量子もつれ中継測定装置無依存 DQPS-QKD

Entanglement Relaying MDI-DQPS-QKD

阪大工　○(M2)陳　思宇，井上　恭
Osaka Univ. , ○SiYu　Chen, Kyo Inoue
E-mail: chen@opt.comm.eng.osaka-u.ac.jp

[はじめに]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）量子鍵配送（QKD）が研究されている[1]。我々は以前に、差動位相シフト（DPS）方式に基づく MDI-QKD プロトコルを提案した[2]。本研究では、これを長距離化するため、単一光子時間位置重ね合わせ状態を 4 値位相変調（DQPS）し、さらに量子もつれ中継系に拡張した方式を提案し、そのシステム性能評価を行った。

[構成]図 1 にシステム構成を示す。Alice(A)/Bob(B)は$\{0,\pi\},\{-\pi/2,\pi/2\}$で 4 値位相変調した単一光子時間位置重ね合わせ状態のパルス列を、もつれ光源は時間位置もつれ光子パルス列を、Charlie1，2 にそれぞれ送信する。Charlie1，2 は送信されたパルス列を 3dB カプラで干渉測定し、光子検出した時刻と検出器を公開する。本システムでは、両 Charlie の時刻 n， m での光子検出事象と A＆B の変調位相差$\{\Delta\theta_a,\Delta\theta_b\}$に次のような相関関係がある。Charlie1,2 が 2 時刻共に同じ検出器あるいは異なる検出器で光子検出した場合、A＆B の変調位相差は$\Delta\theta_a+\Delta\theta_b=0,2\pi$を満たしており、Charlie1 が同じ検出器、かつ Charlie2 が異なる検出器で光子検出、あるいは Charlie 1 が異なる検出器、かつ Charlie 2 が同じ検出器で光子検出した場合、A＆B の変調位相差は$\Delta\theta_a+\Delta\theta_b=\pm\pi$を満たしている。但し、$\Delta\theta_a+\Delta\theta_b=\pm\pi/2$の場合は相関性がない（基底不一致）。そこで、光子伝送後、A&B は光子検出時刻に該当する位相変調基底情報を交換し、基底一致の検出事象につき、上記相関特性に基づき、両 Charlie の検出情報と自身の変調データから鍵を生成する。基底不一致の検出事象は廃棄する。

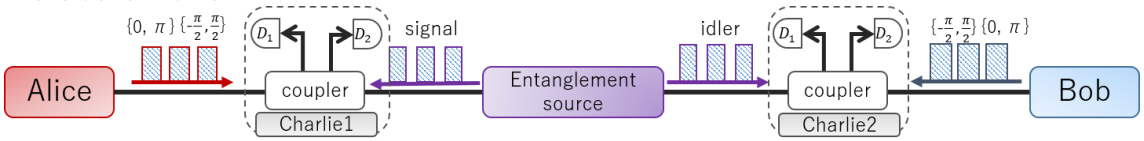

図 1　システム構成

[安全性]本プロトコルはパルス位相差を非直交な 2 基底で変調しており、外部盗聴に対する安全性は BB84 と同様である。本システムは量子もつれパルス列の相関特性を利用しており、盗聴者 Eve がもつれ光源を乗っ取り古典もつれパルス列を送信すると、A&B と基底不一致の場合にビットエラーと誘発する。このビットエラーの増大から、A&B は盗聴を検知する。さらに、Charlie が盗聴者だったとしても、光子検出事象だけからは鍵情報を得ることができないため、安全性が保障される。

[システム性能]図 2 に Intercept-Resend Attack を考慮した最終鍵生成率の計算結果を示す。伝送距離限界は 470 kmである。もつれ中継に適応しない場合に比べ、伝送距離が 2 倍となっている。

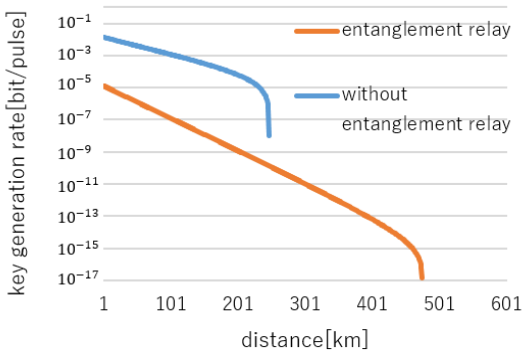

図 2　最終鍵生成率

[1]H. Lo 他, PRL 108, 130503 (2012).
[2]山本、井上、応物 2015 秋，16a-PAI-3.