傍受不能な光量子暗号通信を可能にする単一光子技術

Single Photon Technology for Secure Optical Quantum Communications

アンドリュー　シールズ　Andrew Shields
マーク　スチーブンソン　Mark Stevenson

この論文では，単一光子信号を通信手段として用いることにより，ネットワークの安全性問題をハードウェアによって抜本的に解決する量子暗号通信について述べる。この手法を用いれば，信号の送受信者は暗号鍵（かぎ）を第三者に傍受されることなくネットワーク上で共有することができる。この傍受不能な量子暗号通信システムの実現には，単一光子の発生・検出のための新素子の開発が必要不可欠である。

当社は，ナノテクノロジーを駆使して，単一光子通信に向けた新しい半導体光電変換素子の開発を目指している。今回は，電界効果トランジスタ内部に量子ドット層を設けることにより単一光子検出を実現するとともに，1個の量子ドットを単一光子源として使用できることも紹介する。

This paper describes a hardware-based solution to network security issues which relies on communication using single photon signals. It allows, for instance, two parties on the network to form a shared cryptographic key, with a guarantee that the key cannot be known by anyone else. Crucial to the implementation and performance of such a secure optical communication system is the development of novel devices for the detection and generation of single photons. Using nanotechnology we have fashioned a new class of semiconductor optoelectronic device for this application. By integrating a layer of quantum dots inside a field-effect transistor we have realized a detector of single photons. We also show that the emission from a single quantum dot can be used as a source of single photons.

1 はじめに

光が分割不可能な粒子（光子）から構成されるという概念は，20世紀初頭に黒体放射の発光スペクトル分布を説明するためにプランクによって導入され，その後アインシュタインによる光電効果の説明を通じて，量子物理誕生へとつながった。100 Wの電球が放つ光子の数は1秒間におよそ10^{18}個もあることから，光子1個というのは極めて弱い光である。この弱い光を捕らえる試みは光子計数技術として発展し，現在では医用撮像，分析化学，レーザ計測，レーザイメージング，工業用検査やプロセス制御といった，様々な応用分野で使用されている。しかし，光子を後述する量子通信の信号に用いようとした場合，光子の発生・検出を1個ずつ“厳密に”制御する必要があり，その意味での単一光子技術はいまだ確立されていない。

一方，半導体ナノテクノロジーの進歩は，量子ドットと呼ばれる電子1個を厳密に制御することが可能な，ナノメートルサイズの半導体の箱の作製を可能にした。ここでは，更にこの量子ドットを用いれば，単一光子の厳密な制御も可能となることを示す。ナノテクノロジーを駆使して厳密な単一光子の操作を実現できれば，上述の微弱光を取り扱う技術の精度向上に役だつばかりでなく，量子情報処理という新たな応用分野を切り開くことができる。その市場は，次の10年間に急速に拡大することが予想され，なかでももっとも早く普及すると考えられるのが，量子暗号と呼ばれるオープンな光ネットワーク上での安全な通信方式である。これは，機密保持や認証といった，従来ソフトウェアに依存してきた暗号化プロセスを，ハードウェアによって原理的安全性を実現する技術である。

2 量子情報通信

量子暗号通信とは，2人のユーザーが機密性の保証された共有暗号鍵を，ネット上で自由に形成することを可能にする技術である。この技術の基本は，単一光子1個を送信1ビットに対応させ，そのビット列をコード化することにある。絶対的安全性の根拠は，単一光子がそれ以上分割不可能な光の最小単位であるということに由来する。すなわち，単一光子信号上のビットを決定する測定チャンスはたった1回しかなく，また，量子暗号通信における鍵ビットはあらかじめ決められた受取人が，光子を実際に受け取ったときにだけ0か1を形成することになるため，例えば64ビットのビット列に関して100％正しい答えを確定することは事実上不可能である。すなわち，盗聴者が単一光子信号を盗もうとしても鍵に関する情報をいっさい得ることはできない。

また，量子暗号は，盗聴者が暗号の一部あるいは全部をいったん測定し，次に暗号を盗んだことを隠すために，盗んだ暗号をコピーして受信者に再送する，といういわゆる

“検知・再送”型の攻撃に対しても安全性を保証する。そのような盗聴の手法もまた，単一光子のような量子状態の性質をすべてコピーすることが不可能であるという“非クローニング原理”が存在するため実行不可能となる。この原理によれば，盗聴者が単一光子信号を読み取ろうとすると，必然的に盗聴した証拠を残すことになり，送信者と受信者が盗聴を容易に検知することができる。

