Secure communication

Quantum cryptography with a photon turnstile

Quantum cryptography generates unbreakable cryptographic codes by encoding information using single photons, which until now have relied on highly attenuated lasers as sources[1,2]. But these sources can create pulses that contain more than one photon, making them vulnerable to eavesdropping by photon splitting[3,4]. Here we present an experimental demonstration of quantum cryptography that uses a photon turnstile device, which is more reliable for delivering photons one at a time. This device allows completely secure communication in circumstances under which this would be impossible with an attenuated laser.

Our quantum-cryptography system (see supplementary information for full technical details) implements a protocol known as BB84 (ref. 5). The photon turnstile is a single quantum dot in a micropost cavity[6,7], which is optically excited by a pulsed laser. The security improvements attainable with this device can be quantified by two measurements: the probability that the device will inject a photon into the quantum channel, measured as 0.007 by comparing the count rate at detector 0 (see supplementary information) to the repetition rate of the excitation laser (76 MHz); and the second-order correlation, denoted by $g^{(2)}$ (see supplementary information).

This quantity gives the amount of suppression of multiphoton states from our device relative to attenuated laser light — a laser with perfect intensity stability is characterized by $g^{(2)} = 1$, whereas our turnstile device has $g^{(2)} = 0.14$. The probability that our device will emit a multiphoton state is therefore an order of magnitude smaller than a laser that emits photons at the same rate, meaning that security is improved in the presence of channel losses[8].

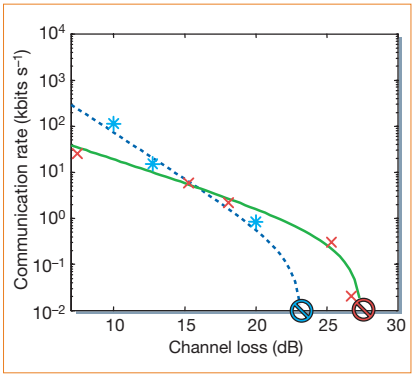

Figure 1 Comparison of the turnstile device with a standard laser. Measured (crosses, turnstile device; stars, laser) and simulated (full line, turnstile device; dashed line, laser) bit rates are shown as a function of total loss from the channel and detection system. Circles: blue, the attenuation at which our system was experimentally shown to reject the entire key using an attenuated laser (23 decibels); red, point at which our system rejected the entire key for the turnstile device (28 decibels). This shows a 5-decibel improvement in the loss cut-off.

In our implementation of BB84, the sender of the message, Alice, encodes information by preparing the polarization of each photon in either the horizontal or right circular polarization for binary 0, and vertical or left circular for binary 1. This is done by an electro-optic modulator. The modulator is driven by a data generator that produces the secret key, giving a random four-level signal that corresponds to the four different polarization states in the BB84 protocol. The state of the data generator is recorded by a time-interval analyser and is stored by a computer.

After the polarization is prepared, the photon is sent into the quantum channel, a 1-metre free-space propagation, and is detected by the receiving party, Bob. Bob measures the photons by using passive polarization optics and avalanche photodiodes with dark counts of about 80 s^{-1} (see supplementary information). The detection probability, due to losses in the optics and photodiodes, is 0.24. Detection events are recorded by a second time-interval analyser and are stored by a second computer for subsequent comparison with Alice.

The error rate of the system is measured as 2.5%. These errors are corrected by using an error-correction algorithm[9]. After error correction, privacy amplification is carried out to create the final key, yielding a communication rate of 25 kbits s^{-1}.

To demonstrate the advantage of our source over standard laser light, we use both the turnstile device and an attenuated laser to carry out quantum cryptography. A variable attenuator is inserted into the quantum channel to simulate channel losses. Figure 1 shows the theoretical and experimentally measured communication rates for our turnstile device and for laser light, as a function of channel loss. When losses are low, the communication rate of the attenuated laser is greater because our turnstile device is limited by its efficiency and by losses in the collection optics. At greater channel losses, however, the laser emits too many multiphoton states, causing a more rapid reduction in communication rate. At around 16 decibels, the turnstile begins to outperform the laser. Above 23 dB of loss, secure communication is no longer possible with the laser — however, our source is able to withstand channel losses of about 28 dB. This demonstrates the security advantage of our photon turnstile in the presence of channel losses.

