Entanglement's Benefit Survives an Entanglement-Breaking Channel

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

Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA

(Received 21 March 2013; published 1 July 2013)

Entanglement is essential to many quantum information applications, but it is easily destroyed by quantum decoherence arising from interaction with the environment. We report the first experimental demonstration of an entanglement-based protocol that is resilient to loss and noise which destroy entanglement. Specifically, despite channel noise 8.3 dB beyond the threshold for entanglement breaking, eavesdropping-immune communication is achieved between Alice and Bob when an entangled source is used, but no such immunity is obtainable when their source is classical. The results prove that entanglement can be utilized beneficially in lossy and noisy situations, i.e., in practical scenarios.

DOI: 10.1103/PhysRevLett.111.010501 PACS numbers: 03.67.Hk, 42.50.Dv, 42.50.Ex

Entanglement is essential to many quantum information applications [1–11], but easily destroyed. Quantum illumination (QI) [12–15] is a radically different entanglement-based paradigm: it thrives on entanglement-breaking loss and noise. For a given transmitter power, an initially entangled state's nonclassical correlation produces a classical state at the output of an entanglement-breaking channel whose correlation can greatly exceed what any classical input of the same power can yield through that channel.

First proposed to increase the signal-to-noise ratio for detecting a weakly reflecting target in a noisy environment [12–14], quantum illumination was later shown, theoretically, to enable classical communication that is immune to passive eavesdropping [15]. In this Letter, we report the first experimental demonstration of QI's passive-eavesdropping immunity. Our experiment also represents the first time that bosonic entanglement has yielded a strong performance benefit over an entanglement-breaking channel. Thus, it implies that the use of entanglement should *not* be dismissed for environments in which it will be destroyed. Unlike the recent experiment [16] reporting the target-detection advantage of photon-pair correlations, our eavesdropping-immune QI protocol *requires* an initial state that is entangled.

Our experiment is shown in Fig. 1. Alice prepares maximally entangled signal and idler beams using a spontaneous parametric down-converter (SPDC), sending the signal to Bob and retaining the idler. Bob encodes his message bits at 500 kbit/s by applying 0 (message bit = 0) or π rad (message bit = 1) phase shifts on the signal he receives from Alice. Bob 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 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 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.

In Fig. 1, Alice's SPDC uses a 20 mm type-0 phase-matched MgO-doped periodically poled lithium niobate (MgO:PPLN) crystal that is continuous-wave (cw) pumped at 780 nm, producing signal and idler outputs at 1550 and 1570 nm. A coarse wavelength division multiplexer (CWDM) separates the signal and idler and band limits them to 16 nm ($W \approx 2$ THz). The $T = 2$ μs bit duration at 500 kbit/s then contains $M = TW \approx 4 \times 10^6$ signal-idler mode pairs per information bit. At ~135 mW pump power, the SPDC generates a source brightness of $N_S = 0.001$ signal (and idler) photons per mode on average. Having $N_S \ll 1$ and $MN_S \gg 1$ are essential for QI. The former ensures that Alice gets a much stronger correlation signature than Eve does, and the latter guarantees that Alice receives sufficient photons/bit to achieve a low error probability.

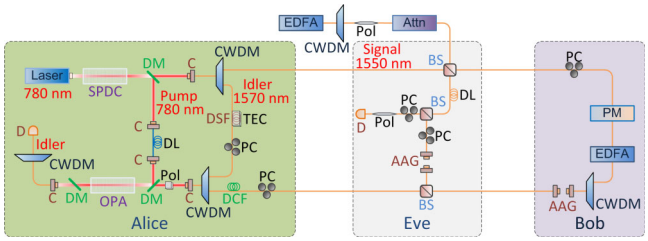

FIG. 1 (color online). Experimental setup. SPDC: spontaneous parametric down-converter; DM: dichroic mirror; C: collimator; CWDM: coarse wavelength-division multiplexer; BS: beam splitter; Attn: attenuator; EDFA: erbium-doped fiber amplifier; DL: delay line; PC: polarization controller; PM: phase modulator;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

Alice retains the idler in a spool of dispersion-shifted fiber, whose propagation delay matches the Alice-to-Bob-to-Alice delay seen by the signal beam. She sends her signal beam to Bob through a single-mode fiber (SMF) into which Eve has placed a 50-50 beam splitter. Bob applies binary phase-shift keying (BPSK) modulation to the signal light he has received using a phase modulator driven by a pseudorandom bit sequence from a bit-error rate (BER) tester. The modulated light is fed to an EDFA set to a measured gain $G_B \approx 1.34 \times 10^4$ whose ASE noise has per-mode average photon number $N_B \approx 1.46 \times 10^4$. A CWDM filter is used to band limit the ASE to the 16 nm occupied by the signal and to attenuate the ASE within the idler spectral band by ~30 dB. Complete suppression of the ASE noise outside of the signal band is achieved with a second CWDM in Alice's receiver (and with additional attenuation in Eve's receiver).

