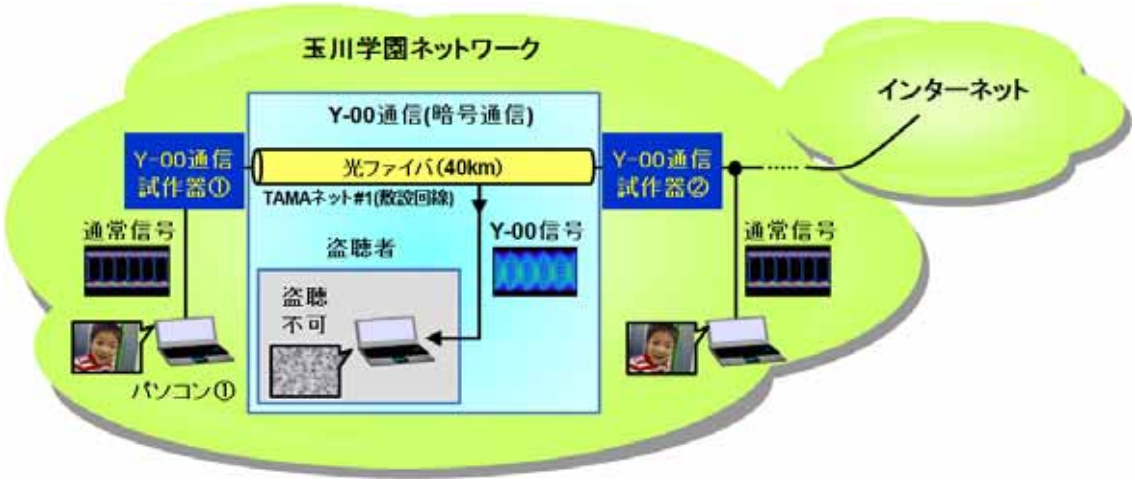
資料

【実験内容】

図に示すように、本学で実運用している光ネットワークおよびインターネットに接続されているネットワーク内に、インターネット用信号と Y-00 プロトコルを相互変換する Y-00 通信試作器 2 台を長さ 40km の敷設光ファイバ回線で接続し、試作器間が盗聴できない通信環境を構築した。その上で一方の Y-00 通信試作器に接続したパソコン①と、他方の Y-00 試作器を介して接続した本学ネットワークおよびインターネットとの暗号通信実験を行い、ホームページ閲覧や電子メールの送受信、動画ストリーミング受信、ファイル転送などネットワーク接続特性および盗聴可能性を調査した。なお、Y-00 通信試作器は、本学の設計に基づき、日立情報通信エンジニアリング株式会社が製作した。



【背景】

現状のネットワークでは、暗号化されていない平文も通信されており、これらの盗聴は容易である。個人情報や機密情報など暗号化されている通信も、数理暗号通信なので解読可能性を完全に否定できない。盗聴による情報漏洩を防ぐために、絶対に解読されない実用的な暗号技術が有効とされる。物理暗号では、理論上、絶対に解読されない究極の暗号を実現できることが知られており、量子鍵配送により秘密鍵を共有する方式や Y-00 方式が有名である。前者の方式の、現存の量子鍵配送装置を用いた実環境の暗号通信の世界最高速(注 2)は、45km の光ファイバ回線で毎秒約 0.1 メガ(10 万)ビットに過ぎず、今日、オフィスや自宅、都市間、大陸間通信の回線速度である毎秒ギガ(メガの千倍)ビット以上とは比較にならないほど遅い。致命的な問題は、既存の量子鍵配送装置の受信機で深刻な技術欠陥が発見され、秘密鍵を 100%の確率で盗聴できることが Nature Photonics 誌で報告(注 3)されたことであり、秘匿通信の実現にはこの欠陥の解消が不可欠と指摘された。従って、実用的な物理暗号方式は Y-00 が唯一の有力候補で、その実用化に大きな期待が寄せられている。

＊注２：プレスリリース「量子暗号ネットワークの試験運用開始」、(独)情報通信研究機構 量子 ICT グループ他　2010 年 10 月 14 日

＊注３：Nature Photonics 誌，Hacking commercial quantum cryptography systems by tailored bright illumination，686-689 頁　2010 年 8 月 29 日

【光通信量子暗号(Y-00)】

Y-00 方式は、高い安全性の保証が可能、毎秒ギガビット以上の高速で長距離通信(数100km 以上)が可能、現状の光ファイバ通信ステムと整合性がよいなどの特長があり、量子が持つ特性である量子雑音を利用し、解読不能な暗号を実現できることが理論的に証明されている。現在、実用化に向け、安全性や通信システム特性の実験検証が求められる開発段階にある。既に、敷設光ファイバ回線で 360km の伝送実験に成功しており、ネットワークにおける暗号通信の早急な実験検証が求められていた。