強度変調 DPS 量子鍵配送方式の提案

Intensity-Modulated DPS Quantum Key Distribution

○楠 知也、田中 善人、井上 恭(阪大工)

○Tomoya Kusunoki, Yoshito Tanaka, Kyo Inoue (Osaka Univ.)

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

[はじめに]差動位相シフト量子鍵配送（DPS-QKD）方式は、構成が簡便で利便性に優れた QKD プロトコルである[1]。このプロトコルに対する最も強力な盗聴法として、連続クリック攻撃（SQA）が知られている[2]。本研究ではこの盗聴対策として、信号の平均光子数をフレーム毎にランダムな二値とするプロトコル（IM-DPS-QKD）を提案する。

[構成]図 1 に、提案方式の構成と送信パルス列の例を示す。アリスはコヒーレント信号パルスを$(0,\pi)$でランダムに位相変調する。そして、パルス列を 10 から 20 パルス毎にフレーム化し、フレーム毎にパルス当りの平均光子数が 2 値（μ_1,μ_2）のいずれかとなるようにランダムに強度変調する。ボブはこれをＭＺ干渉計で受信し、パルス間位相差から鍵ビットを得る。その後、アリスはボブにフレームの切り替え時刻を通知し、ボブからアリスへは光子検出時刻を通知する。アリスは自身の変調データから鍵ビットを知ることができ、誤り訂正・秘匿性増強後に、両者で秘密鍵を得る。

[盗聴検知方法]IM-DPS-QKD では 2 値の強弱パルスの平均光子数をチェックすることで盗聴を検知する。SQA では、イブはアリスの送信パルスを連続測定し、測定結果に応じてボブに連続パルス列を再送する。このときイブは、受信信号の光子数が微少であるため、各フレームの平均光子数は分からず、フレーム毎のボブの光子検出確率を変えないように信号再送することはできない。そのため、フレーム毎のボブの光子検出確率が正常時と異なることになり、これより盗聴が発覚する。

[計算結果]イブは光子数揺らぎに紛れて SQA を行うものとして、提案方式のシステム性能を評価した。図 3 に従来 DPS-QKD 方式(μ = 0.2[photon/pulse])と IM-DPS-QKD 方式($\mu_1 = 0.1, \mu_2 = 0.3$)の最終鍵生成率を示す。本方式の有効性が示されている。

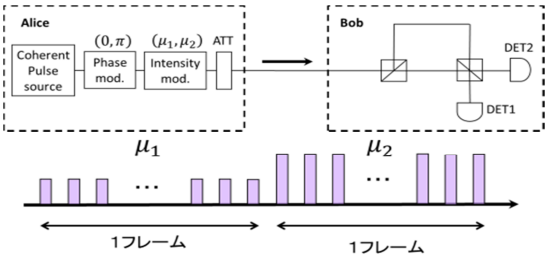

図 1　提案方式の構成

[1]K.Inoue et al., Phys. Rev. A 68, 022317(2003)

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

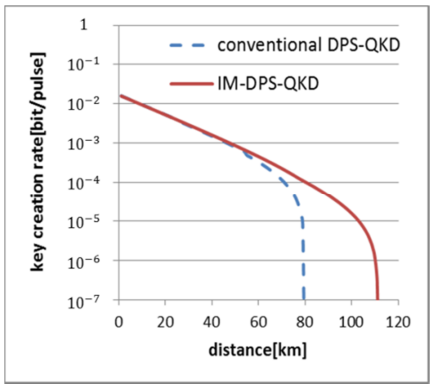

図 2　最終鍵生成率