18p-C2-2

物理レイヤ暗号の秘密伝送可能情報量の具体的評価

Evaluation of the Secrecy Capacity of the Physical Layer Encryption

早大理工[1]，NICT[2]　○遠藤 寛之[1,2]，韓 太舜[2]，青木 隆朗[1]，佐々木 雅英[2]

Waseda Univ.[1]，　NICT[2]　°Hiroyuki Endo[1,2], Te Sun Han[2], Takao Aoki[1], Masahide Sasaki[2]

E-mail: h-endo-1212@ruri.waseda.jp

物理レイヤ暗号は，盗聴者の能力に対して合理的な物理的仮定を課した上で情報理論的安全性を保証する暗号技術であり，量子鍵配送(QKD)より長距離かつ高速な秘匿転送が可能であると期待される．特に，衛星-地上局間での見通し通信のように，盗聴者が正規受信者よりも劣悪な状況で盗聴を行うと予想される通信路においては，情報理論的安全性と伝送効率をバランス良く両立した秘匿通信を行えると期待される．

本講演では，図 1.に概要を示すワイヤタップ通信路モデル[1]において，現実に即した状況を設定し，秘密伝送可能情報量の上限である秘匿容量の具体的評価を行った結果を示す．すなわち，送信者(アリス)は通常のパルス位置変調と同様に，送信電力Pが 1W で波長λが 1550nm であるレーザを確率qで生起する強度n_A [photons/pulse]，繰り返し時間Δ_pが 10ps である光パルス信号に変調して情報を伝送する．ここで，送信電力制約$qn_A hc\lambda^{-1} \le P\Delta_p$が満足される必要がある．ただし，$h$と$c$はそれぞれプランク定数と光速度である．イブはボブの信号に対して 99.9%の強度までしか盗聴できないとする一方で，ボブとイブの検出器の暗計数をそれぞれ 10kHz，1Hz とし，その時間分解能をそれぞれ 10ps とした．これらの仮定の元で，秘匿容量C_sをアリス-ボブ間とアリス-イブ間の通信路の相互情報量$I(X;Y)$及び$I(X;Z)$から，$C_s = \max_q [I(X;Y) - I(X;Z)]$として計算を行い，ボブの通信路の透過率に対してプロットしたグラフが図 2.である．このグラフが示すように，物理レイヤ暗号はイブの通信路がボブの通信路よりも劣悪であるという条件が成立する限りにおいて，おとり付 BB84 や量子増幅転送型 BB84[2]のような長距離伝送可能な QKD プロトコルを超える秘密伝送可能情報量と伝送可能距離を獲得している．この結果は，既存の量子暗号技術ではカバーできない都市圏内や衛星-地上局間においても，物理レイヤ暗号を用いることで情報理論的に安全な光ネットワークが構築可能であることを示唆している．

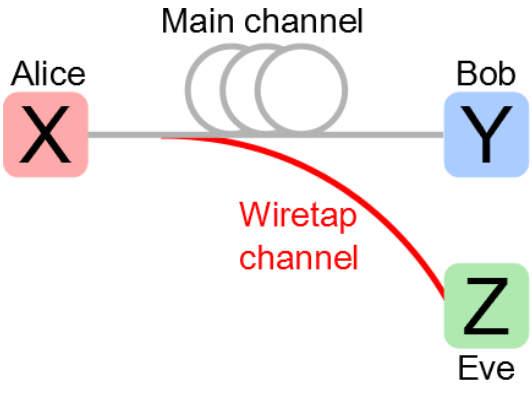

Fig.1. A schematic diagram of a wiretap channel.

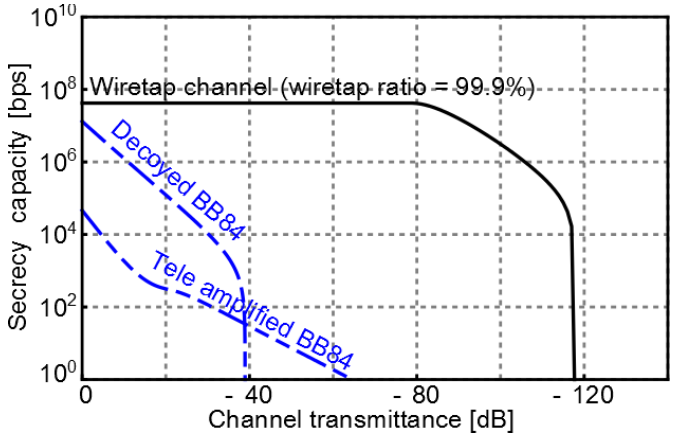

Fig.2. A numerical example of the secrecy capacity of a wiretap channel with typical key rate of QKD.

参考文献

[1] A. D. Wyner, *Bell Syst. Tech. J.*, vol.54, pp.1355-1387, 1975.

[2] J. S. Neergaard-Nielsen, et al., *Nature Photonics* 7, 439, 2013.