Our QI protocol is intrinsically interferometric, so Bob uses a free-space delay line with ~80% efficiency to fine tune the timing between the signal and the idler paths. Dispersion in the SMFs connecting Alice and Bob broadens the SPDC's ~0.22 ps biphoton wave function to ~27 ps. Thus, Alice injects the light returned from Bob into ~10 m of dispersion-compensating fiber before combining it with her retained idler through a CWDM. The signal path sustains a measured channel loss of ~16.4 dB that includes SMF coupling loss, fiber-optic component insertion loss, and Eve's 50% (10%) tap placed before (after) Bob's apparatus. (Eve's 50% Alice-to-Bob tap minimizes her BER when her receiver is ASE limited. Her tapping more than 10% of Bob-to-Alice light does not improve her BER, because she is ASE limited with the 10% tap.) Alice's idler suffers ~4.1 dB channel loss from SMF coupling and component insertion loss.

Alice decodes Bob's message bits by applying the returned and retained light to the signal and idler ports of a low-gain optical parametric amplifier (OPA), and then doing direct detection on the OPA's idler-port output followed by matched filtering of the output current and threshold-decision logic. The returned and retained light are free-space coupled with the cw pump beam through a dichroic mirror to an OPA based on a 20 mm MgO:PPLN crystal. The OPA converts the cross correlation between the phase-modulated signal and the retained idler into amplitude modulation in the output idler that can be sensed with direct detection. After the OPA, a dichroic mirror is used to remove the pump, and the OPA's signal and idler outputs are coupled into an SMF and separated by a CWDM filter. The separated idler is coupled into free space and detected by an avalanche photodiode (APD) setup that is 45% efficient, when coupling and CWDM loss are combined with detector quantum efficiency.

The APD's output current passes through a low-noise current amplifier, whose output is sent to a high-pass filter, to reject dc, followed by a low-pass filter. The sampled output from the second filter is supplied to a field programmable gate array (FPGA) that yields two outputs. The FPGA program to produce the first output approximates the matched filter for a single bit, and it is subsequently dc shifted and amplified to transistor-transistor logic levels for BER measurements. The second output provides a feedback signal to a lock-in amplifier that is part of a servo-control system which stabilizes the relative phases between the OPA pump, Alice's retained idler, and the modulated light she receives from Bob. The servo-control system also includes a slow thermal-control loop for Alice's fiber spool. Typical incident power at the APD is approximately 10 nW. It is dominated by the signal-band ASE noise converted to the idler band by the OPA. The OPA gain G_A is kept low, $G_A - 1 \ll 1$, to prevent the ASE noise from overwhelming the amplitude modulation in the OPA's idler output. We implement Eve to demonstrate Alice's entangled-input QI performance advantage over what Eve achieves with her classical-state input. Eve decodes Bob's message by combining the light she has tapped from Alice and Bob's transmissions on an asymmetric beam splitter, and then doing direct detection followed by matched filtering of the output current and threshold-decision logic.

Neither Alice nor Eve's receivers are quantum optimal, but both represent their best receivers for which explicit realizations are known. With these receivers, Alice and Eve's BERs are given by (see Supplemental Material [17] for details)

$$\mathrm{BER}_A = Q\left(\frac{\sqrt{M}\zeta_A\sqrt{N_S(N_S+1)}}{\sigma^{\mathrm{tot}}_{A_+} + \sigma^{\mathrm{tot}}_{A_-}}\right), \tag{1}$$

$$\mathrm{BER}_E = Q\left(\frac{\sqrt{M}\zeta_E N_S}{\sigma^{\mathrm{tot}}_{E_+} + \sigma^{\mathrm{tot}}_{E_-}}\right). \tag{2}$$

Here: Q is the tail integral of the standard Gaussian probability density; $\zeta_A\sqrt{N_S(N_S+1)}$ ($\zeta_E N_S$) is the modulation-depth signature of Bob's message bit seen by Alice (Eve), where ζ_A (ζ_E) is a transmission efficiency; and $\sigma^{\mathrm{tot}}_{A_\pm}$ ($\sigma^{\mathrm{tot}}_{E_\pm}$) are Alice's (Eve's) per-mode noise standard deviations for bit values 0 and 1. The transmission efficiencies include (see Supplemental Material [17]) the EDFA gain, channel loss, and an effective modulation-depth factor due to residual dispersion and less than optimal mode-pair coupling into an SMF.

