位相非同期 MDI-DPS-QKD のシステム性能

System Performance of phase-asynchronized coherent MDI-DPS-QKD

阪大工　○(M2)山本　利龍，井上　恭

Osaka Univ. , ○Toshitatsu Yamamoto, Kyo Inoue

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。前回我々は、差動位相シフト（DPS）QKD 方式に基づく MDI-QKD プロトコルの性能評価を行ったが、そこではアリス/ボブの信号光が位相同期されているものとした[1]。今回は、位相非同期状態でのシステムを性能評価したので報告する。

[構成]Fig. 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タイミングを合わせて２×２カプラで合波し、出力端にて光子検出する。そして、隣り合う二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/検出器情報を基に鍵ビットを生成する。ここで、アリス/ボブのパルス列が位相非同期であると鍵の誤り率は高くなるが（平均 25%）、この誤りはバースト的であるため誤り率の高いブロックを廃棄することで秘密鍵を生成することができる。

[盗聴法]本プロトコルへの代表的な盗聴法である、Beam Splitting Attack(BSA)に対するシステム性能を検討した。BSA においてイブは、アリス/ボブそれぞれの伝送路上で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。

[計算結果]Fig. 2 に位相同期時と非同期時の計算結果を示す。位相非同期時には廃棄するビットが多いため最終鍵生成率が低くなるが、最大伝送距離はほぼ同じという結果が得られた。

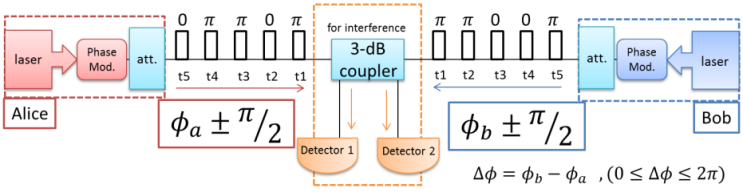

Fig.1 System configuration

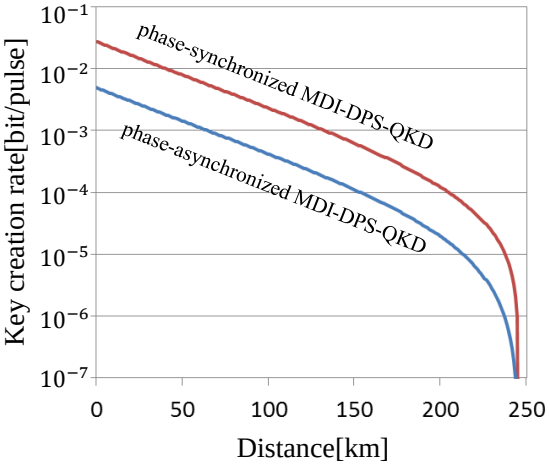

Fig.2 Key creation rate as a function of distance

[1]山本　利龍，井上　恭、応物 2015 秋、16a-PA1-3.