2011.1.24

玉川大学 学術研究所

世界初！ Y-00 暗号の強い安全性の根拠 「ランダム暗号性」の検証実験に成功

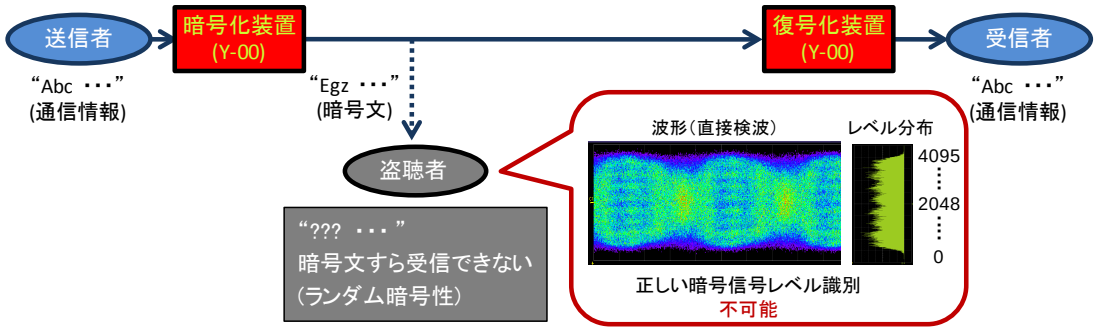
玉川大学（東京都町田市玉川学園 6-1-1　学長：小原芳明）学術研究所 量子情報科学研究センターの二見史生（ふたみ ふみお）准教授は、Y-00 暗号プロトコル（光通信量子暗号）が強い安全性を実現する画期的な性質である「ランダム暗号性」の実験検証に成功した。

従来の一般的な暗号では暗号化された信号そのものを盗聴でき、そこから暗号化前の通信情報を解読される可能性がある。今回の実験により、Y-00 暗号プロトコルは暗号化された信号そのものを盗聴することができないことが検証され、その強い安全性を裏付ける現象を確認することができた。本実験評価により Y-00 暗号プロトコルの実用化に向け大きく研究開発が前進した。

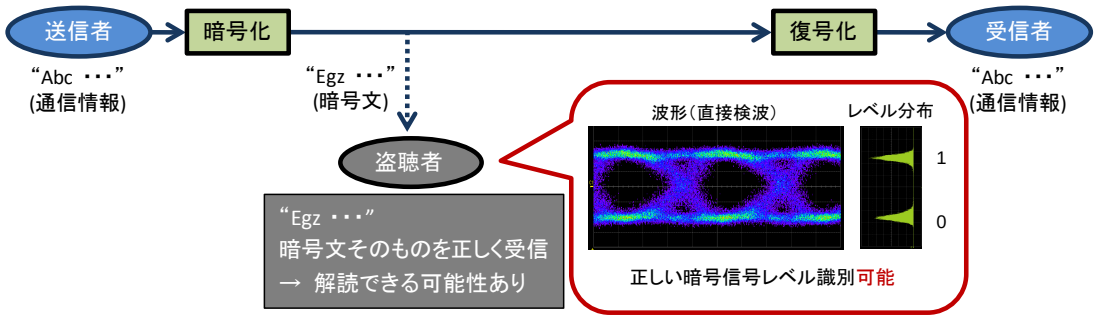
なお、本成果の詳細は 2011 年 1 月 27 日(木)、電子情報通信学会の光通信システム研究会において発表する。

題名：Y-00(光通信量子暗号)のランダム暗号としての性能評価実験

【本成果】 Y-00暗号プロトコル （信号レベル数：4096値）



【参考】 一般的な暗号 （信号レベル数：2値）



【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

2011.1.24

School To You!

資料

【今回の成果】

玉川大学では、クラウドコンピューティングをはじめとする様々なネットワークの利用形態の更なる発展が、安全性不備が原因で妨げられることがないように、盗聴できない通信を実現する暗号の研究開発を推進している。

安全性の保証を定量的に保証できない数理暗号と異なり、同大が研究開発を行っている Y-00 暗号プロトコルは安全性の定量化が可能とされる物理暗号で、通常の暗号が"0"、”1”の 2 値信号を用いるのに対して、Y-00 暗号プロトコルは多値の信号を用いる。一般に、暗号文を伝送する信号を正しく受信できなければ、情報の盗聴に繋がらない。物理暗号によるランダム暗号性は、鍵を有する正規受信者には暗号文を伝送している信号の正しいレベルを認識できるが、鍵を持たない盗聴者は正しい暗号信号レベルを識別できないという性質である。ランダム暗号性は、Y-00 暗号の安全性を保証する様々な性質のひとつであり、そのランダム量は安全性評価の重要な指標の一つであることが同大で示されている。

今回、盗聴者が直接検波方式で、Y-00 暗号プロトコル信号光（信号レベル数 4096 値）の盗聴を試み、正しい信号レベルの識別ができないというランダム暗号性の実験検証に成功した。

【実験検証内容】

今回、信号レベル数 4096 の暗号文の信号を出力する Y-00 通信試作器（日立情報通信エンジニアリング社製）を用いてランダム暗号性の実験検証を行った。直接検波方式と呼ばれる最も一般的な信号光受信方式を用いて信号光の盗聴を試みた。参考に、信号レベル数 2 値の一般的な暗号の信号光は、信号レベルが明確に分離され、正しい信号レベルの識別が可能、即ち、暗号そのものを認識できることを、前ページ図下段に示す。一方、前ページ図上段に示すように、Y-00 の暗号文を伝送している信号光の信号レベルは複数の信号レベルにまたがり、正しい信号レベルを識別できないことを実験検証した。実測値から定量的な解析を行った結果、1 つの正しい信号が 80 以上の信号レベルに誤って盗聴者に認識されることが解った。これにより、Y-00 暗号プロトコル信号光（信号レベル数 4096 値）の盗聴を試みても、正しい信号レベルの識別ができないというランダム暗号性が検証された。正規受信者は暗号を復号するための鍵をもっているので、このような波形からでも正しい信号を受信できる。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情報も通信されており、このような通信は容易に盗み見られることを同大では実験検証した。個人情報や機密情報など数理暗号により暗号化されている通信情報もあるが、数理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、物理層における物理暗号の導入が有効である。同大では、物理暗号のひとつである Y-00 暗号プロトコルの理論研究をすすめ、数理的なアルゴリズムによる解読法がなく、その高い安全性を示している。一方、実験研究は、毎秒 10 ギガビットの高速で通信距離 360 km の暗号通信、Y-00 通信試作器を用いた実運用中の GbE ネットワークとの接続試験など、Y-00 暗号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。光ファイバ通信応用とし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おり、理論検討に加えて、安全性評価に関する実験検証が求められていた。