測定装置無依存 DPS-QKD のシステム性能

System Performance of Measurement-Device-Independent DPS-QKD

山本　利龍、○井上　恭（阪大工）

Toshitatsu Yamamoto, ○Kyo Inoue (Osaka Univ.)

E-mail: toshitatsu@procyon.comm.eng.osaka-u.ac.jp

[はじめに]近年、量子鍵配送（QKD）研究では、光子検出器の不完全性を突くサイドチャンネル攻撃を回避する測定装置無依存（MDI）QKD の検討が進められている[1,2]。我々は、その一方式として差動位相シフト（DPS）QKD 方式に基づく MDI-QKD プロトコルを提案した[3]。本研究では、その性能評価を行った。

[構成]図１に MDI-DPS 方式の構成を示す。アリス/ボブは、位相がランダムに{0, π}変調された微弱コヒーレントパルス列をチャーリーに送信する。チャーリーは、送られたパルス列を同じタイミングで２×２カップラで合波し、出力端にて光子検出する。そして、隣り合う２回の光子検出事象につき、{同じ検出器が検出したか、異なる検出器が検出したか} をアリス/ボブに通知する。アリス/ボブはチャーリーからの時刻/検出器情報を基に秘密鍵を生成する。本システムでは、チャーリーが盗聴者に乗っ取られていても鍵の秘匿性は保たれる。

[盗聴法]本プロトコルに対する盗聴法として、Beam Splitting Attack（BSA）および、なりすまし盗聴（IRA）を検討した。BSA においてイブは、分岐したパルス列を保持しておき、チャーリーの光子検出時刻情報を得た後に、所望の２パルスを干渉させることで鍵ビットを得る。この BSA はアリス/ボブそれぞれの伝送路で行うことができる。IRA では、イブはインターセプトした信号を MZ 干渉計で受信し、アリス/ボブの信号のパルス間位相差を読み取る。イブが、アリス/ボブの光子を同時刻に検出した場合に盗聴成功となる。なお IRA では、無損失ファイバを用いることにより伝送損失分、アリス側とボブ側での検出時刻が異なる事象を廃棄することができ、これにより盗聴量が最大化される。

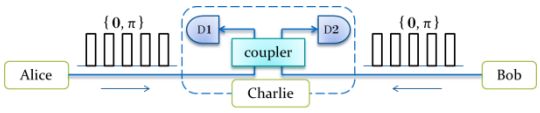

図１　システム構成

[計算結果]図２に従来 DPS-QKD と MDI-DPS-QKD の最終鍵生成率の計算例を示す。本プロトコルの方が従来プロトコルより最大伝送距離が伸びていることがわかる。また本プロトコルに対しては、BSA の方が IRA より伝送距離を制限する強力な盗聴法であることがわかる。

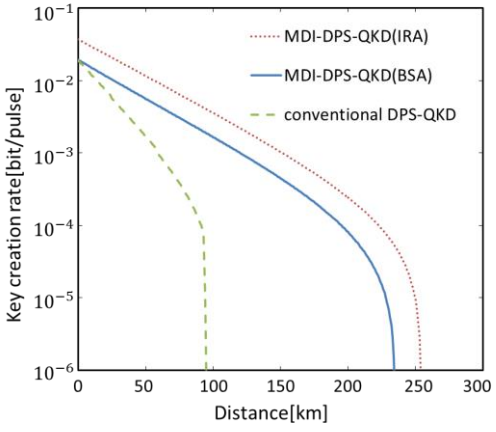

図２　最終鍵生成率

[1]H. Lo 他, PRL **108**, 130503 (2012).

[2]X. Ma and M. Razavi, PRA **86**, 062319 (2012).

[3]井上　恭、応物 2014 秋、18p-C2-3.