LA-UR- 99-266

Approved for public release;
distribution is unlimited.

CONF-990802--

Title: PRACTICAL POINT-TO-POINT FREE-SPACE QUANTUM
KEY DISTRIBUTION OVER 1/2 KM

Author(s): William T. Buttler, Richard J. Hughes, Paul G. Kwiat,
Steve K. Lamoreaux, George L. Morgan, Charles G. Peterson
(P-23)

Jane E. Nordholt (NIS-1)

RECEIVED

MAR 12 1999

Submitted to: INTERNATIONAL COMMISSION FOR OPTICS **OSTI**
CONFERENCE: ICO XVIII, 2-6 AUGUST 1999,
SAN FRANCISCO, CALIFORNIA

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Los Alamos
NATIONAL LABORATORY

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the University of California for the U.S. Department of Energy under contract W-7405-ENG-36. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Form 836 (10/96)

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Practical point-to-point free-space quantum key distribution over 1/2 km

W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux,
G. L. Morgan, J. E. Nordholt, and C. G. Peterson

Los Alamos National Laboratory, MS H803

Los Alamos, NM 87545, USA

Email: buttler@lanl.gov, hughes@lanl.gov

Abstract. We have demonstrated point-to-point single-photon quantum key distribution (QKD) over a free-space optical path of ~ 475 m under daylight conditions. This represents an increase of $>1,000$ times farther than any reported point-to-point demonstration [1], and >6 times farther than the previous folded path daylight demonstration [2]. We expect to extend the daylight range to 2 km or more within the next few months. A brief description of the system is given here.

The QKD transmitter, a.k.a. “Alice” (Fig. 1), consists of three thermoelectrically cooled diode lasers, a single interference filter (IF), two optical attenuators, two linear polarizers, two non-polarization beam-splitters (BSs), and a $27\times$ beam expander. The two data-lasers’ (dim-lasers’) wavelengths are temperature controlled and constrained by the IF to $\sim 773 \pm 0.5$ nm, while the transmitted wavelength of the bright-laser (timing-laser) is ~ 768 nm; the data-lasers are configured to emit a weak pulse of approximately 1 ns duration. The transmitter incorporates no active polarization switching — a first in QKD.

The QKD receiver, a.k.a. “Bob” (Fig. 2), comprises a 8.9 cm Cassegrain telescope followed by polarization analyzing optics, two multi-mode (MM) fiber-coupled single-photon counting modules (SPCMs), and a “warm” detector which uses the bright timing pulse to set a coincidence trigger to “look for” dim-pulse firings of the SPCMs. The analyzing optics comprise a 50/50 BS to randomly direct collected photons onto one of two distinct optical paths. The lower optical path contains a polarization controller (a quarter-wave retarder and a half-wave retarder) followed by a PBS and an IF, and the upper optical path contains a polarization controller followed by a linear polarizer and an IF. Each analysis path couples to a SPCM, and the portion of the bright-pulse split along the lower path is polarized to be mostly directed by the PBS along a third optical path containing the “warm” detector. The receiver incorporates no active polarization switching.

Alice starts the QKD protocol by generating a secret random binary number sequence. She then pulses the bright timing-laser at a rate, R , compatible with Bob’s electronics ($R \leq 1$ MHz) while randomly pulsing one of the data-lasers based on her random bits values [the random key-bits are encoded as either a right 45° polarized dim-pulse ($|45\rangle$, taken here as 1), or a vertical polarized dim-pulse ($|v\rangle$, taken here as 0), which is attenuated to an average photon number per dim-pulse of $\bar{n} < 1$ at transmission]. Bob collects

FIG. 1. Free-Space QKD Transmitter (Alice).

FIG. 2. Free-Space QKD Receiver (Bob).

the bright- and dim-pulses and randomly tests the latter for superposed single-photon states. The firing of the warm detector tells Bob when to expect the dim-pulse allowing him to watch for one of his SPCMs to fire within the temporally narrow coincidence window (<5 ns). (Alice transmits the dim-pulses before the timing-pulse to minimize noise caused by reflections within the system. Bob detects the bright-pulse before the dim-pulse by using MM fibers of differing lengths.)

