Can Two-Way Direct Communication Protocols Be Considered Secure?

Mladen Pavičić
Center of Excellence for Advanced Materials and Sensing Devices (CEMS), Photonics and Quantum Optics Unit, Ruđer Bošković Institute, Zagreb, Croatia and *Department of Physics, Nanooptics, Humboldt-University Berlin, Germany* Email: mpavicic@irb.hr, web site: http://www.irb.hr/users/mpavicic

We consider intercept-resend attacks on two kinds of direct two-way QKD protocols - ping-pong Bell state protocol with entangled photons [1] and LM05 with single photons [2] - in which an undetectable Eve can decode all the messages in the message mode (MM) and show that the mutual information between parties (Alice, Bob, and Eve) is not a function of disturbance but is always maximal and equal to unity as shown in Figure 1(b).

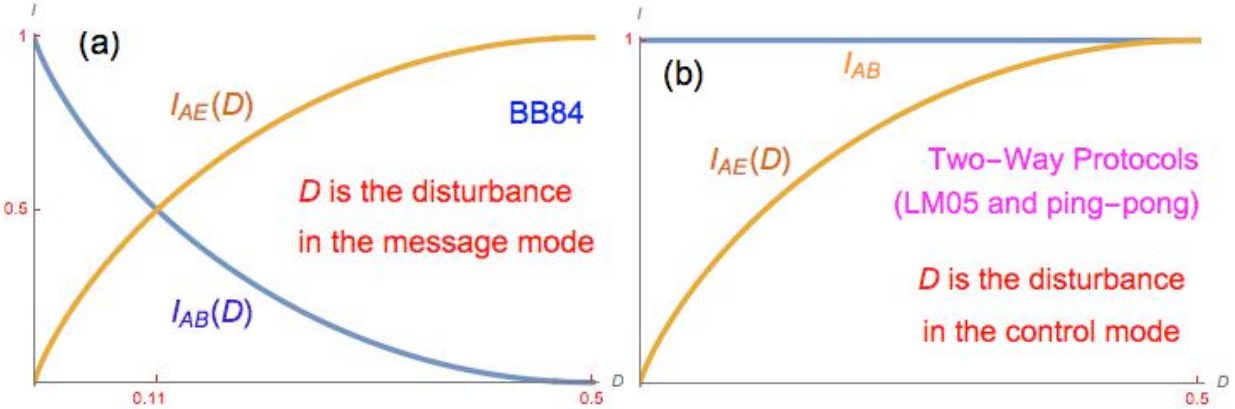

Fig. 1. Mutual information plots for (a) the one-way probabilistic protocol BB84 vs. (b) two- way deterministic protocols with either entangled Bell states or with LM05-like single photon states. Essential difference between them is that in (a) Eve causes polarization flips in the message mode, while in (b) Eve ideally does not cause any polarization flip in the message mode.

The disturbance (D) Eve induces is in the control mode (CM) and therefore the standard approach and protocols for estimating and calculating the security are not available since they all assume the presence of D in MM. As a result, a critical D cannot be determined, the standard error correction procedure might not applicable for eliminating Eve's information, the efficiency of the privacy amplification is curtailed, and the unconditional security as proposed in [3] and [4] cannot be considered proved without solving these issues. In a way, Alice's sending of the key is equivalent to sending an unencrypted plain text "secured" by an unreliable indicator of Eve's presence and the protocols cannot be considered for implementation before one proves or disproves that a novel kind of privacy amplification for such deterministic attacks can be designed.

Acknowledgements. Supports of the Croatian Science Foundation through project IP-2014- 09-7515 and of the Ministry of Science, Education, and Sport of Croatia through the CEMS funding are acknowledged.

References

1. Boström, K., T. Felbinger, Deterministic secure direct communication using entanglement, *Phys. Rev. Lett.* **89**, 187902– 1–4 (2002).
2. Lucamarini, M., S. Mancini, Secure deterministic communication without entanglement. *Phys. Rev. Lett.* **94**, 140501–1–4 (2005)
3. Lu, H., C.H.F. Fung, X. Ma, Q. yu Cai, Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. *Phys. Rev. A* **84**, 042344-1-5 (2011).
4. Li, J., L. Li, H. Jin, R. Li, Security analysis of the "PingPong" quantum communication protocol in the presence of collective-rotation noise, *Phys. Lett. A* **377**, 2729–2734 (2013).

Presentation Method (Oral Invited 20 minutes):
Specific Workshop Choice: Quantum Secure Direct Communication