

量子鍵配送に向けた自己相関関数による光子数分布評価

Evaluation of photon number distribution using autocorrelation function for

Quantum Key Distribution

北大院情報科学¹, 北大院情報科学研究²

○(M1) 松本 遼司¹, 富田 章久², 岡本 淳²

IST-Hokkaido Univ.¹, Fac. of IST-Hokkaido Univ.²

○Ryoji Matsumoto¹, Akihisa Tomita², Atsushi Okamoto²

E-mail: matsumoto.ryoji.w6@elms.hokudai.ac.jp

はじめに

量子鍵配送 (Quantum Key Distribution, QKD) を実装する際、現状ではレーザ光の平均光子数を 1 以下に減衰させた WCP 光源が用いられている。ところが、WCP 光源を用いる場合は 2 光子以上を含むパルスの発生を利用した光子数分離攻撃 [1] の存在が安全性に影響を及ぼす。光子数分離攻撃の対策が可能であるデコイ法 [2, 3, 4] を用いるためには光源の光子数分布に関する知識が必要であり、従来ではポワソン分布に従うと仮定されてきた。ところが、パルスレーザのように発振時にキャリア密度や光強度が急激に変化する際にはポワソン分布に従うかは自明ではない。このように QKD の安全性保証のためには光子数分布を実験的に検証する手法の確立が求められている。そこで本稿では、光子数分布の間接的な評価が可能な自己相関関数の測定をパルスレーザを対象に行い、ポワソン分布に従うことに矛盾しないことを示した。

自己相関関数を用いた光子数分布評価

同時刻における 2 次の自己相関関数 $g^{(2)}(0)$ は光子数分布 $P(m)$ と以下の関係がある。

$$g^{(2)}(0) = \frac{1}{\mu^2} \sum_{m=0}^{\infty} m(m-1)P(m) \quad (1)$$

ここで μ は 1 パルスあたり平均光子数、 m は 1 パルスに含まれる光子数である。光子数分布の仮定のもとで計算できる $g^{(2)}(0)$ と測定値を比較

することで $P(m)$ の評価を行う。いま、光子数分布がポワソン分布 $P(m) = e^{-\mu}\mu^m/m!$ に従うと仮定すると $g^{(2)}(0) = 1$ が μ によらず成り立つ。そこで実験では μ を 1.0、0.5 および 0.2 の 3 種類として測定した。実験としては光源から出た光をハーフビームスプリッタで分岐させ、各分岐先での一光子の計数率と同時計数率を調べることで $g^{(2)}(0)$ の測定値を得る。今回はポワソン分布に従うことが既知である CW レーザで予備実験を行い、 $g^{(2)}(0) = 1$ となることを確認した実験系を用いた。

測定結果を Fig.1 に示す。結論として、いずれの平均光子数においてもポワソン分布に従うことに矛盾しないことを示した。

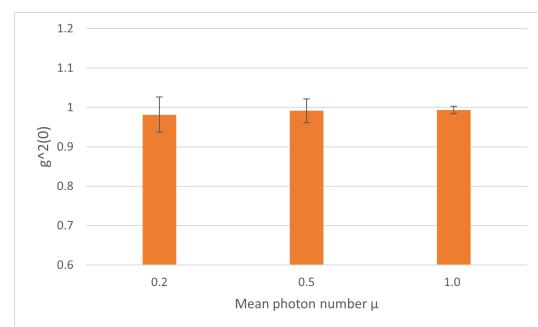


Fig.1 Results of $g^{(2)}(0)$ measurements

参考文献

- [1] G.Brassard et al., Phys.Rev.Lett. 85, 1330(2000).
- [2] W.Y.Hwang., Phys.Rev.Lett. 91, 057901(2003).
- [3] X.B.Wang., Phys.Rev.Lett. 94, 230503(2005).
- [4] H.K.Lo et al., Phys.Rev.Lett. 94, 230504(2005).