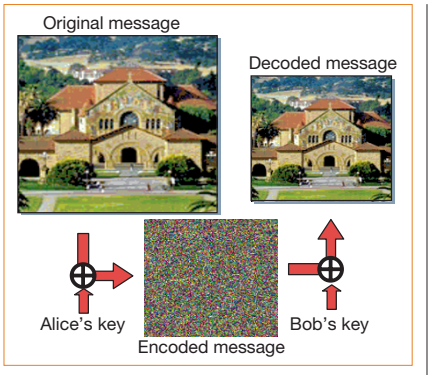

Figure 2 Demonstration of the final stage of the cryptographic protocol. The message, a 140 × 141,256-pixel colour bitmap of Stanford University's Memorial Church, is encoded by a secure quantum key exchanged through our system from Alice to Bob, using standard one-time pad techniques. The encoded image appears as white noise to a third party that does not possess a copy of the key. Using the exchanged key, however, Bob decodes the message, recovering the pixel image with no error. Further details are available from the authors.

In the final phase of communication, the secret key is used as a one-time pad to exchange the message (here a picture of Stanford University's Memorial Church; Fig. 2). The cryptography system is used to exchange a 20-kilobyte key. Alice uses her copy of the key to do a bitwise exclusive OR logic operation with each bit of the message. The resulting encrypted message looks like white noise to anyone without a copy of the key, but Bob decodes it by carrying out a second bitwise exclusive OR operation using his copy of the key.

A similar experiment using diamond colour centres has recently been reported[10].

Edo Waks*, Kyo Inoue†, Charles Santori*, David Fattal*, Jelena Vuckovic*, Glenn S. Solomon‡, Yoshihisa Yamamoto*†

**Quantum Entanglement Project, ICORP, JST, MURI, UCLA, E. L. Ginzton Labs, and ‡Solid State Photonics Laboratory, Stanford University, Stanford, California 94305, USA*
e-mail: edo@stanford.edu
†NTT Basic Research Laboratories, Atsugi, Kanagawa 243-0198, Japan

1. Buttler, W. T. *et al. Phys. Rev. Lett.* **24,** 5652–5655 (2000).
2. Marand, C. & Townsend, P. D. *Optics Lett.* **20,** 1695–1697 (1995).
3. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. *Phys. Rev. Lett.* **85,** 1330–1333 (2000).
4. Lütkenhaus, N. *Phys. Rev. A* **61,** 052304 (2000).
5. Bennett, C. H. & Brassard, G. *Proc. IEEE Int. Conf. Comp. Syst. Sig. Process., Bangalore, India* 175–179 (IEEE, New York, 1984).
6. Santori, C., Pelton, M., Solomon, G., Dale, Y. & Yamamoto, Y. *Phys. Rev. Lett.* **86,** 1502–1505 (2001).
7. Santori, C., Fattal, D., Vuckovic, J., Solomon, G. S. & Yamamoto, Y. *Nature* **419,** 594–597 (2002).
8. Waks, E., Santori, C. & Yamamoto, Y. *Phys. Rev. A* **66,** 042315 (2002).
9. Brassard, G. & Salvail, L. *Advances in Cryptology: Eurocrypt '93, Lecture Notes in Computer Science* Vol. 765 (ed. Hellseth, T.) 410–423 (Springer, Berlin, 1994).
10. Beveratos, A. *et al. Phys. Rev. Lett.* **89,** 187904 (2002).

Supplementary information accompanies this communication on *Nature*'s website.
Competing financial interests: declared none.