The points in Fig. 2 are Alice and Eve's measured BERs. Each is the average of 10 measurements—1 Msample per measurement, which typically takes only a few seconds—with error bars indicating ±1 standard deviation. At Alice's maximum SPDC output, Eve's measured modulation depth is insufficient to permit BER_E measurements that would reveal their N_S dependence. Thus to demonstrate that scaling, we replace Alice's SPDC source with the attenuated, CWDM-filtered ASE from an EDFA, whose flat-top spectrum thermal state mimics SPDC signal

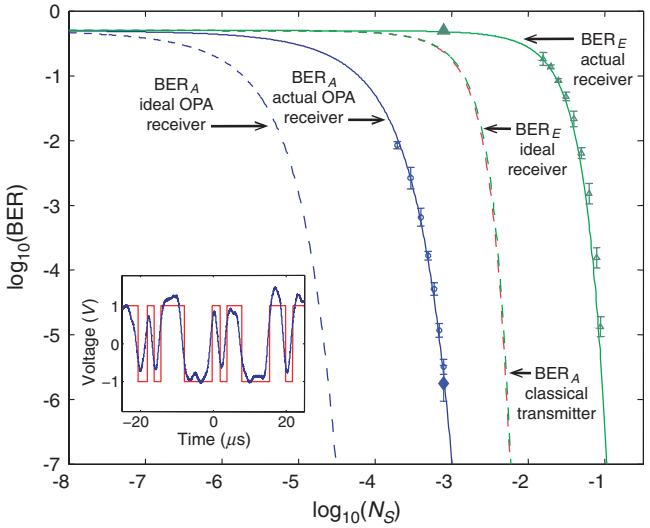

FIG. 2 (color). BER$_A$ and BER$_E$ versus source brightness N_S for 500 kbit/s communication. Inset: 25 bits of OPA-receiver detector output (blue) and Bob's corresponding modulation waveform (red). See text for more information.

light, but easily produces tens of nW of power for Eve. Eve stores the light split from the Alice-to-Bob channel using a fiber spool, which matches the total fiber length inside Bob's setup, and employs a free-space delay line to fine tune the timing between the two paths. The free-space delay line's coupling is adjusted to optimize Eve's receiver and further suppress the out-of-band ASE noise. Light she has split from the Alice-to-Bob and Bob-to-Alice channels are interfered on a 99-1 beam splitter, with 99% of the power coming from the light taken from the Alice-to-Bob channel, and 1% of the power coming from the light taken from the Bob-to-Alice channel. Eve uses a feedback arrangement similar to Alice's to stabilize her interferometer. Eve obtains her BER values by measuring the combined light using the same APD detection setup employed by Alice.

The dashed and solid blue curves in Fig. 2 are theory for BER$_A$ when Alice uses a maximally entangled SPDC source and an OPA receiver with gain $G_A - 1 = 1.86 \times 10^{-5}$. The dashed blue curve shows Alice's performance when she has an ideal OPA receiver, viz., no loss of modulation depth due to residual dispersion or suboptimal mode-pair coupling, unity detection efficiency, unity APD noise figure, no OPA pump-power fluctuations, and no electronics noise; the solid blue curve employs the experimentally determined values for these receiver nonidealities. The dashed red curve assumes that Alice uses a classical-state source with maximally correlated signal and idler and an ideal OPA receiver. The gap between the dashed red and solid blue curves shows that Alice's performance using an SPDC source and imperfect OPA reception exceeds what can be achieved with that classical-state source and ideal OPA reception.

The dashed and solid green curves in Fig. 2 are theory for BER$_E$ when Alice uses a maximally entangled SPDC source *or* a maximally correlated classical source and Eve employs an interference receiver. The dashed curve assumes Eve's receiver is ideal; the solid green curve employs the experimentally determined values for her receiver's nonidealities. The near-identical nature of the dashed red and dashed green curves is coincidental.