これまでにいくつかの研究グループが，数十kmの光ファイバや数kmの自由空間での鍵配布の実行可能性を実証してきた。もっとも進んだシステムでも，光検出にアバランシェフォトダイオードを用いているため暗雑音が大きく，この雑音が通信距離やビットレートを律速する。そのため，現在では，より低雑音の単一光子検出器の開発へ関心が高まってきている。一方，原理的安全性にもう一つ必要不可欠な要素は，真の単一光子発生器である。従来の半導体パルスレーザを減光する方法では，複数の光子が同時に発生されている可能性があるため，論理的に盗聴を100％排除できなくなってしまう。

当社は，単一光子の効率の良い発生・検出技術を実現するため，現実的な作製方法として，量子ナノ構造を従来の半導体素子に集積する方法を採用した。半導体の活性領域をナノサイズまで小さくした量子ドットにおいて支配的となる単一キャリア物性の制御が動作の鍵となる。

3 量子ドットの特長とその作製方法

ナノスケールの量子ドットを形成するために簡便で効率的な方法の一つは，若干異なる格子定数（例えばガリウムヒ素（GaAs）の上のインジウムヒ素（InAs））を持つ基板上での半導体の自己組織化モードを利用することである。InAsは，最初GaAs上にぬれ層（wetting layer）と呼ばれる非常に薄い二次元面として成長する。しかし，InAsはわずか数原子層の臨界膜厚を超えると，格子ひずみを最小化にするためにwetting layerから小さなドット状に自己組織化してしまう。

図1は，原子間力顕微鏡によって観察した成長表面上でのドット状成長の像である。これらのドットの上に更にGaAs層を成長させることによって，GaAs格子中にInAsの量子ドットを成形することができる。InAs/GaAs系における量子ドットの典型的な大きさは，高さ数nm，直径数十nmと小さく，室温で0次元の量子力学的性質を持つのに十分な大きさである。

量子ドットは，周りを取り囲む物質よりも伝導帯端が低い位置にあるため，電子を捕獲する性質を持つ。一方，量子ドットのエネルギー準位は量子化しているため，捕獲される電子の個数は有限である。その個数はドットの大きさだけでなく，電子が負電荷を帯びているため，捕獲された電子どうしが反発し合うエネルギーにも依存する。より小さな量子ドットに捕獲されて強く閉じ込められた電子は，ドットの中だけでなく，ドット周囲近傍の電子とも大きな相互作用を及ぼし合うことになる。

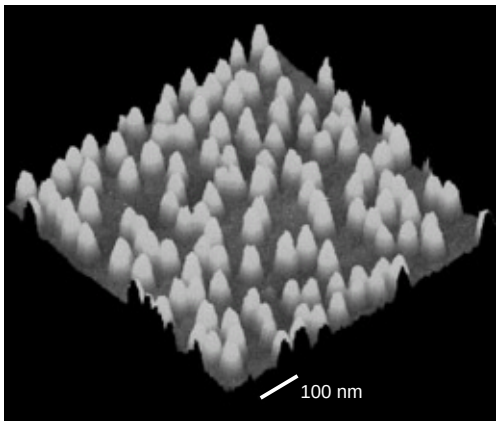

図1．自己組織化量子ドット層　原子間力顕微鏡により観察した成長表面上でのドット状成長の像を示す。
Atomic force microscope (AFM) image of layer of self-assembled quantum dots

4 量子ドット トランジスタによる単一光子の検出

当社は最近，電界効果トランジスタ（FET）の中に前述した自己組織化成長モードを利用して量子ドット層を集積することにより，単一光子検出素子の作成に成功した[(1)]。基本的な素子構造は，**図2**に示すように量子ドット層の近傍に伝導チャネル層を設けたFET構造である。量子ドット層とチャネル層の間隔をわずか数nmに設計すると，単一電子によって単一量子ドットを荷電しただけで，FETのチャネル層の抵抗は敏感に変化する。この特長により，半導体中で光子が吸収されると電子・正孔対が生成され，どちらか一方のキャ

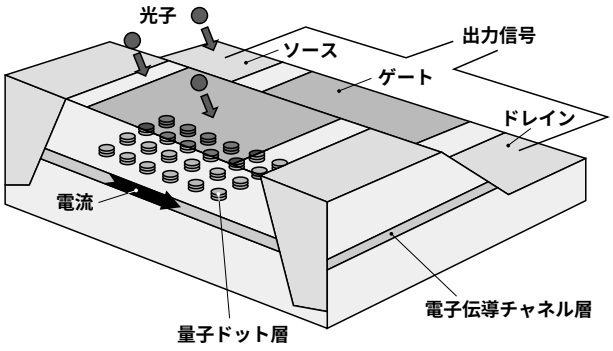

図2．量子ドット単一光子検出器の模式図　この素子は，薄い$Al_{0.33}Ga_{0.67}As$障壁層によって導電性のGaAsチャネルから分離されたInAs量子ドット層を持つ，$GaAs/Al_{0.33}Ga_{0.67}As$変調ドープFETである。
Schematic of quantum dot single photon detector

