



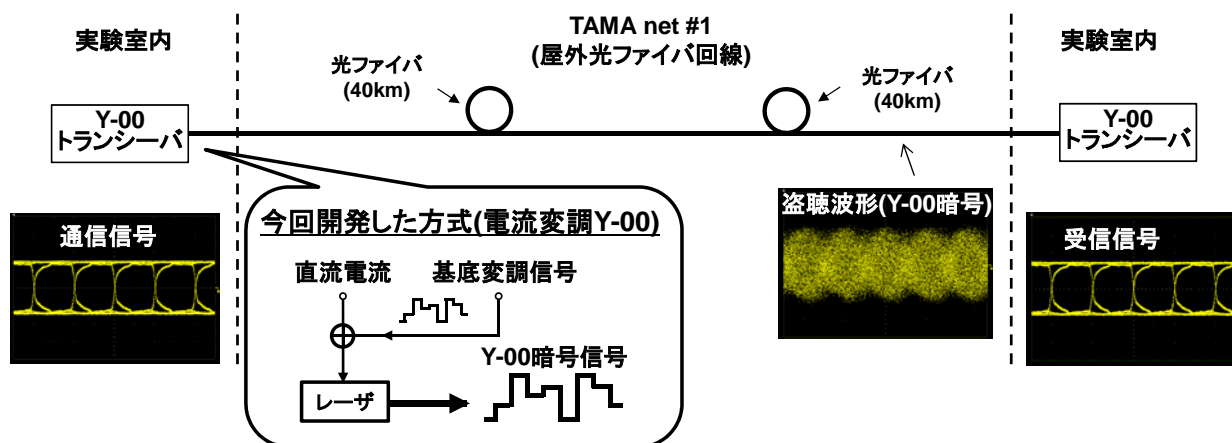
【背景】

現状のネットワークでは、光ファイバ回線で通信される情報は必ずしも暗号化されていない。そのため、光ファイバ回線から信号光を盗み、通信情報を盗み見られる危険性がある。通信情報は数値暗号によって暗号化される場合もあるが、数値暗号は解読の危険性が否めず、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。実際、DARPA は 5 月にギガビット毎秒を超える回線保護の暗号技術の本格開発を提案した。これにより、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および実験研究をすすめてきているが、Y-00 プロトコルの特長は、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、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、10 ギガビット毎秒で伝送距離 360 キロメートル、1 ヶ月にわたる長期運用試験など、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。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。

これまで外部変調器を用いた Y-00 暗号トランシーバの開発を行ってきたが、トランシーバの小型化は、加入者系などへの適用に向けた一つの重要な研究課題だった。外部変調器は小型化が困難なので、今回、光を発生するレーザの電流を変調する方法を提案し、本方式の Y-00 暗号トランシーバを試作し、屋外にある光ファイバ回線を用いて通信特性の評価を行い、良好な通信特性を検証した。

【実験検証内容】

電流変調方式の Y-00 暗号トランシーバ(2.5 ギガビット毎秒)を試作した。下図に示す本学内に敷設してある屋外光ファイバ回線において、80 キロメートル伝送後の通信特性を評価した。暗号鍵のない盗聴者が観測できる盗聴波形(Y-00 暗号信号)は信号レベルを識別できないが、暗号鍵を共有する正規受信者は、信号を正しく受信できた。伝送後の信号品質は、大きな劣化はなく良好な特性だった。通信特性(符号誤り率特性)を評価し、定量的にも良好な特性であることを検証した。なお、今回の検証実験では、光増幅器を使用しない加入者系の安価なシステムを想定した伝送路を用いたため、光パワー減衰が伝送距離を 80 キロメートルに制限した。光増幅器を用いれば、伝送距離の更なる延伸が可能である。



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。