If Bob's upper path polarizer (Fig. 2) is oriented to transmit horizontally polarized photons, $|h\rangle$, and if Alice sends a single $|v\rangle$ photon and Bob collects it and it travels along the upper path, then the upper path polarization controller can be adjusted to convert $|v\rangle$ to $|-45\rangle$ leading to a 50% detection probability at the upper path SPCM; however, a single $|45\rangle$ polarized photon traveling this path is converted to $|v\rangle$ and absorbed by the polarizer in this path. Similarly, if Alice sends a single $|45\rangle$ photon and it travels along the lower path, the polarization controller can be adjusted so that it leaves the $|45\rangle$ unchanged (zero wave retardation), leading to a 50% detection probability at the lower path SPCM; similarly, a single $|v\rangle$ polarized photon traveling this path is unchanged and reflected away from the SPCM in this path by the PBS. Thus, Bob determines a random 25% portion of the random states (key-bits) transmitted by Alice by testing for superposed single-photon states. This 25% efficiency is the price Alice and Bob must pay for secrecy in the B92 protocol [3]. (The preceding discussion assumes single-photon Fock states on transmission, and perfect receiver optics and single-photon detect-ability.) We tested out our QKD system down to an average dim-pulse photon number of $\bar{n} \sim 0.3$ during daytime operation ($\sim 16:30$ on 19 November 1998). [Note (1): the attenuated pulse only approximates a "single-photon" Fock state. Dim-pulses of $\bar{n} \sim 0.3$ will have a 2-photon probability of $\sim 4.0\%$, implying that ~ 18 of every 100 detectable pulses will contain more than one photon. Note (2): we measured $\bar{n}$ at the transmitter after calculating $\bar{n}$ at the receiver with data collected during nighttime experiments (not discussed here). Based on similar reasonable assumptions, we calculated $\bar{n}$ with data collected during the daytime experiments.]

Bit exchange is completed when Bob openly communicates the locations, but not the values, of his photon detections in Alice's random bit string. The non-orthogonal basis states ensure eavesdropping will be detected by the elevated error rate caused by the irreversible collapse of the wave-function [4]. A complete QKD system will incorporate signature authentication and privacy amplification [5] protocols.

The daytime optical coupling efficiency between the transmitter and receiver was $\eta \sim 0.15$ and accounts for losses between the transmitter and MM fibers at the receiver. The 0.25 efficiency of B92 (η_Q) and the detectors' efficiencies ($\eta_D \sim 0.6$) lower the overall system efficiency to ~ 0.022 , and leads to a detection probability for Bob of $P_B = 1 - \exp(-\eta \times \eta_Q \times \eta_D \times \bar{n})$. The key-rate was ~ 7 kHz at $\bar{n} \sim 0.3$ photon per dim-pulse when the lasers were pulsed at $R = 1$ MHz. The average bit error rate was $\sim 1.5\%$.

We have demonstrated practical point-to-point free-space QKD over ~ 475 m through a turbulent medium under daylight conditions, and have described a passive QKD transmitter and receiver that provides a secure method to secretly communicate with a simple system based on the B92 protocol. A more detailed discussion of the methods, reconciliation and error detection protocols, B92 protocol weaknesses, and important physics related to quantum cryptography and surface-to-satellite QKD can be found in [6].

- [1] C. H. Bennett *et al.*, *Lect. Notes in Comput. Sci.*, **473**, 253-265 (1990).
- [2] B. C. Jacobs and J. D. Franson, *Opt. Lett.* **21**, 1854-1856 (1996).
- [3] C. H. Bennett *Phys. Rev. Lett.* **68**, 3121-3124 (1992).
- [4] A. K. Ekert *et al.*, *Phys. Rev. A*, **50**, 1047-1056 (1994).
- [5] C. H. Bennett *et al.*, *IEEE Trans. Inf. Theory* **41**, 1915-1923 (1995).
- [6] W. T. Buttler *et al.*, *Phys. Rev. Lett.* **81**, 3283-3286 (1998).