OUKA
Osaka University Knowledge Archive

Title	Efficient quantum key distribution with practical single-photon sources
Author(s)	足立, 頼俊
Citation	大阪大学, 2010, 博士論文
Version Type	
URL	https://hdl.handle.net/11094/54254
rights	
Note	著者からインターネット公開の許諾が得られていないため、論文の要旨のみを公開しています。全文のご利用をご希望の場合は、大阪大学の博士論文についてをご参照ください。

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

【73】

氏名	足立頼俊（あだちよりとし）
博士の専攻分野の名称	博士（理学）
学位記番号	第　23894　号
学位授与年月日	平成22年3月23日
学位授与の要件	学位規則第4条第1項該当 基礎工学研究科物質創成専攻
学位論文名	Efficient quantum key distribution with practical single-photon sources （現実的な単一光子源を利用した高効率量子鍵配送）
論文審査委員	（主査） 教授　井元　信之 （副査） 教授　北川　勝浩　　教授　竹内　繁樹

論文内容の要旨

量子鍵配送とは、送信者アリスと受信者ボブとの間で、物理法則に従う範囲であらゆることのできる盗聴者イヴが居たとしても、安全鍵を生成できる手段の1つであり、最も有名なプロトコルにBB84がある[1]。BB84プロトコルの実現には様々な課題があるが、その1つに現実的な単一光子源から発生する多光子の存在がある。この多光子部分において、イヴは「光子分岐盗聴」と呼ばれる攻撃を用いると、エラー無しで完全な情報を得られることから[2]、実際の光源では、短距離通信や低生成率しか達成できなかった。近年の研究から「デコイ状態」を用いれば光子分岐盗聴を検知できることが示されているが[3]、その一方で、特定の光源における光強度の能動的な変調や、実験装置を複雑にすることでしかデコイ状態の用意の仕方が解明されていなかった[5]。

本論文では、一般的な単一光子源を利用した場合において受動的にデコイ状態を用意できる方法を2つ示し、その結果、効率的に量子鍵配送を行えることを示す。

1つ目は、パラメトリック下方変換を利用した光源を用いた方法である。この光源は理想的な単一光子源と同程度の距離まで安全鍵を生成できるが、従来の方法では光子分岐盗聴の可能性を最大限に考慮しなければならず、その結果として安全鍵生成率は理想的な場合と比べ極端に低くなってしまう[4]。一方、提案する方法では従来と全く同じ装置を用いるが、古典的なデータを上手く処理することでデコイ法を利用することができ、安全鍵生成率を飛躍的に上昇させることができる。

2つ目は、より一般的な単一光子源に適用できる方法である。これは、アリス側にビームスプリッターを挿入し、その反射された方に光子検出器を置いて信号の一部分を見張ることで、デコイ法を利用できるというものである。この方法では、高光子数分布の把握が重要である一方、多光子発生率を極端に低くする必要が無いため、現在世界中で開発が進められている様々な単一光子源に適用できる可能性がある。また、より正確に分布を見積もることで通信距離を伸ばすことができ、数個程度の光子数までを調べれば、理想的な光源とほぼ同じ距離を達成できる。

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp.175–197.

[2] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[3] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[4] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[5] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305(R).

論文審査の結果の要旨

提出された論文は、理想的な単一光子源でなく現実的な疑似単一光子源を用いた量子暗号の新しい方法を二つ提案し、それが理想的な単一光子源を用いる量子暗号と遜色ない性能（伝送距離の関数としての安全鍵生成効率で評価される）を有することを理論的に示したものである。そればかりでなく、疑似単一光子源として従来考えられていた厳しい要求条件は必要でなく、代わりに光子数分布を精密に知りさえすればよいことを明らかにしたもので、今後の単一光子源開発研究に大きく資するものである。

量子暗号とは、暗号化および復号化に用いる鍵と呼ばれる乱数を第三者に見られることなく離れた二地点に生成するものである。光源が完全な単一光子源であり、伝送路が無損失無雑音であり、光子検出器が量子効率1かつダークカウント0であるなどの理想的な場合は容易に実現できるが、現実には完全なものは何一つない。この中で完全な単一光子源になるべく近い疑似単一光子源の開発が従来の大きな研究テーマの一つであった。たとえばパラメトリック下方変換により双子の光子を発生し、片方が検出されたタイミングにもう一方のパルスに光子が出ていることがわかるので、それを利用する疑似単一光子源や、半導体量子ドットのエキシトン発光による疑似単一光子源が研究されている。しかしこれらの疑似単一光子源は一つの光パルスに光子が一つも無かったり二つ以上の光子が発生したりするため、送受信者に気付かれずに盗聴者がその情報を読み取ることが可能であり、これが「安全鍵」の生成効率を大きく下げていた。

本研究では上記の問題を克服する二つの量子暗号方式を提案している。まず上記パラメトリック下方変換により双子の光子を発生し、片方が検出された場合のみならず検出されなかった場合のもう一方のパルスの光子数確率分布がわかることも利用する。検出された場合とされなかった場合に異なる光子数分布となるが、実は二種類（多種類でもよくその方が望ましい）の光子数分布を利用すると「おとり暗号」と呼ばれる方法が使えることが知られている。これは盗聴の検知効率を上げるためのおとり捜査のようなものであるが、これにより量子暗号の効率が格段に上がり、たとえば伝送距離200kmほどでは通常の方法より1万倍も改善され、その結果「完全な単一光子源」を用いる量子暗号にほぼ匹敵する性能となる。本研究のもう一つの提案は、パラメトリック下方変換に拘泥せず量子ドットであろうが何であろうが適用できる方法であるが、任意の光子源で光子数分布さえ測っておけば「おとり暗号」としてやはり「完全な単一光子源を用いる方法」に匹敵するための条件を出したものである。それによると光子数にして0から7程度までの分布を測っておけば良いことが明らかとなった。

以上の成果は、既にPhyscal Review LettersおよびNew Journal of Physicsに論文掲載されている。候補者は物理的直観と数学的厳密性の両方を要求される本研究をよく展開させた。実験的実現性についても理解しており、理論家の陥りやすい非現実的理論展開が避けられている。発表はわかりやすくよく構成されており、質問への受け答えはスムーズであった。研究テーマの発掘・研究推進・発表・議論等の能力は博士号の授与を受けるものとして十分であると考えられる。

以上から、本論文は博士（理学）の学位論文として価値のあるものと認める。