Abstract Submitted
for the MAR11 Meeting of
The American Physical Society

Security Proof for QKD Using Qudits and Finite Key Length Analysis of Protocols LANA SHERIDAN, THINH LE, Centre for Quantum Technologies, National University of Singapore, VALERIO SCARANI, Department of Physics and Centre for Quantum Technologies, National University of Singapore — It is advantageous to use d-dimensional quantum systems for QKD because each signal carries $\log d > 1$ bits, allowing a larger amount of information to be sent per transmission through the channel, and moreover, studies have indicated that the resistance to noise of the protocols increases when the dimension is increased. We provide a security bound against coherent attacks that takes into account finite-key effects for two families of protocols: two-basis protocols, the natural generalization of the Bennett-Brassard 1984 protocol for qubits, and $(d + 1)$-basis protocols, the generalization of the six-state protocol for qubits. In the asymptotic limit, our bound vindicates the previous partial results concerning the higher resistance to noise. We also show that for finite key lengths the key rate corrections vary little with d for $2 \leq d \leq 20$ indicating the protocol can be effective in realistic conditions. Finally, we consider some other finite key techniques for more general protocols.

Lana Sheridan
National University of Singapore

Date submitted: 19 Nov 2010 Electronic form version 1.4