Experimental Demonstration of Secure Communication based on Quantum Illumination

Zheshen Zhang, Maria Tengner, Tian Zhong, Franco N. C. Wong, and Jeffrey H. Shapiro

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Abstract: We report the first experimental demonstration of an entanglement-based secure communication protocol that is resilient to entanglement-breaking loss and noise on the communication channel. Passive eavesdropping immunity is demonstrated in bit-error rate measurements and Alice's information advantage over Eve is estimated.

Entanglement is a key ingredient to many quantum information applications, but quantum decoherence arising from loss and noise easily destroys entanglement. Quantum illumination (QI) [1]–[3] is a novel concept of utilizing entanglement in an entanglement-breaking lossy and noisy environment to achieve a substantial performance benefit. First proposed for enhancing the signal-to-noise ratio for detecting a weakly-reflecting target in the presence of strong background noise [1], quantum illumination was later shown, theoretically, to enable high data-rate classical communication that is immune to passive eavesdropping [3]. In this work we report the first experimental demonstration of the QI communication protocol [4], showing a strong performance benefit of using bosonic entanglement over an entanglement-breaking channel and QI's passive-eavesdropping immunity. Quantum illumination achieves a substantial benefit from its initial entanglement, despite the roundtrip lossy, noisy propagation channel's having left the retained and returned light in a separable classical state. This work also suggests that the use of entanglement should *not* be dismissed for environments in which it will be destroyed.

The basic QI communication protocol is shown in Fig. 1. Alice prepares a pair of maximally-entangled signal and idler light beams from a spontaneous parametric downconverter (SPDC), sending the signal to Bob and retaining the idler. Bob encodes his message bits with a phase modulator by applying 0 (message bit = 0) or π rad (message bit = 1) phase shifts on the signal he receives from Alice. Bob then intentionally breaks the signal-idler entanglement by passing his modulated signal light through an erbium-doped fiber amplifier (EDFA), whose amplified spontaneous emission (ASE) noise masks his bit stream from Eve. Eve is implemented by allowing her to tap 50% of the signal light that Alice sends to Bob and 10% of the modulated return signal light that Bob sends to Alice. Eve must rely on the joint classical-state light she has tapped from the Alice-to-Bob and Bob-to-Alice channels, while Alice combines her noisy returned light with her retained idler in a joint quantum measurement to decode Bob's bit stream. QI makes Alice's cross-correlation signature between her retained and returned light beams far stronger than Eve's corresponding signature for her two tapped beams, even though Alice and Eve's receivers only have classical states at their disposal. In our experiment the QI communication protocol allows Alice and Bob to enjoy a five-order-of-magnitude advantage in bit-error rate (BER) over Eve despite channel noise that is more than 8 dB beyond the threshold for entanglement breaking. This entanglement-based scheme allows for direct secure communication between two parties despite no entanglement surviving at the receiver end.

In the experimental implementation we operate at a data rate of 500 kbit/s. The SPDC generates signal and idler beams that are entangled over a large number ($\sim 4 \times 10^6$) of temporal modes per bit duration of $2\,\mu$s, and the average number of photon pairs per mode N_S is much smaller than unity. In comparison the EDFA operating at a gain of over 40 dB adds more than 10^4 noise

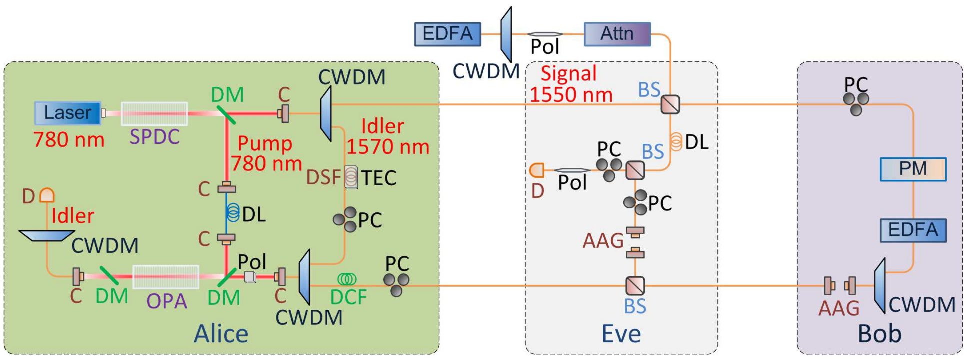

Figure 1: Experimental setup. SPDC: spontaneous parametric downconverter; DM: dichroic mirror; C: collimator; CWDM: coarse wavelength-division multiplexer; BS: beam splitter; Attn: attenuator; EDFA: erbium-doped fiber amplifier; DL: delay line; PC: polarization controller; PM: phase modulator; AAG: adjustable air gap; Pol: polarizer; DCF: dispersion-compensating fiber; DSF: dispersion-shifted fiber; TEC: thermoelectric cooler; OPA: optical parametric amplifier; D: detector.

photons per mode to the modulated signal that Bob sends to Alice. Alice's receiver is a low-gain optical parametric amplifier (OPA) that converts phase-sensitive cross correlation into amplitude modulation that is then measured by direct detection using an InGaAs avalanche photodiode on the OPA's idler-port output. Eve's eavesdropping—passive eavesdropping, because she does not inject any light into Bob's terminal—relies on the interference between the light she tapped from the Alice-to-Bob and Bob-to-Alice channels. She measures this interference by direct detection of an unequal mixture of those two beams that she has optimized for minimum BER by choosing an optimum coupling efficiency of her adjustable air gap to suppress the ASE noise from the EDFA.

