Relativistic Quantum Cryptography

Evan Jeffrey, Joseph Altepeter, and Paul G. Kwiat
Department of Physics, University of Illinois at Urbana-Champaign, 1110 W Green St., Urbana IL 61801
Tel: (217) 333-9116; FAX: (217) 244-7559; e-mail: kwiat@uiuc.edu

Abstract: Using entangled photons and a low-loss optical delay, we implement a novel quantum cryptography protocol in which every photon contributes to the key, yielding enhanced efficiency, and an advantage for six- versus four-basis state protocols.

OCIS codes: (060.4510) Optical communications; (030.5260) Photon counting; (270.0270) Quantum optics

In the traditional quantum key distribution (QKD) protocols, Bob chooses at *random* how to measure any given photon sent to him by Alice. This is necessary so that a potential eavesdropper cannot predict how it will be measured; however, it has the unfortunate consequence that the maximum efficiency is only 50%. This intrinsic loss is even worse for the 6-state protocol, where Alice and Bob use the same basis only 1/3 of the time (this protocol is otherwise superior because the eavesdropper induces higher error rates, which are more easily detectable [1]). However, we can eliminate this inefficiency by having Bob store his photon until Alice announces the correct basis, allowing him to measure his photon correctly 100% of the time, while preventing Eve from having that information in time to use it maliciously [2]. Because every photon can then in principle contribute to the final key, the effective data rate of the standard BB84 protocol is increased considerably, and makes six-state protocols practical alternatives. The protocol is secure as long as the backward light cone of the event when Bob receives the photon and the forward light cone of when Alice sends the classical message do not overlap (see Fig. 1), so that a potential eavesdropper cannot have access to both the quantum transmission and the classical signal at the same time.

We have implemented this protocol using a source of polarization-entangled photons [3], in addition to several unique technological elements: low-loss storage cavity, fast classical signaler, fast active analysis system. Bob accomplishes the storage by means of a specially constructed optical delay line – a pair of mirrors arranged so that his photon makes many round trips between them before emerging and entering the detector. We have constructed a very low latency classical optical modulation system, by which Alice sends the basis information to Bob (in less than 200 ns). The basis choice at the receiver is implemented using a fast Pockel cell; a novel arrangement enables a single device to select all three mutually unbiased bases.

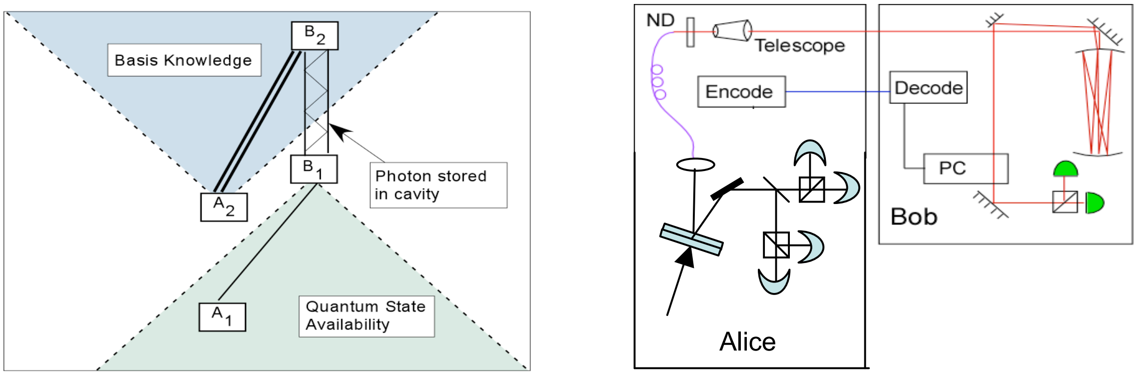

Fig. 1. left: Space-time diagram indicating the light-cone requirements for secure "relativistic" QKD; right: Experimental setup to realize protocol, using polarization-entangled photons.

We have successfully transferred quantum keys using this system in both a 4-state and a 6-state configuration. Typical bit error rates are less than 2%. We observe yield enhancements of up to 1.2 (for the 4-state protocol), and 1.9 (for the 6-state protocol); further enhancements up to the theoretical limits of 2-3 may be realized with improved mirrors in the storage system.

References

[1] E. Jeffrey, M. Brenner, and P. Kwiat, "Delayed-choice quantum cryptography", Proc. SPIE 5161, (2004).

[2] D. G. Enzer, R. J. Hughes, C. G. Peterson, and P. G. Kwiat, "Entangled-photon Six-state Quantum Cryptography", in *Focus Issue on Quantum Cryptography* in New J. Phys. **4**, 45 (2002).

[3] P. G. Kwiat, et al. "Ultrabright Source of Polarization-Entangled Photons", Phys. Rev. A **60**, R773 (1999).