30p-D1-1

２値強度変調/直接検波方式による量子鍵配送

Quantum Key Distribution Based on Binary IM/DD Transmission

阪大工　岡　徹*，○井上　恭

Osaka Univ.　Akira Oka*, ○Kyo Inoue

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

[はじめに] 我々は以前に、量子雑音を利用した巨視的差動位相シフト量子鍵配送（QKD）の検討を行った[1]。この方式は通常の光通信の装置構成で QKD が可能という特徴を有する。本論文では、同様のアイデアを強度変調/直接検波に適用した QKD 方式[2]について検討した。

[構成及びプロトコル] 図１に本方式の構成を示す。送信者アリスはレベル差が微小である２値強度変調信号光｛I_0, I_1｝を送信する。受信者ボブはこれを光前置増幅器を通して直接検波する。検出信号の確率密度分布は、信号光の量子雑音及び増幅器雑音のため I_0 と I_1 とで一部重なり合う（図２）。これに対しボブは、I_1 の分布の高レベル側にしきい値 d_1 を、I_0 の分布の低レベル側に d_0 を設定し、d_1 以上の信号をビット「1」／d_0 以下の信号をビット「0」とするとともに、ビットを生成した信号をアリスに知らせる。アリスは、当該信号が I_1（I_0）なら「1」（「0」）としてビットを作る。するとアリス/ボブはほぼ同じビット列を共有することになり、これをシフト鍵とする。盗聴者は量子雑音のため２状態を完全に識別することはできず、また、どの信号がしきい値を超えるか予測不可である。このことより鍵の安全性が確保される。

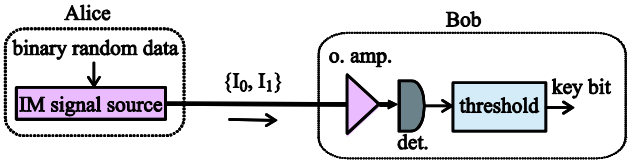

図 1. システム構成

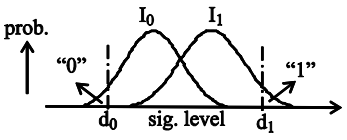

図 2. 受信信号分布

[システム性能] いくつかの盗聴法を想定して、本方式のシステム性能をシミュレートした。図 3 にﾋﾞｰﾑｽﾌﾟﾘｯﾄ攻撃とｲﾝﾀｰｾﾌﾟﾄ･ﾘｾﾝﾄﾞ攻撃を組み合わせた盗聴[1]に対する性能を示す。ここでは、誤り訂正はボブからアリスへの一方向とし、また、２値のレベル差は鍵生成率が最大となるように最適化した。数十 km 程度の鍵配送が可能であることが示されている。

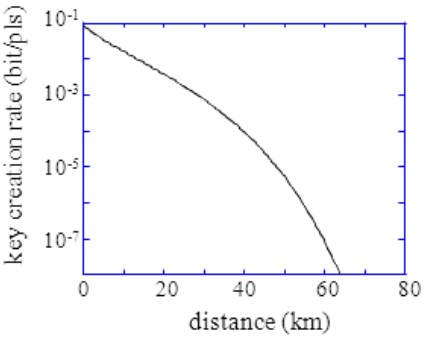

図 3　鍵生成率のシミュレーション

[1] T. Kukita, H. Takada, K. Inoue, Jpn. J. Appl. Phys. **49** (2010) 122801.

[2] H. Yuen, A. M. Kim, Phys. Lett. A **214** (1998) 135-138.

* 現所属 株式会社フジクラ Fujikura Ltd.

© 2013 年　応用物理学会