



参考資料（玉川大学 量子情報科学研究所）

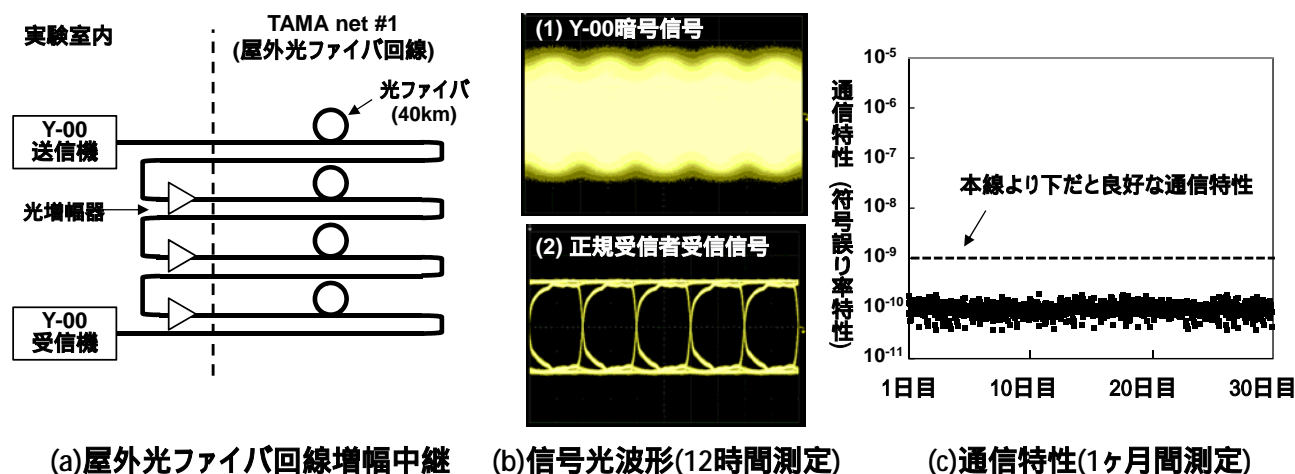
【背景】

現状のネットワークでは暗号化されていない情報も通信されており、光ファイバ回線から信号光を盗み、容易にこれらの通信情報を盗み見られることを本学のデモネットワークで実験検証が行われている。一般にデータは数値暗号によって暗号化される場合もあるが、数値暗号は危殆化の懸念があり、大量の重要なデータを伝送する光ファイバ回線で用いることは問題があると言われている。このような背景のため、DARPAは5月に回線保護の暗号技術の本格開発を提案した。これより、物理層に物理暗号を導入することは今後のネットワークでは必須の状況となった。本学では、物理暗号のひとつである Y-00 プロトコルの理論研究をすすめてきているが、Y-00 プロトコルの特長は、本文の図に示すように、盗聴者に Y-00 の暗号文を読ませない（正しく識別させない）点で、数値暗号と異なり、実装モデルにおいて数理的なアルゴリズムによる解読法がないことや、理想モデルでは原理的に解読不可能性を証明している。既に、40 ギガビット毎秒の高速暗号通信や 10 ギガビット毎秒で伝送距離 360 キロメートルなど、Y-00 プロトコルの通信システム性能評価実験に成功し、光ファイバ通信システムとの高い整合性を検証している。また、理論研究で示した強い安全性の根拠であるランダム暗号性の検証にも成功している。実用的な物理暗号は Y-00 プロトコルが唯一の有力候補で、実用化に大きな期待が寄せられている。

実用化を視野に入れると、実験室内の通信特性評価のみならず、より実環境に近い屋外にある光ファイバ回線を用いた通信特性評価が求められる。今回、本学内に敷設光ファイバ回線で通信特性評価を行い、良好な特性を検証した。

【実験検証内容】

Y-00 暗号プロトコル通信装置の通信特性を、本学内に敷設してある屋外光ファイバ回線において、1ヶ月間にわたり評価した。2.5 ギガビット毎秒の Y-00 暗号信号を、全長 160 km (1 スパン = 40 km, 計 4 スパン) の屋外光ファイバ増幅中継伝送路 図(a)を伝送させた。伝送後、Y-00 プロトコル受信機を用いて伝送特性を評価した。図(b)に示すように、12 時間連続して観測した暗号波形 (Y-00 プロトコル) および正規受信者が受信する波形は、良好な特性だった。1ヶ月間にわたり、通信特性(符号誤り率特性)を評価した結果を図(c)に示すが、昼夜、天候を問わず、通信に十分な伝送特性(符号誤り率が 10^{-9} 未満)だった。なお、伝送距離 160 km は今回準備した実験装置(光増幅器)の数で制限されており、伝送限界ではない。



こちらの図のデータ送付をご希望の場合は【取材に関するお問い合わせ先】までご連絡ください。