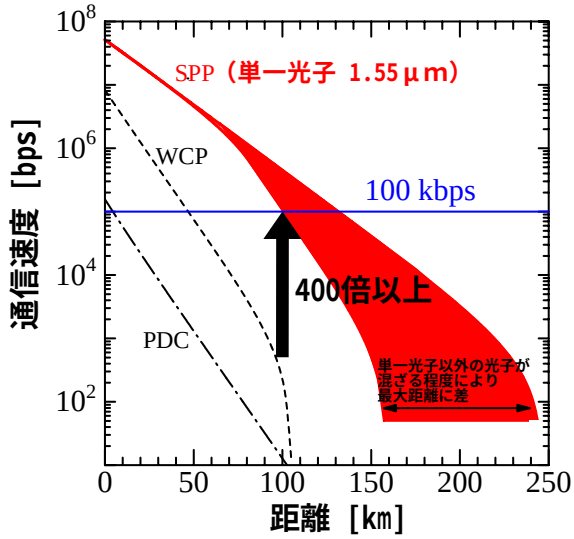

図 単一光子を用いた場合(赤)とレーザーを用いた場合(WCP, PDC 方式、詳しくは用語説明参照)の 1.55 マイクロメートル帯での通信速度比較。 単一光子を用いれば、100km 地点で 400 倍以上の速度向上が可能となる。

用語説明

量子暗号通信

量子力学を利用して、秘密鍵を送信者と受信者の間で安全に共有することができる通信技術。一個の光子に鍵情報をのせて伝送する。「光子は、それを分割して情報をコピーすることができない」という量子力学原理から、盗聴者が光子を盗もうとすると、受信者には光子の消失あるいは情報の変化として伝わるため、盗聴が検知できる。量子鍵配布(QKD: Quantum Key Distribution)とも呼ばれ、1984 年に C.Bennett と G.Brassard が開発した BB84 プロトコルをはじめ幾つかの方式がある。実用化に最も近い方式が BB84 で、一個の光子に鍵情報をのせて伝送する。なお、慣用的に、送信者を Alice、受信者を Bob、盗聴者を Eve と擬人化して説明する場合がある。

One time pad (OTP)

唯一、絶対安全が保証された暗号。手順は送信者がデータを同じ長さの完全にランダムな秘密鍵で暗号化し、受信者は同じ秘密鍵で解読する。一度使用した秘密鍵は再利用しない。但し、秘密鍵を安全に送る方法が無かった為、広く普及していない。量子暗号通信によって、安全な鍵配布が可能になり注目されている。バーナム暗号とも呼ばれている。

マイクロメートル、ナノメートル

長さの単位。　1 ミリメートルの千分の１が 1 マイクロメートル。１マイクロメートルの千分の１が１ナノメートル。従って 1 ナノメートルは１ミリメートルの百万分の 1。

量子ドット

半導体中の電子や正孔（ホール）をナノメートルの大きさの狭い場所に閉じ込めることが出来る構造。今回我々が使用した量子ドットは、高さが 2 から 3 ナノメートル、直径 20 から 50 ナノメートル程度のサイズである。電子や正孔（ホール）を狭い場所に閉じ込めることで、様々な量子効果が現れる。この量子効果を利用して、単一光子発生器の他、半導体レーザーや光増幅器等に利用が検討されている。今回我々が使用した量子ドットでは、1.3～1.55 マイクロメートルの広い波長領域で鋭い輝線スペクトルを持つ発光を確認している。

通信波長帯

光通信に適した光の波長帯をいう。光ファイバの光透過率の高い（つまり伝送距離が長い）波長帯波長に相当する。1.26 マイクロメートルから 1.63 マイクロメートルで、5 つのバンド、O バンド（1.26～1.36 マイクロメートル）、E バンド（1.36～1.46 マイクロメートル）、S バンド（1.46～1.53 マイクロメートル）、C バンド（1.53～1.565 マイクロメートル）、L バンド（1.565～1.625 マイクロメートル）に分かれる。そのなかでも特に、波形歪の小さい O バンド（1.3 マイクロメートル帯とも呼ばれる）と高い光透過率を持つ C バンド（1.55 マイクロメートル帯）が良く使われている。

単一光子測定

光のパルスが一つだけの光子を含むかどうか検証する測定法。単に光のスペクトルを調べる場合に比べ、単一光子を検証する実験なので検出器や光学系に格段の性能が求められる。特に通信波長帯では今まで成功した事例は無い。 我々は、量子ドットデバイスや光学系の改良を進めた上で、最も発光強度が強い量子ドット（0 バンド、すなわち 1.3 マイクロメートル帯）を選び、世界ではじめての検証実験を行った。今後は、更に長い距離を伝送可能な C バンド（1.55 マイクロメートル帯）で実験を進める予定である。

単一光子発生器

光子が一つだけ含まれる光パルスを発生させるデバイス。現在のところ、通信波長帯に対応できるのは、材料選択や大きさの制御が出来る量子ドットのみ。量子ドットのような小さな構造では量子効果が強く働き、閉じ込められている電子や正孔の数によって発光波長が変化するため、電子と光子一対だけからの発光だけをフィルターで選別することが可能となる。

SPP: Single Photon Pulses の略。

単一光子発生器によって生成した光パルス。パルス中には 2 個以上の光子が殆んど含まれていない為、減衰させたレーザー光を用いる方法に比べ、量子暗号通信の速度を速めることができる。

WCP: Weak Coherent Pulses の略。

レーザー光を減衰器で弱めた光パルス。これまでは通信波長帯での単一光子発生器が存在しなかったため、量子暗号通信で主流の光パルス生成法として用いられてきた。レーザー光を減衰器で弱め、１パルス当り平均光子数を約 0.1 個以下にした光パルスを用いるため、通信速度は極めて遅く、数 100bps 程度。

PDC: Parametric Down-Conversion の略。

非線形光学素子にレーザー光を照射し、光子対を生成すし、量子暗号通信を行う技術。WCP と同様、2 個以上の光子対を含むパルスが発生する為、光子対の数を少なくする必要があり、通信速度は遅くなる。