The blue circles in Fig. 2 are measured BER$_A$ values under the operating conditions used to obtain the solid blue curve; they show our experimental results to be in excellent agreement with theory with no free parameters being adjusted. The filled blue diamond in Fig. 2 is Alice's measured BER at $N_S = 7.81 \times 10^{-4}$ when her OPA gain was increased to $G_A - 1 = 2.48 \times 10^{-5}$, and the filled green triangle above it is the measured BER$_E$ (Alice's SPDC is used for this measurement). These two points represent our secure-communication operating point at which BER$_A = 1.78 \times 10^{-6}$ and BER$_E \approx 0.5$. The inset overlays 25 bits of Alice's receiver output (blue), with the dc level removed, on Bob's corresponding modulation waveform (red), which is scaled to match the data's peak-to-peak range. The joint state of Alice's returned and retained beams, conditioned on Bob's BPSK value, is zero mean and Gaussian. Hence, it becomes classical (see Supplemental Material [17]) when $N_B \geq N_B^{\text{thresh}} = 2.14 \times 10^3$, so our measured $N_B = 1.46 \times 10^4$ is 8.3 dB above the threshold for classicality.

The disparity between Alice and Eve's BERs at the secure-communication operating point, the N_S gap between the dashed red and solid blue theory curves at the same BER values, and N_B's exceeding N_B^{thresh} by 8.3 dB confirm the essential feature of quantum illumination that is exploited here in a communication setting: a large performance gap between an entangled-state input and a classical-state input in a lossy and noisy channel.

The open green triangles in Fig. 2 were obtained using attenuated ASE from an EDFA source in lieu of light from a down-converter. They show our measurements to be in excellent agreement with theory with no free parameters being adjusted. 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.

It is instructive to consider what would happen had Alice used a cw laser, instead of an SPDC source, and performed homodyne detection on the returned light from Bob. That receiver is ASE limited, with an error exponent that is 3 dB inferior to that of an ideal OPA receiver, so it might seem to provide a much easier route to passive eavesdropping immunity. Such is not the case: when Eve taps the Alice-to-Bob and Bob-to-Alice links and uses her own homodyne receiver, it, too, is ASE limited and its BER is the same as Alice's. So Alice's initial broadband signal-idler

entanglement is absolutely essential to her obtaining immunity to Eve's passive eavesdropping, because Eve can then only employ the broadband thermal light she taps from Alice and its modulated version that she captures from Bob.

Our measurements show Alice enjoying five orders of magnitude error-probability advantage over Eve at the secure-communication operating point. If Bob's bit sequence is equally likely and statistically independent, then: (1) Alice receives very close to one bit of information for each bit that Bob has transmitted; and (2) Eve receives nearly zero information about each of Bob's bits at this operating point.

It is useful to evaluate the QI performance gap in a different way: Alice's information advantage over Eve. The two panels in Fig. 3 display Alice's Shannon information I_{AB}, an upper bound (UB) on Eve's Holevo information χ_{EB}^{UB}, and a lower bound (LB) on Alice's information advantage $\Delta I_{AB}^{\mathrm{LB}} \equiv I_{AB} - \chi_{EB}^{\mathrm{UB}}$. (See Supplemental Material [17] for details.) In the top panel, Alice's Shannon information is computed using the error probabilities from the solid blue curve in Fig. 2, while the upper bound on Eve's Holevo information is the most she could learn about an infinitely long sequence of Bob's bits from an optimum collective quantum measurement on the light she extracts from the Alice-to-Bob and Bob-to-Alice channels. Here, we see that 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.