リアが量子ドットに捕獲されると観測可能なチャネル抵抗の変化を引き起こすため，単一光子の検出が可能となる。図2の素子構造の場合，GaAsチャネルの伝導帯端よりエネルギーの低い位置に量子ドットのエネルギーレベルがあるので，初期状態では各ドットは過剰な電子を捕獲することになる。この負電荷が引き起こすクーロン反発力により，個々の量子ドットに隣接したチャネル層内の電子を空乏化し，その結果，チャネル層の電子移動度は著しく低下する。

ゲート電圧を調整してチャネル層が若干の導電率を持つ状態にもっていくと，チャネル層の電流はドットに捕獲された単一電荷にもっとも敏感になることを発見した。この状態では，単一光子入射によって励起された単一キャリアは，ドットに捕獲され，その結果チャネルの導電率をステップ状に変化させることになる。

この素子による単一光子の検出結果の例を**図3**に示す。曲線は，2 μAの電流を流した発光ダイオード（LED）による非常に弱い発光（波長：650 nm）を照射した条件下でのチャネル伝導度の時間変化を表す。一連の鋭いステップ状の伝導度の上昇が見られるが，各々のステップが単一光子によってゲート領域下の量子ドットから1個の負電荷が消去されたことに対応する。また，その微分値は1光子に対応するパルス状信号が得られる。図から1光子の信号レベルに比べ雑音レベルは十分に低いことがわかる。

このデータは，4 Kの液体ヘリウム温度で観測したものであるが，同様の挙動が77 Kの液体窒素温度でも得られており，室温でも原理的に達成可能であると考えている。この素子構造における単一光子検出効率は約1%と見積もられ，光電子増倍管と同程度の値ではあるが，光子計数用アバランシェフォトダイオードの効率にはまだ及んでいない。この理由は，入射光の75 %が表面の金属ゲート電極によって反射されてしまうこと，ゲートを透過した光の一部しか薄い量子井戸層に吸収されないためであると考えられる。したがって，透過ゲート電極を採用し，光のほとんどが活性領域に吸収されるよう層構造を再設計することにより，量子効率をアバランシェフォトダイオードと同等以上にすることは将来十分可能であると考えている。

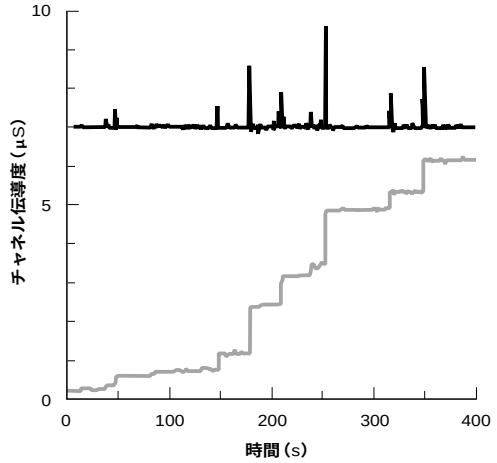

図3．プロトタイプ単一光子検出器の実験データ　1光子の検出は量子ドットトランジスタのソース―ドレイン間伝導度のステップ状の増加に対応する。微分値（上）はパルス状になるが，これは1光子の検知に対応する。
Experimental data recorded with prototype single photon detector

5 量子ドットを利用した単一光子の発生

報告されている量子暗号通信のデモンストレーションでは，すべてパルスレーザダイオードの出力を大幅に減光することにより近似的な単一光子源として利用してきた。この方法は，量子暗号の潜在能力の証明には有益ではあったが，原理的安全性は真の単一光子源によってだけ保証される点を忘れてはならない。レーザ光を減光しただけの通常の方法では，多光子パルスの発生が避けられず，盗聴者が光子の一部を鍵の情報を得るために利用できてしまうからである。

更に，パルスレーザ光源の減光率は，90 %以上のクロックサイクルを無出力にするほど強いもので，その間情報を何も伝達していないことになる。これは明らかに非効率的であり，結果的には鍵配布に要する時間が増大し情報伝達距離を縮めてしまうことになる。

これに対し当社では，より純粋な単一光子源として，量子ドットを組み込んだ素子を利用できることを実証した[(2)]。この素子は，InAs量子ドット1個だけを含む直径0.8 μmの微小なGaAsメサ柱（台地状構造）から構成される。パルスレーザ光照明によってGaAsのバルク部分で生成された電子・正孔対が量子ドットによって捕捉（ほそく）されると，そこで再結合することにより光子が放射される。量子ドットはサイズが非常に小さいため，1個ないしごく限られた数の電子・正孔対しか捕獲することができず，したがって1個ないしごく少数の光子だけを放射することが可能となる。実験の結果，光子1個の放出と複数個の光子放出では，異なる波長で放射されることがわかった。したがって，分光器を使って放射光をフィルタリングすることによって，入射レーザパルス当たり1個の放射光子を保証することができるようになった。

