Title: **On the Computational Security of Quantum Algorithms for Transformation of Information.**

Authors: **Skobelev, V. G.**

Published in: *Cybernetics and Systems Analysis*, **46**:6, 855–868, (2010)

Review by: Mario Forcinito

The security of Quantum Key Distribution (QKD) schemes is founded on the physical properties underlying the exchange of polarized photons and the disturbances on the probability distribution introduced by an eavesdropper reading photons polarization state.

QKD protocols make use of a quantum channel to exchange photons and a classical channel to exchange bits of information about the measurement performed by both parties. The Bennet and Brassard protocol (or a variation thereof) is used to reconcile the bits that both parties have in common without revealing them. Thus both parties of the exchange should end up with identical strings of bits that are to be used as the key. The presence of an eavesdropper on the quantum channel will be detected by the disturbance it introduces and the key thus generated can be discarded as insecure (opening the door for a denial of service attack).

In this work the author explores the case in which the security of the distribution scheme is weakened by allowing an active eavesdropper/attacker to control the probabilities of selection of basic vectors for qubit measurement. This can be understood as an enhanced version of the Man in the Middle attack, as it needs the attacker to actively control both, the quantum and the classical channels. The analysis of the security under these paradigm rest heavily on the quality and security of the random sequence generator.

The author also introduce a cipher based on the dense coding algorithm and provides some analysis of its security. This protocol is proven to have better security than the Bennet and Brassard protocol against the active eavesdropper postulated in this paper. Several lines of future research are also delineated.

See also:

1. Cederlöf, J. *Authentication in quantum key growing, Master Thesis (2005)* available on-line at:
   http://www.lysator.liu.se/∼jc/mthesis/mthesis.pdf

2. Bruen, A. et al. *Error Correcting Codes, Block Designs, Perfect Secrecy and Finite Fields*, Acta Applicandae Mathematica **93** No.1-3, (2006), doi:
   http://dx.doi.org/10.1007/s10440-006-9043-4