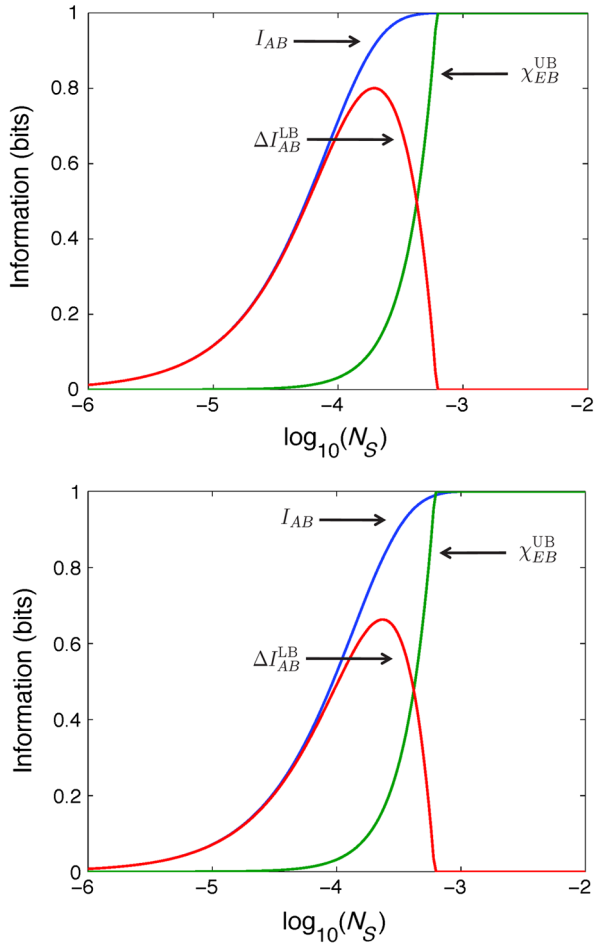

FIG. 3 (color online). Alice's Shannon information, an upper bound on Eve's Holevo information, and a lower bound on Alice's information advantage, versus Alice's source brightness N_S. The top panel computes Alice's Shannon information using the error probabilities from the solid blue curve in Fig. 2. The bottom panel computes Alice's Shannon information when Eve takes 90% of the Bob-to-Alice light instead of the 10% she receives in the top panel.

A more convincing demonstration that quantum illumination offers Alice a significant information advantage is shown in the bottom panel of Fig. 3. Here, we have changed the beam splitter that Eve uses to tap the Bob-to-Alice transmission to have 10% transmissivity. Under these conditions, Eve gets the same amount of Alice's light that Bob does and nine times the amount of Bob's light that Alice does. Nevertheless, the upper bound on her Holevo information is unchanged from what is seen in the top panel because her received BPSK modulation depth and the standard deviation of the ASE-generated noise that dominates the fluctuations in the jointly Gaussian state she receives both increase in proportion to the fraction of the light she taps. Alice's BER, however, is somewhat degraded by reducing the amount of light she gets from Bob, because of her receiver's technical noise. Consequently, her information advantage over Eve's optimum collective quantum measurement now peaks at 0.66 bits/bit.

Our experiment demonstrates the QI-communication protocol's immunity to *passive* eavesdropping that was predicted, theoretically, in [15]. That reference already noted that this protocol is vulnerable to *active* attacks, in which Eve injects her own light into Bob's terminal. Indeed, Eve could inject her own SPDC signal light into Bob, retaining her source's idler light for use with the light she taps from the Bob-to-Alice channel. Steps that could be taken to ward off active attacks were suggested in [15], and initial analyses of many of these approaches have been performed [18], but more work is needed on defeating active attacks.

In conclusion, we have demonstrated that the benefits of bosonic entanglement can be reaped over an entanglement-breaking channel. Our QI protocol experimentally achieved more than five orders of magnitude BER advantage for Alice over a passive eavesdropping Eve when both use realistic receivers. Based on the excellent fit between our data and theory, we claim that Alice enjoys an information advantage that can exceed 0.6 bits per Bob's transmitted bit over the optimum collective quantum Eve when Eve taps 50% of Alice's transmission and 90% of Bob's transmission. These advantages are consequences of

Alice's initial broadband signal-idler entanglement, because they disappear when Alice's signal-idler phase-sensitive cross correlation is classical, or when Alice uses a laser source.

The authors thank Eric Dauler for the loan of the bit-error rate tester and Poul Erik Schmidt at OFS for providing the dispersion-compensating fibers. This research was supported by an ONR Basic Research Challenge Grant.

*zszhang@mit.edu

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).
[3] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, Nature (London) **489**, 269 (2012).
[4] H. J. Kimble, Nature (London) **453**, 1023 (2008).
[5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[6] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
[7] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Nat. Phys. **4**, 282 (2008).
[8] P. Shor, SIAM J. Comput. **26**, 1484 (1997).
[9] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. C. Chuang, Nature (London) **414**, 883 (2001).
[10] A. Politi, J. C. F. Matthews, and J. L. O'Brien, Science **325**, 1221 (2009).
[11] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[12] S. Lloyd, Science **321**, 1463 (2008).
[13] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, Phys. Rev. Lett. **101**, 253601 (2008).
[14] S. Guha and B. I. Erkmen, Phys. Rev. A **80**, 052310 (2009).
[15] J. H. Shapiro, Phys. Rev. A **80**, 022320 (2009).
[16] E. D. Lopaeva, I. Ruo Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, Phys. Rev. Lett. **110**, 153603 (2013).
[17] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.111.010501 for more details on the theoretical calculations and experimental parameters.
[18] W. Xu and J. H. Shapiro, in *Quantum Communication, Measurement and Computing (QCMC)*, edited by T. Ralph and P. K. Lam, AIP Conf. Proc. No. 1363 (AIP, New York, 2011), pp. 31–34.