成功した素子動作のようすを**図4**に示す。ここで，入射パルスレーザの波長750 nm，周期76 MHz，測定温度は5 Kである。ここでは，二つの放射光子の時間間隔を繰り返し測定することによって得られた，光子対間の時間相関がプロットしてある。相関信号の時間間隔 $\tau = 0$ におけるピークが抑制されているのがわかるが，これは2個以上の光子が同時に放射されることが極めてまれであることを表す。

2個以上の光子の同時放射を抑制することは真に安全な量子通信システムにとって不可欠であることから，これらの

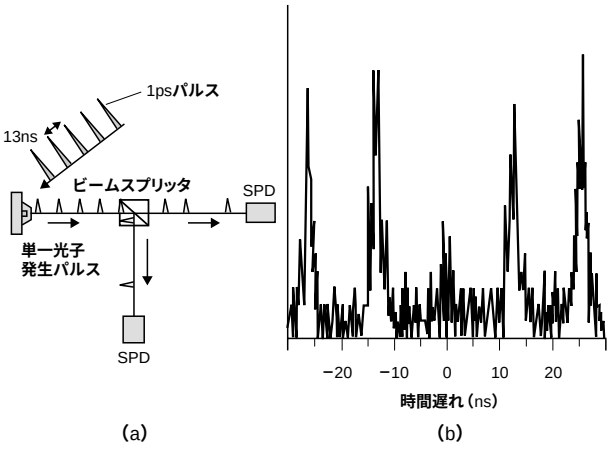

図4．量子ドット素子による単一光子の発生実験　(a)量子ドットから放射された1対の光子間の時間遅れを測定するための二つの単一光子検出器(SPD)を使用した実験装置の配置図を示す。(b)単一光子の発生を証明する量子ドット素子の実験データ。ヒストグラムは量子ドットから放射された対光子間の異なる時間遅れの周波数依存性を表す。時間遅れ0での対光子の強い抑制はドットが2光子を同時に放出しないことを示す。

Single photon emission experiment with quantum dot device

結果は，従来のレーザを用いる方法に比べ量子ドットを用いて単一光子を発生させる方法のほうが優れており，したがってより安全で，潜在的により高速かつより長距離の通信に適していることがわかる。

今後，室温動作と実際の光ファイバ通信で用いられる波長帯域での単一光子生成を実現することにより，この素子の実用化を目指す。

6 あとがき

量子ドットは単一光子の発生・検出を実現するのに極めて有望なナノ構造である。アバランシェ雑音を回避することより，量子暗号の長距離かつ高ビットレートの伝送が可能となる。また，量子ドットによる単一光子源が実現すれば，従来のレーザ光源を用いた場合に必然的に発生してしまう多光子パルスを用いたシステムの欠陥を取り除くことができる。

量子暗号通信は量子情報処理技術の中で最初に実現する応用として期待されているが，応用分野はそれだけにとどまらない。現在開発している単一光子素子は，将来量子テレポーテーションや量子計算のような，より複雑で高度なプロトコルを実現するための基本素子として利用できる可能性がある。量子情報処理分野は，次々と出てくる新しい応用アイディア提案とともに，非常に急速に発展している分野である。この研究により開発されるであろう単一光子素子が現実的になる時代には，これらの夢のようなアイデアも次々と実現されていくであろう。

謝　辞

英国ケンブリッジ大学キャベンディッシュ研究所のR. Thompson, M. O'Sullivan, I.Farrer, D. A. Ritchie各氏の有益な議論に感謝の意を表します。

文　献

(1) A.J.Shields, et al.Detection of single photons using a field effect transistor gated by a layer pf quantum dots. Appl. phys. Lett.76, 3676 (2000).
(2) R.M.Thompson, et al. Single Photon Emission from Exciton Complexes in Individual Quantum Dots. Phys. Rev. B64, 201302(R)(2001).

アンドリュー　シールズ　Andrew Shields, Ph.D.
東芝欧州研究所 ケンブリッジ研究所主任研究員，理博。
量子情報通信の研究・開発に従事。
Toshiba Research Europe Ltd., Cambridge Research Lab.

マーク　スチーブンソン　Mark Stevenson, Ph.D.
東芝欧州研究所 ケンブリッジ研究所，理博。
量子情報通信の研究・開発に従事。
Toshiba Research Europe Ltd., Cambridge Research Lab.

和　訳

加藤　理一
東芝欧州研究所 ケンブリッジ研究所副所長。

江草　　俊
研究開発センター 研究企画担当参事。