# 強度変調/直接検波秘密鍵配送システム性能の受信器依存性

## Dependence of IM/DD-SKD system performance on receiver

阪大工，井上研　○(M1C)寺澤 大智，井上 恭

Osaka Univ., Inoue Lab., ○(M1C)Daichi Terazawa, Kyo Inoue

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

【まえがき】　我々は強度変調/直接検波系の装置構成を用いた秘密鍵配送方式(IM/DD-SKD)の研究を進めている。そのシステム性能評価にあたり、これまでは pinPD 受信系を想定していた。一方、通常光通信システムでは、光前置増幅受信系の方が高感度である事が知られている。また本方式は、システム内雑音を利用するため、システム性能が受信器雑音特性に依存する。そこで本研究では、IM/DD-SKD に光前置増幅受信系を用いた場合の性能を評価し、pinPD 受信系と比較検討した。

【プロトコル】　IM/DD-SKD は暗号通信に用いる共通秘密鍵を安全に 2 者間に供給するシステムである。送信者は、CW レーザーから出力された光を微小に 2 値で強度変調し、低（高）レベルをビット 0(1)として送信する。受信者の受信信号レベルの確率密度分布は雑音のため、Fig1 のように 0、1 信号が一部重複する。これに対し受信者は、2 つの閾値を設定し、受信信号レベルが下（上）の閾値を下回った（上回った）場合、ビット 0(1)を生成する。それ以外は廃棄する。その後、送信者にビットを生成した時間スロットを伝える。これにより送信者と受信者はほぼ同一のビット列（シフト鍵）を共有し、これに誤り訂正と秘匿性増強を施して、最終秘密鍵を生成する。

【安全性】　IM/DD-SKD の安全性は「伝送系の雑音特性から盗聴により漏洩し得る情報量の上限を見積もり、秘匿性増強によりシフト鍵からその盗聴量分を除外する事」が可能なことにより担保される。本研究では、盗聴方法として、Beam Splitting Attack、Intercept Resend Attack の組み合わせ盗聴を想定した。

【シミュレーション結果】　Fig2 に計算結果を示す。光プリアンプ受信系、APD 受信系、pinPD 受信系の順に性能が良いという結果が得られた。

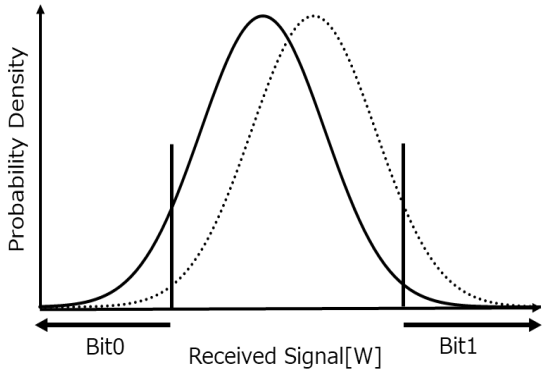


Fig. 1 Received Signal

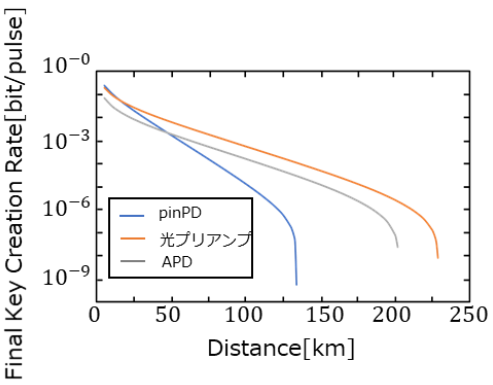


Fig. 2 Key creation rate