総当たり差動位相シフト量子鍵配送実験

Round-robin differential phase shift quantum key distribution experiment

NTT 物性研 [1]、東京大学 [2]
○ 武居弘樹 [1]、佐々木寿彦 [2]、玉木潔 [1]、小芦雅斗 [2]
NTT BRL[1], Univ. of Tokyo[2]
○H. Takesue[1], T. Sasaki[2], K. Tamaki[1], M. Koashi[2]
E-mail: takesue.hiroki@lab.ntt.co.jp

はじめに: 従来の量子鍵配送 (quantum key distribution: QKD) においては、秘匿性増幅量を見積もるために誤り率の監視が必須であると考えられてきた。最近提案された総当たり差動位相シフト (round-robin differential phase shift: RRDPS)QKD は、誤り率測定を必要とせず、システムのパラメータのみにより秘匿性増幅量が決定される新しい QKD 方式である。今回、RRDPS 方式に基づく QKD 実験を初めて行ったので報告する。

RRDPS 方式: アリスは従来の差動位相シフト（DPS）方式 [2] と同様に、L 連の微弱コヒーレントパルスからなるパケットに対しランダムな $\{0, \pi\}$ 位相変調を施した後、光伝送路を介してボブに送付する。ボブは、従来の DPS 方式では隣接する 2 パルス間の位相差のみを測定していたのに対し、RRDPS 方式では各パケットからランダムに 2 パルスを選択し位相差を測定する。この測定位相差選択のランダム性により、盗聴者が取得可能な情報量が著しく制限される。その結果、シフト鍵 1 ビットあたりの秘匿性増幅係数は $\sim h(\nu/(L-1))$ となる（$h(x)$ は 2 値エントロピー関数、ν は L パルス中の総光子数)。すなわち、秘匿性増幅係数が誤り率に依存せず、パケット長 L と光源の光子統計のみによって決定されるという特徴を有する。

実験系: 実験系を図 1 に示す。繰り返し周波数 2 GHz で発生されたコヒーレントパルス列に対し 5 パルス毎にパケットを定義する ($L = 5$)。アリスは各パケットのパルスに $\{0, \pi\}$ のランダム位相変調を行い、パルスあたり平均光子数 $\mu \ll 1$ となるように減衰した後、光ファイバ伝送路を介してボブに送付する。ボブは、受信したパケット列を 1×4 スプリッタに入力する。スプリッタの 4 つの出力ポートには、2 光路の時間遅延が $\{T, 2T, 3T, 4T\}$ の 4 つの遅延干渉計がそれぞれ接続されている ($T = 500$ ps)。遅延干渉計から出力された光子は超伝導単一光子検出器 (SSPD) により検出される。この構成により、ボブが受信する各光子に対し 4 つの時間遅延をランダムに選択して位相差測定を行うことができる。なお、本実験では遅延時間 T と $4T$、$2T$ と $3T$ の干渉計出力を、一方に対し 250 ps の遅延を付与した後それぞれ 3 dB カプラで合波し、一つの検出器で受信することで、必要な光子検出器の台数を半減した。

実験結果: 伝送距離 30 km において、誤り率 1.8%、漸近極限での安全鍵生成率 6 bit/s を得た。また、有限長解析を行った結果、最大伝送距離 20 km における安全鍵生成が可能であった。

本研究は革新的研究開発推進プログラム (ImPACT) により委託されたものです。

参考文献

[1] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **19**, 18091 (2014).
[2] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).

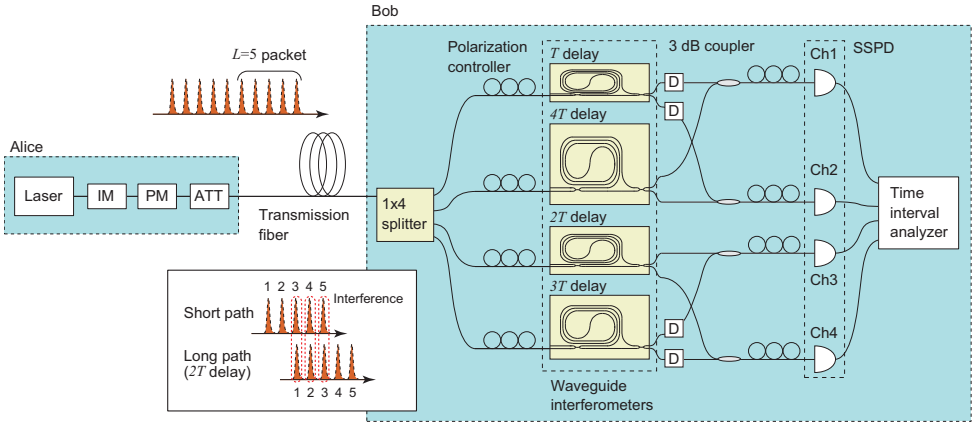

図 1: Experimental setup of RRDPS QKD