



Y-00 光通信量子暗号の光ファイバ通信応用

玉川大学 量子情報科学研究所
二見史生

1. はじめに

昔から情報を秘密にするために暗号が用いられてきた。古くは、紀元前 5 世紀にスパルタで転置式暗号が、紀元前 1 世紀にはジュリアス・シーザーにより換字式暗号（シーザー暗号）が用いられた。現代暗号以前のこれらの暗号では暗号アルゴリズム自体が秘匿にされていた。現代暗号では暗号アルゴリズムは公開される。暗号アルゴリズム自体を秘密にすることは困難である上、公開することによりアルゴリズム上の弱点がないか専門家が調査できる利点があるのが一つの理由である。一般的な暗号通信の方式は、共通鍵暗号方式と公開鍵暗号方式がある。両者の相違点は、暗号化と復号化に使う鍵である。共通鍵暗号方式では、事前に共有した暗号鍵を暗号化・復号化に利用する。公開鍵暗号方式では、誰でも取得できる公開鍵を暗号化に利用し、復号化には自分だけが秘密に保持している秘密鍵を用いる。数理論法を暗号アルゴリズムに用いる数理論暗号は実用的で、我々は日常生活で意識せず利用し、恩恵を受けている。ただ、便利で有益であるが、万能ではない。効率的な解読方法の発見により暗号が危殆化する可能性をはらんでいる。これは数理論暗号の原理的な課題で、数理論暗号だけで安全性を保証することはかなりの難問である。そのため、常に解読リスクに留意する必要がある。

ところで、光ファイバ通信技術に目を向けると、90 年代後半から急激に通信容量が増大し、現在では、一本の光ファイバ回線で毎秒ペタビット以上の通信が可能になっている。大容量通信技術の発展により、便利で豊かな社会が実現されているが、一方で、光ファイバ回線から大容量のデータが一気に盗まれるという新たな危険性が生じた。大容量データ流失の被害は甚大になるとことが予想されている。対策の一つは、数理論暗号を用いる。別の対策法は、光ファイバ回線である物理層は他の上位の階層と異なり物理現象が伴うため、これを利用して情報を守る。当研究所では物理効果も用いて物理層を守る暗号技術の研究開発に取り組んでいる。数理論法で生成する擬似乱数と物理現象に起因する物理的ランダム性の両者を組み合わせた暗号で、Y-00 光通信量子暗号（以下、Y-00 暗号）と呼んでいる。本暗号は、雑音のランダム性を利用して、暗号文を盗聴者（暗号鍵を持たない者）に読み取らせない点を最大の特徴とする。

ここで、「光通信量子暗号」と呼ぶ理由を説明しておく。雑音で暗号信号を覆ってしまうと、暗号信号を隠せる。原理的に除去できる雑音と除去できない雑音があるが、検出される光子数の揺らぎに起因する量子雑音は除去できない。この量子雑音が暗号信号をマスクすることにより高い安全性を実現する。暗号鍵を所有する正規の通信者は量子雑音の影響を無視でき、通常の光通信ができる。以上の理由で、光通信量子暗号と呼んでいる。

本稿では、はじめに光ファイバ回線が直面している脅威を説明する。次に、Y-00 暗号の原理や特徴を解説し、試作した GbE 対応の Y-00 暗号トランシーバを紹介する¹⁾。最後に、光ファイバ通信への応用実験を紹介する²⁻⁶⁾。Y-00 暗号トランシーバを用いた波長分割多重伝送実験やネットワーク応用実験は詳細も紹介する。