2010．8．16

クラウドコンピューティングの安全性の脆弱性を実証

玉川大学学術研究所の量子情報科学研究センターの二見史生（ふたみ ふみお）准教授は、安心で安全なネットワーク構築には、絶対に解読されることがない可能性を秘めた光通信量子暗号(Y-00 プロトコル)の活用が重要であることを訴えることを目的に、学内光 LAN において通信情報のモニタ実験を実施し、現状のネットワークの安全性の脆弱さを露わにした。

【今回の成果】

現状のネットワークでは、平文(暗号化されていない文)もしくは数理暗号による暗号文が通信されており、情報漏洩の危険性を完全に排除できているとは考えがたい。解読される可能性のある数理暗号とは異なり、絶対的に解読が不可能な光通信量子暗号(Y-00)を次世代ネットワークに導入する必要性を訴えるため、実運用している本学 LAN において、電子メールやホームページ閲覧の通信情報をモニタし、ネットワークを流れる通信情報を容易にモニタできることを実験的に検証した。

本成果を、2010 年 8 月 16 日(月)、電子情報通信学会新世代ネットワーク時限研究専門委員会主催の新世代ネットワーク・ワークショップ 2010 において発表する。

題名：光通信量子暗号(Y-00)の高セキュアフォトニックネットワークへの展開に関する検討

【実験内容】

図１に示すように、本学で実運用している LAN に接続されているネットワークにおいて、情報伝達を担う光信号が行き交う光ファイバから光信号を採取し、ある特性の実験用パソコンによるホームページ閲覧(HTTP:HyperText Transfer Protocol)および電子メールの読み込み(POP3:Post Office Protocol v.3)の通信情報を解析機器に取り込み、それに含まれる情報の解析を行った。解析の結果、パソコン操作で得られた情報と同一の情報をモニタできた（図２）。更に、電子メール読み込み時の ID およびパスワードもモニタ可能だった。

なお、本実験は学内光 LAN に接続している他の情報端末を切り離すルータを介入させ、実験チームの情報端末のみをモニタする環境で実施された。

【取材に関するお問い合わせ先】
玉川学園 キャンパス インフォメーション センター
〒194‐8610　東京都町田市玉川学園 6‐1‐1
TEL：042‐739‐8710　E-mail：pr@tamagawa.ac.jp

2010．8．16

資料

【背景】

クラウドコンピューティングに代表される個人情報や機密情報がやり取りされるネットワークでは、通信情報の秘匿性（第三者に盗み見られないこと）が強く求められている。しかし、現状のネットワークでは、暗号化されていない平文で通信されている情報が少なくない。暗号化されていても数理暗号によるものである。数理暗号は、主に数学理論および計算量的安全性をその安全性の拠としているために、新たな解読手法が発見され解読に必要な計算量が激減する危険性、また、計算機能力の増大による危険が避けられない。実際にこれまで数理暗号解読は多数報告されており、現状のネットワークでは、情報漏洩の危険性を完全に排除できているとは考えがたく、情報を絶対に盗聴されない実用的な暗号技術が強く求められている。数学理論に基づかず、量子論的な特徴に着目した物理暗号は、絶対に解読できない暗号化を実現でき、その実用化は急務と考えられている。

【光通信量子暗号(Y-00)開発状況】

本学では、物理暗号の一つである光通信量子暗号(Y-00)の研究開発を行ってきている。量子が持つ特性である量子雑音を利用し、究極的に解読不可能な安全性を実現できる可能性のある暗号で、数理暗号を遙かに凌ぐ数々の特長を有している。今日、毎秒ギガ(10^9)ビット程度以上の速度で利用さている光ファイバ通信システムでの実用の目処が立たない、単一光子光源を利用する旧来の量子暗号方式とは異なり、Y-00 方式は、現在の光ファイバ通信システムと高い整合性があり、実用化の一歩手前の所まで来ている。既に玉川大学と日立情報通信エンジニアリング(株)は、毎秒 10 ギガビットの光強度変調-直接検波方式の Y-00 送受信器を開発し昨年 9 月に 360km の伝送実験に成功しており、安全で安心なネットワーク構築に Y-00 は大きな貢献が期待されている。

これらの期待に応じ、伝送距離の更なる延伸、伝送容量の拡大の研究開発と併せて、実用化に向け、実運用 LAN における試験や耐久試験の実施を計画している。現時点では、数理暗号の安全性を遙かに凌ぐ実用的な暗号方式は Y-00 が唯一と考えられ、高セキュアネットワークの早期実現に向け、その実用化が切に望まれる。