18p-C2-3

測定装置無依存 DPS 量子鍵配送

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] 近年、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、測定装置無依存（MDI）QKD の検討が進められている[1, 2]。これまで提案された MDI-QKD は、基本的には伝統的な BB84 プロトコルに準拠している。これに対し本報告では、差動位相シフト（DPS）QKD 方式に基づく MDI-QKD プロトコルを提案する。

[構成] 図１に提案方式の構成を示す。アリス/ボブは、位相がランダムに｛0, π｝変調された単一光子時間位置重ね合わせ状態または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光カップラで合波し、出力端にて光子検出する。そして、異なる時刻で光子検出した事象につき、｛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。すなわち、光子検出器の特性に依らずに秘密鍵が生成される。

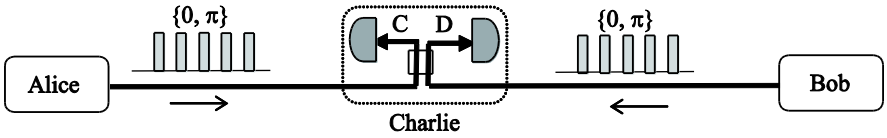

図１．システム構成

[動作原理] 単一光子信号の場合、ビームスプリッタ後の量子状態のうち、時刻 j と時刻 k で共に光子検出される状態は次のように表される。

$$|\Psi_{\mathrm{out}}^{(jk)}\rangle = \frac{i}{2N} e^{i(\theta_{\mathrm{a}(j)}+\theta_{\mathrm{b}(j)})}[\{e^{i(\theta_{\mathrm{b}(k)}-\theta_{\mathrm{b}(j)})} + e^{i(\theta_{\mathrm{a}(k)}-\theta_{\mathrm{a}(j)})}\}\{|j\rangle_{\mathrm{c}}|k\rangle_{\mathrm{c}} + |j\rangle_{\mathrm{d}}|k\rangle_{\mathrm{d}}\}$$

$$+\{e^{i(\theta_{\mathrm{b}(k)}-\theta_{\mathrm{b}(j)})} - e^{i(\theta_{\mathrm{a}(k)}-\theta_{\mathrm{a}(j)})}\}\{|j\rangle_{\mathrm{c}}|k\rangle_{\mathrm{d}} - |j\rangle_{\mathrm{d}}|k\rangle_{\mathrm{c}}\}]$$

（$|j\rangle_{\mathrm{c(d)}}$：端子 c（d）において j 番目パルスに１光子が存在する状態、$\theta_{\mathrm{a}(j),\mathrm{b}(j)}$：アリス/ボブの j 番目パルスの位相、N：パルス数）。上式は、$\{\theta_{\mathrm{a}(k)} - \theta_{\mathrm{a}(j)} = \theta_{\mathrm{b}(k)} - \theta_{\mathrm{b}(j)} = 0\}\{\theta_{\mathrm{a}(k)} - \theta_{\mathrm{a}(j)} = \theta_{\mathrm{b}(k)} - \theta_{\mathrm{b}(j)} = \pi\}$ ならば同じ検出器で、$\{\theta_{\mathrm{a}(k)} - \theta_{\mathrm{a}(j)} = 0, \theta_{\mathrm{b}(k)} - \theta_{\mathrm{b}(j)} = \pi\}\{\theta_{\mathrm{a}(k)} - \theta_{\mathrm{a}(j)} = \pi, \theta_{\mathrm{b}(k)} - \theta_{\mathrm{b}(j)} = 0\}$　ならば異なる検出器で、それぞれ光子検出することを示している。この相関特性を利用してアリス/ボブは鍵ビットを生成する。微弱コヒーレント信号の場合は、アリス/ボブが位相同期されていれば、同様にして鍵ビットが生成される（ただし生成確率は小）。

[まとめ] DPS 方式に準拠した測定器無依存量子鍵配送プロトコルを提案した。

[1] H. Lo 他, PRL **108**, 130503 (2012). [2] X. Ma and M. Razavi, PRA **86**, 062319 (2012).

© 2014 年　応用物理学会