量子もつれ中継による測定装置無依存 DPS 量子鍵配送の提案

Entanglement Relaying Measurement Device Independent DPS Quantum Key Distribution

阪大工　○井上　恭

Osaka Univ.　○Kyo Inoue

E-mail: kyo@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量子鍵配送（QKD）方式として、測定器無依存（MDI）QKD が研究されている[1, 2]。これに関し我々は、差動位相シフト（DPS）信号光を用いる MDI-QKD プロトコルを提案した [3]。本発表ではこれを量子もつれ中継系に拡張した方式を提案する。

[構成] 図 1 に提案方式の構成を示す。アリス/ボブは｛0, π｝で位相変調された微弱コヒーレントパルス列を、もつれ光源は時間位置もつれ光子パルス列を、それぞれ送信する。チャーリー１（２）は、送られた信号光を 3dB カップラで合波して光子検出し、検出時刻と検出器をアリス/ボブに通知する。アリス/ボブはチャーリーの情報及び自身の変調データから秘密鍵を生成する。

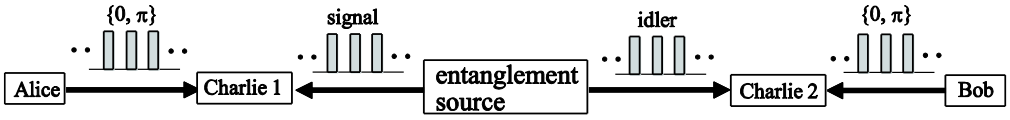

図１． システム構成

[動作原理] 平均光子数が十分小とすると、時刻{t_n, t_m}でチャーリー1&2 が共に光子検出する状態は次のように表される。

$$|\Psi_{nm}\rangle \propto e^{i(\theta_{am}+\theta_{bm})}(i|n\rangle_{11}+|n\rangle_{12})(i|n\rangle_{21}+|n\rangle_{22})(|m\rangle_{11}+i|m\rangle_{12})(|m\rangle_{21}+i|m\rangle_{22})$$
$$+e^{i(\theta_{an}+\theta_{bn})}(|n\rangle_{11}+i|n\rangle_{12})(|n\rangle_{21}+i|n\rangle_{22})(i|m\rangle_{11}+|m\rangle_{12})(i|m\rangle_{21}+|m\rangle_{22})$$

$|n\rangle_{12}$: チャーリー１の検出器２が時刻 t_n で光子検出する状態、θ_{an} : アリスの n 番目パルスの位相、他も同様。上式は 16 状態の重ね合わせとなっているが、１行目からの項と２行目からの項の干渉の結果、$\Delta\theta_a + \Delta\theta_b = 0$ では８状態、πでは残りの８状態、のみが存在し得る（$\Delta\theta_a = \theta_{an} - \theta_{am}$、$\Delta\theta_b = \theta_{bn} - \theta_{bm}$）。そこでアリス/ボブは、時刻{$t_n$, t_m}で両チャーリーが共に光子検出した事象について、前者のパターンの場合は$\Delta\theta_a = \Delta\theta_b = 0\ (\pi)$ なら「０（１）」、後者のパターンの場合は一方がビット反転、としてビットを生成する。これによりアリス/ボブは秘密鍵ビットを得る。

本方式では連続パルス列を用いており、同時検出の度にその前の同時検出状態との位相差から鍵ビットが生成される。このような信号光がインターセプト盗聴されると、盗聴パルスと次の同時検出パルスとの位相差情報が失われ、ビット誤りが生じる。これより盗聴が検知される。

[1] H. Lo 他, PRL **108**, 130503 (2012). [2] X. Ma and M. Razavi, PRA **86**, 062319 (2012). [3]山本、井上、応物講演会 2015 秋, 16a-PA1-3.