



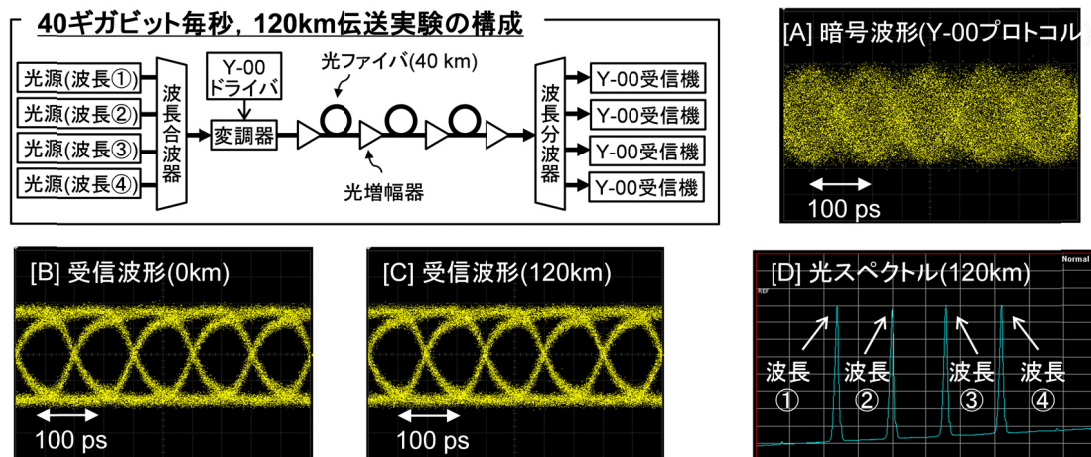
【背景】

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、前頁に示すように、光ファイバ回線から信号光を盗むことにより、容易に通信情報を盗み見られることを本学では実験検証した（大学プレスセンター、「クラウドコンピューティングの安全性の脆弱性を実証」、2010年8月16日）。ネットワークでは、個人情報や機密情報など数値暗号により暗号化されている通信情報もある。数値暗号は実用的な反面、解読可能性を完全に否定できない。更に安全性を高めるために、物理層に物理暗号を導入することが有効である。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た。Y-00 プロトコルの特長は、前頁に示すように、盗聴者に Y-00 の暗号文を盗ませない（正しく識別させない）点で、数値暗号と異なり、数理的なアルゴリズムによる解読法がないことや原理上盗聴不可能性を証明している。実験研究では、10 ギガビット毎秒の高速で通信距離 360 km の暗号通信、Y-00 通信試作器を用いた本学の実運用中の GbE ネットワークとの接続実験など、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。更に、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。光ファイバ回線に適用でき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。

今日、光ファイバ通信の伝送容量は大容量化が急速に進んでいる。そのため、これまでの最大伝送容量 10 ギガビット毎秒より大容量の Y-00 プロトコル通信を実現する方法の実験検証が求められていた。

【実験検証内容】

今回、異なる 4 波長の信号光を用いた WDM 方式による伝送実験を行った。各波長は 10 ギガビット毎秒の Y-00 プロトコルで、合計 40 ギガビット毎秒の容量の Y-00 プロトコルを一本の光ファイバに入力し、全長 120 km（1 スパン 40 km，計 3 スパン）の光ファイバ増幅中継伝送路を伝送させた。伝送後、波長毎に分岐して、Y-00 プロトコル受信機を用いて伝送特性を評価した。盗聴者が観測する暗号波形（Y-00 プロトコル）では、信号レベルを正しく識別できなかった（図 A）。一方、伝送前後の受信波形（図 B，C）に示すように、受信者は信号レベルを正しく識別できた。また、伝送後の受信波形は、伝送前の受信波形と同様の品質だった。伝送後の光スペクトル（図 D）は、各波長の信号が相互に悪影響を与えることはなかった。定量的な評価により、高品質な伝送を実現できたことが分かった。なお、伝送距離 120 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。