

Exploiting Entanglement in Quantum Cryptographic Probes

Howard E. Brandt

U.S. Army Research Laboratory, Adelphi, MD

The mathematical physical bases are given for quantum cryptographic probes which exploit entanglement to eavesdrop on quantum key distribution. The quantum circuits and designs are presented for two different optimized entangling probes for attacking the BB84 Protocol of quantum key distribution (QKD) and yielding maximum information to the probes [1-4]. The designs are based on two different optimum unitary transformations. Probe photon polarization states become optimally entangled with the signal states on their way between the legitimate transmitter and receiver. Standard von-Neumann projective measurements of the probe yield maximum information on the pre-privacy amplified key once basis information becomes available during reconciliation.

[1] H. E. Brandt, Phys. Rev. A **71**, 042312 (2005).

[2] H. E. Brandt, "Design for a quantum cryptographic entangling probe," to appear in J. Mod. Optics (2005).

[3] H. E. Brandt, Phys. Rev. A, Phys. Rev. A **66**, 032303 (2002).

[4] H. E. Brandt, Quantum Information Processing **2** 37 (2003).

Exploiting Entanglement in Quantum Cryptographic Probes

Howard E. Brandt

U.S. Army Research Laboratory, Adelphi, MD

The mathematical physical bases are given for quantum cryptographic probes which exploit entanglement to eavesdrop on quantum key distribution. The quantum circuits and designs are presented for two different optimized entangling probes for attacking the BB84 Protocol of quantum key distribution (QKD) and yielding maximum information to the probes [1-4]. The designs are based on two different optimum unitary transformations. Probe photon polarization states become optimally entangled with the signal states on their way between the legitimate transmitter and receiver. Standard von-Neumann projective measurements of the probe yield maximum information on the pre-privacy amplified key once basis information becomes available during reconciliation.

[1] H. E. Brandt, Phys. Rev. A **71**, 042312 (2005).

[2] H. E. Brandt, "Design for a quantum cryptographic entangling probe," to appear in J. Mod. Optics (2005).

[3] H. E. Brandt, Phys. Rev. A, Phys. Rev. A **66**, 032303 (2002).

[4] H. E. Brandt, Quantum Information Processing **2** 37 (2003).