16p-A14-9

レーザ光を用いた差動位相シフト量子鍵配送の連続クリック攻撃による距離制限

Practical DPS-QKD Distance Limited by Sequential Attack

阪大工　　岡　徹*，○井上　恭

Osaka Univ.　　Akira Oka*, ○Kyo Inoue

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

[はじめに] 差動位相シフト量子鍵配送(DPS-QKD)に対しては、連続クリック攻撃(SQA）が最も強力とされている[1]。これに対し我々は、有限線幅の光源を用いたシステムでは必ずしもそうではないことを報告した[2]。今回これを再検討し[3]、結果を更新したので報告する。

[レーザ光を用いた DPS-QKD に対する SQA] SQA では、DPS 信号を USD(Unambiguous State Discrimination)測定し、その結果に基づいて連続パルスを再送する。USD 測定にあたっては信号光の搬送波位相を知っておく必要があるが、レーザ光は位相が変動するため、搬送波位相を抽出したうえで USD 測定を行うことになる。この際、光源線幅に依存して抽出誤差が生じ、USD 測定に誤り発生→SQA 盗聴能力低下→DPS-QKD システム性能向上、となる。本報告では、この USD 誤り率の導出過程を見直し、より実際の状況に近いものとした。

[計算結果] 図 1 に位相抽出誤差の確率分布（平均光子数 0.2/pls）、図 2 に USD の誤り率と識別確率、のシミュレーション結果を示す。位相抽出誤差のため識別誤りが起こる様子が示されている。図 3 は伝送距離に対する秘密鍵生成率、図 4 は光源線幅に対する伝送距離である（パルス周波数 =1GHz、up-conv.検出器を想定）。比較のため、図 4 には一般個別攻撃及び遅延干渉計を用いた SQA についての結果も示してある。SQA が最強ではないことが示されている。

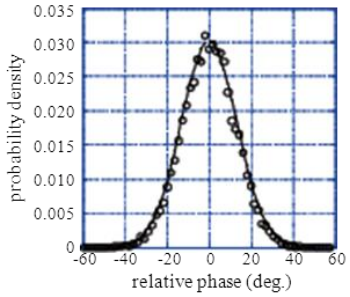

図 1　位相抽出誤差分布

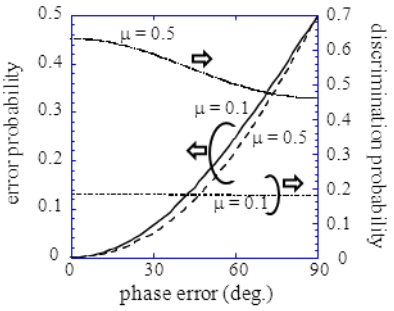

図2　USD誤り率/識別確率

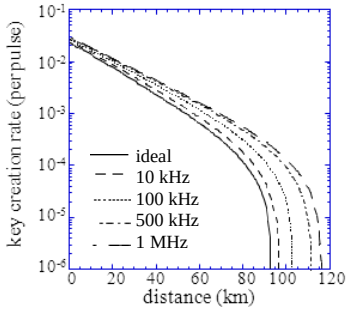

図3　秘密鍵生成率

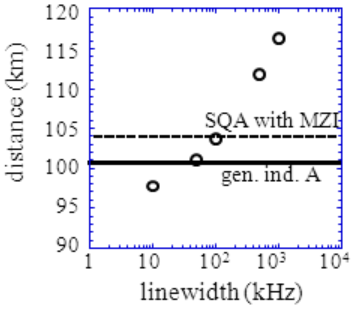

図4　QKD伝送距離

[1] T. Tsurumaru, Phys. Rev. A **75**, 062319 (2007).

[2] 岡、井上、応物 2012 春、17p-GP2-1.

[3] A. Oka, K. Inoue, “Quisi-umbiguous state discrimination for coherent states with phase fluctuation,” to be published in Opt. Comm.

* 現所属 株式会社フジクラ Fujikura Ltd.

© 2013 年　応用物理学会