Fig. 2 (left) displays Alice and Eve's BERs versus N_S (signal-photons/mode at Alice's SPDC output). The blue and red curves are theory for BER_A. Blue curves assume a maximally-entangled SPDC source and an OPA receiver with gain $G_A - 1 = 1.86 \times 10^{-5}$. The dashed one is for an ideal receiver—no dispersion-induced loss of modulation depth, no detector technical noise, and a perfect matched filter—and the solid one employs the experimentally-determined values for her receiver's nonidealities. The red curve assumes a maximally-correlated classical-state source and ideal OPA reception. The gap between the dashed red and the solid blue curves shows that Alice's performance using an SPDC source and imperfect OPA reception exceeds what can be achieved with a classical-state source and ideal OPA reception. The green curves are theory for BER_E with an ideal receiver (dashed) or accounting for nonidealities (solid).

The blue circles in Fig. 2 (left) are BER_A versus N_S measurements under the operating conditions for the solid blue curve; they show excellent agreement with theory. The blue diamond is the measured BER_A at $N_S = 7.81 \times 10^{-4}$ with $G_A - 1 = 2.48 \times 10^{-5}$; the green triangle above it is the corresponding BER_E. These filled points are our secure-communication operating point: $\text{BER}_A = 1.78 \times 10^{-6}$ and $\text{BER}_E \approx 0.5$. The joint state of Alice's returned and retained beams is classical when the per-mode ASE noise photon number $N_B \geq N_B^{\text{thresh}}$. For our experiment, $N_B^{\text{thresh}} = 2.14 \times 10^3$, so our measured $N_B = 1.46 \times 10^4$ is 8.3 dB above that threshold.

The other green triangles in Fig. 2 are BER_E points obtained using attenuated ASE from an EDFA to mimic the statistics of Alice's signal beam at brightness values unattainable from her source with our available pump power. The N_S gap between the blue circles and the green triangles in Fig. 2 at the same BER values quantifies Alice and Bob's entanglement-derived communication advantage when Alice and Eve both use realistic receivers.

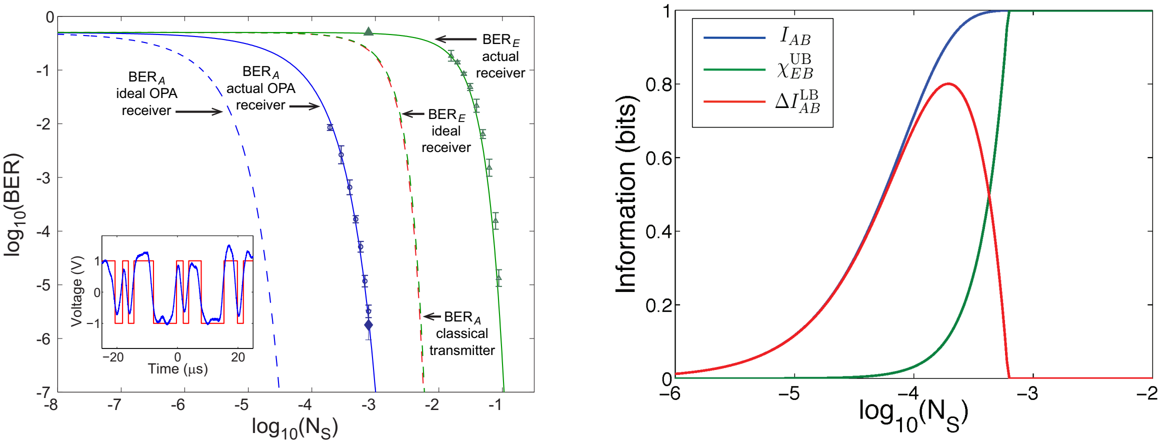

Figure 2: (left) BER_A and BER_E vs. N_S for 500 kbit/s communication. Blue and red curves are theory for BER_A for an OPA receiver with gain $G_A - 1 = 1.86 \times 10^{-5}$. Circles are Alice's measured BERs, and the diamond is her measured BER with $G_A - 1 = 2.48 \times 10^{-5}$. Triangles are Eve's measured BERs; the lowest N_S point (filled triangle) was obtained using Alice's SPDC source, and the remaining triangles employed attenuated ASE from an EDFA source. See text for more details. (right) Alice's information advantage over Eve.

A more convincing evaluation of the immunity to passive eavesdropping is illustrated in Fig. 2 (right), where Alice's Shannon information I_{AB}, Eve's Holevo information upper bound χ_{EB}^{UB}, and Alice's information advantage lower bound $\Delta I_{AB}^{\mathrm{LB}} \equiv I_{AB} - \chi_{EB}^{\mathrm{UB}}$ are displayed as a function of the source brightness. With Alice using her imperfect OPA receiver she can get up to 0.8 bits of information advantage, per Bob's transmitted bit, over Eve's optimum collective quantum measurement.

In summary, we have implemented a secure-communication protocol based on quantum illumination. The passive-eavesdropping immunity stems from harnessing entanglement and performing a joint quantum measurement on the retained and returned light, even though the initial entanglement is broken at the receiver. We conclude that quantum illumination allows utilizing entanglement beneficially in lossy and noisy situations.

This work was supported by a Basic Research Challenge grant from the U.S. Office of Naval Research.

References

[1] S. Lloyd, Science **321,** 1463 (2008); S.-H. Tan, *et al.*, Phys. Rev. Lett. **101,** 253601 (2008).

[2] S. Guha and B. I. Erkmen, Phys. Rev. A **80,** 052310 (2009).

[3] J. H. Shapiro, Phys. Rev. A **80,** 022320 (2009).

[4] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. Lett., accepted for publication.