次世代量子鍵配送としての RRDPSQKD

RRDPSQKD as a next-generation quantum key distribution protocol

○ 佐々木 寿彦 [1](1. 東大院工)
○Toshihiko Sasaki[1] (1.Univ. of Tokyo)
E-mail: sasaki@qi.t.u-tokyo.ac.jp

量子鍵配送は量子通信路 (主に光ファイバー) で結ばれた遠隔 2 者 (Alice, Bob) 間で情報論的に安全な秘密鍵を共有するための手法である。広く受け入れられている原理の説明としては、Alice と Bob が量子的な状態によって情報をやりとりしようとしたときに、盗聴者が誤差を小さくするように状態を測定しようとするならば量子力学の不確定性関係により必ず擾乱がおこるので、Alice と Bob は擾乱を監視することで Eve の盗聴を検出することができるというものである。

一方で、最近 Round-robin differential-phase-shift 量子鍵配送方式 (RRDPSQKD) という方式を提案した [1]。この方式は下図のように、送信側は微弱光パルス発生装置と位相変調機、受信側は遅延長さを変更可能な遅延干渉計という構成になっている。この構成で遅延を隣あうパルスの間隔に固定し光を強くすると、光通信における差動位相変調方式 (DPS) になる。Round-robin は総当りという意味で、遅延長さを変えることにより、確率的にではあるが様々なパルス間の位相差を調べることを表している。このように比較的シンプルな構成でありながら、この方式では擾乱を監視せずに安全性を保証することができる。つまり、前述の説明のような「読まれたら気づく」というような方式ではなく「そもそも読みづらい」という方式になっている。

さて、確かに理論的には面白い RRDPSQKD ではあるが、鍵配送としての利点はあるのだろうか。「読まれたら気づく」という方式では、通信路のノイズは盗聴行為によるものとみなさなくてはいけなくなるので、通信路のノイズが増えるとそれが盗聴によるものかどうかに依らず性能が低下する。また、気づくためにはサンプリングを行う必要があり、一定数以上のサンプルを確保するためのコストも発生する。「そもそも読みづらい」という方式である RRDPSQKD の場合、通信路のノイズが増えても盗聴量が増えたとは思わなくてよいので高いエラー耐性がある。また、安全性の保証のためにサンプリングを行う必要もなく、短い通信時間で効率的な通信ができる。

本講演では、RRDPSQKD が何故「そもそも読みづらい」方式になっているのかを解説し、課題や最近の進展について議論したい。

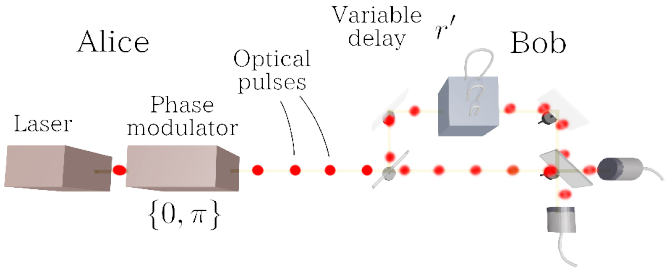

図 1: RRDPSQKD の実験概要図

[1] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014)