強度変調/直接検波秘密鍵配送方式のシフト鍵生成実験

Experimental demonstration of sift-key creation in intensity-modulation/direct-detection secret key distribution system

阪大工　山森　直毅，○井上　恭

Osaka Univ.　Naoki Yamamori, ○Kyo Inoue

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

[はじめに] 単一光子または超微弱光を用いる量子鍵配送の研究が進められているが、光子検出器または超微弱光のホモダイン検波を要することが実装上の課題となっている。これに対し我々は、通常の強度変調/直接検波系の装置構成を用いて秘密鍵を生成する方式を検討している[1, 2]。今回、実際にシステムを実装してシフト鍵生成実験を行ったので報告する。

[構成] 図１に実験構成を示す。送信者は LD 光の強度を疑似ランダム 10Gbps 信号で微小に２値変調して送信する。受信者はそれを PIN 受信器で直接検波し、増幅後、デジタルオシロスコープに入力する。そして、デジオシに記録されたデータから１ビット区間の中心時刻における受信レベルを抽出する。図２に抽出された受信レベルのヒストグラムを示す。図において、赤点/青点はそれぞれ送信ビット１/0 に対応した受信レベル分布を表している。

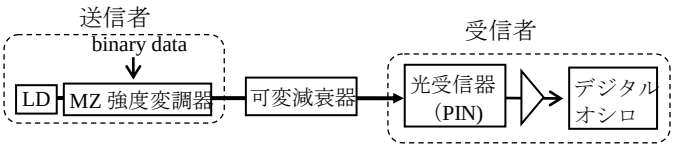

図１．実験構成

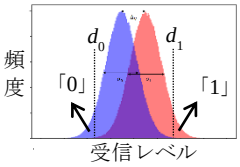

図２．受信レベルのヒストグラム

[鍵ビット生成] 送信光の変調度は微小であるため、２値の信号分布は LD 光の量子雑音/送信器過剰雑音/受信器雑音のため一部が重なり合っている（図２）。これに対し受信者は、図２に示すように閾値 d_0（d_1）を設定し、受信レベルが d_0(d_1)より小（大）であればビット「0」（「１」）を生成する。そしてビットを生成したスロットを送信者に通知する。送信者は受信者の情報と自身の変調データからビット列を生成する。これをシフト鍵とする。こうして生成された鍵の安全性は、伝送信号が量子雑音のため完全には識別不可であることにより担保される。

[結果] 図３に結果を示す。横軸は送受信間の損失を 0.2dB/km でファイバ長に換算した値である。各距離において、送信変調度及び受信閾値は、ﾋﾞｰﾑｽﾌﾟﾘｯﾄ攻撃及びｲﾝﾀｰｾﾌﾟﾄﾘｾﾝﾄﾞ攻撃を考慮した最終鍵生成率が最大となるように最適化している。この結果より見積もられる最終鍵生成率は、5km/20km/40km においてそれぞれ 1.6×10^{-1}/$1.8\times^{-2}$/1.6×10^{-3} であり、秘密鍵生成可能な結果が得られている。

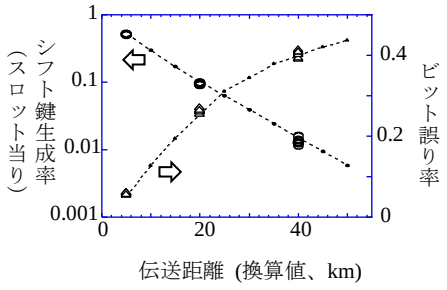

図３．　実験結果

[1] T. Ikuta, K. Inoue, New J. Phys. vol. 18 (2016) 013018.　[2] 山森、井上、応物 2017 秋、6a-PA4-1.