Abstract Submitted
for the MAR07 Meeting of
The American Physical Society

Security aspects of the authentication used in quantum key growing[1] JAN-ÅKE LARSSON, JÖRGEN CEDERLÖF, Linköping University — Unconditionally secure message authentication is an important part of Quantum Cryptography (QC). We analyze security effects of using a key obtained from QC for authentication purposes in later rounds of QC. In particular, the eavesdropper gains partial knowledge on the key in QC that may have an effect on the security of the authentication in the later round. Our initial analysis indicates that this partial knowledge has little effect on the authentication part of the system, in agreement with previous results on the issue. However, when taking the full QC protocol into account, the picture is different. By accessing the quantum channel used in QC, the attacker can change the message to be authenticated. This together with partial knowledge of the key does incur a security weakness of the authentication. The underlying reason for this is that the authentication used, which is insensitive to such message changes when the key is unknown, becomes sensitive when used with a partially known key. We suggest a simple solution to this problem, and stress usage of this or an equivalent extra security measure in QC.

[1]Work is supported financially by the Swedish Science Council.

Jan-Åke Larsson
Linköping University

Date submitted: 17 Nov 2006 Electronic form version 1.4