18p-C2-4

過剰雑音及びビットエラー分布を考慮した光プリアンプを用いない IM/DD QKD

IM/DD Quantum Key Distribution Considering Excess Noise and Bit Error Distribution

阪大工　○生田 拓也，井上 恭

Osaka Univ. ○Takuya Ikuta, Kyo Inoue

E-mail: ikuta@procyon.comm.eng.osaka-u.ac.jp

【はじめに】量子雑音を利用して安全な秘密鍵を配送する、連続変数量子鍵配送 (QKD) の研究が進められている。我々は以前にその一方式として、2 値 IM/DD 方式による QKD の検討を行った [1]。このプロトコルは、通常の光通信と同じ簡便な装置を用いて QKD が可能という特徴を有する。以前の検討では、量子雑音と光プリアンプの ASE が考慮されていたが、本論文では光アンプを用いずに、量子雑音、レーザの過剰雑音、受信器の熱雑音を考慮した、より簡便で現実的な IM/DD QKD の性能評価を行った。性能評価に際しては、受信者のビットエラーレートを確率変数として、その確率分布を考慮した。

【構成とプロトコル】図 1 に本プロトコルの構成を示す。送信者 Alice は、ランダムに微小二値強度変調された信号光を受信者 Bob に送信し、Bob はそれを直接検波する。すると Bob の受信信号は、平均値 $\{i_0, i_1\}$、分散 $\{\sigma_0^2, \sigma_1^2\}$ の、互いの一部が重なったような分布に従う (図 2)。これに対して Bob は、2 つの閾値 $\{d_0, d_1\}$ を設け、d_0 を下回ったら bit 0、d_1 を上回ったら bit 1 を生成する。閾値を適切に設ければ、Bob は低い誤り率で bit を生成することができる。その後、Bob が bit 生成時刻を Alice に伝えることで、Alice・Bob はほぼ同じ bit 列を共有することができ、これをシフト鍵とする。盗聴者は、信号分布が重なりを持つために完全に識別することが出来ず、また、雑音の多くを占める量子雑音の無相関性により、閾値を超える信号の予測が不可能である。このことにより、鍵の安全性が保証される。

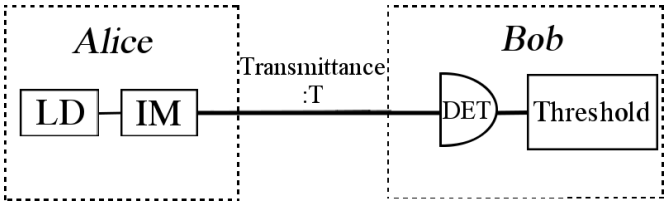

図 1: IM/DD QKD の構成

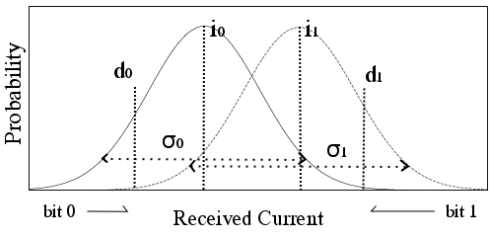

図 2: 受信信号分布

【受信者のビットエラー分布】QKD への代表的な盗聴法として、Intercept Resend Attack(IR 攻撃) が挙げられる。IR 攻撃について議論する際には、Bob のビットエラーレートが重要な要因となるが、これは通常、一定値として取り扱われる。しかし、有限ビット長の場合、二項分布に従う確率変数となる。本論文では、その分布を考慮したより現実的なシステム性能評価を行った。

【システム性能】上記の IR 攻撃並びに Beam Splitting Attack に対する本プロトコルのシステム性能を計算した。図 3 に結果を示す。100km 以上の鍵配送が可能であることが示されている。

[1] 岡徹, 井上恭 第 60 回応用物理学会春季学術講演会 30p-D1-1

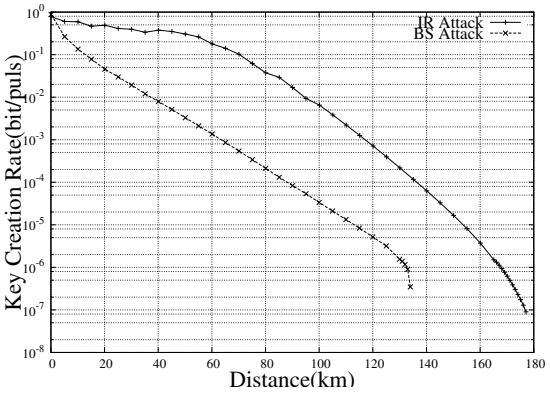

図 3: 鍵生成率の数値計算結果