Secure communication via quantum illumination

Citation: Shapiro, Jeffrey H., Zheshen Zhang, and Franco N. C. Wong. “Secure Communication via Quantum Illumination.” Quantum Information Processing 13.10 (2014): 2171–2193.

As Published: http://dx.doi.org/10.1007/s11128-013-0662-1

Publisher: Springer US

Persistent URL: http://hdl.handle.net/1721.1/103793

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Quantum Information Processing manuscript No.
(will be inserted by the editor)

Secure Communication via Quantum Illumination

Jeffrey H. Shapiro · Zheshen Zhang ·
Franco N. C. Wong

Received: date / Accepted: date

Abstract In the quantum illumination (QI) protocol for secure communication, Alice prepares entangled signal and idler beams via spontaneous parametric downconversion. She sends the signal beam to Bob, while retaining the idler. Bob imposes message modulation on the beam he receives from Alice, amplifies it, and sends it back to her. Alice then decodes Bob's information by making a joint quantum measurement on the light she has retained and the light she has received from him. The basic performance analysis for this protocol—which demonstrates its immunity to passive eavesdropping, in which Eve can only listen to Alice and Bob's transmissions—is reviewed, along with the results of its first proof-of-principle experiment. Further analysis is then presented, showing that secure data rates in excess of 1 Gbps may be possible over 20-km-long fiber links with technology that is available or under development. Finally, an initial scheme for thwarting active eavesdropping, in which Eve injects her own light into Bob's terminal, is proposed and analyzed.

Keywords Secure communication · Entanglement · Spontaneous parametric downconversion · Optical parametric amplification

1 Introduction

Governments, businesses, and the general populace are increasingly dependent on the Internet, and many of their communications thereon need to be protected from interception by unauthorized parties. To date, that protection has been provided by classical cryptosystems—such as the RSA public-key system—whose security relies on the computational complexity (proven or presumed) of decoding the plaintext from an intercepted ciphertext. Quantum mechanics, however, offers

This research was supported by an ONR Basic Research Challenge grant and the DARPA Quiness Program.

J. H. Shapiro (E-mail: jhs@mit.edu) · Zheshen Zhang · Franco N. C. Wong
Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

an alternative approach. In particular, quantum key distribution (QKD) [1–3] enables two geographically separated users—Alice and Bob—to create a shared set of completely random key bits in a manner that precludes an eavesdropper (Eve) from having anything more than an inconsequentially small amount of information about them. That such a goal is possible arises from a fundamental quantum mechanical principle: Eve cannot tap a quantum channel without creating a disturbance on that channel.

QKD has moved from its early theoretical roots [1–3] to major network demonstrations [4,5], and its protocols and technologies continue to improve. Nevertheless, the key rates of current QKD systems fall short of enabling the ultimate, information-theoretic security afforded by one-time pad encryption [6]. For example, the Tokyo QKD network's TREL system [5] demonstrated a record ∼300 kbps secure key rate over a 45-km-long link of installed fiber, but this key rate pales in comparison with the Gbps capability of widely-available ethernet connections that are candidates for one-time pad encryption. Moreover, although the TREL system used a 1 GHz pulse rate, only ∼0.3% of the transmitted bits were received, and ∼4% of them were received in error. So, although this system can provide shared secret bits, it is not a viable means for direct information transmission. Specifically, it is incapable of directly transmitting the random bit stream that results from lossless data-compression of an information-bearing message to its Shannon limit [7].

In 2009 [8], we introduced a two-way optical communication protocol that defeats *passive* eavesdropping—in which Eve merely listens to Alice and Bob's transmissions—while operating at data rates far in excess of current QKD key rates. There we showed, theoretically, that Alice and Bob could communicate an uncoded 50 Mbps bit stream over 50 km of low-loss fiber with a bit-error probability of less than 10^{-6}, while an Eve who collected *all* the light that did not reach its intended destination—i.e., 90% of the light Alice sent to Bob and 90% of the light Bob sent to Alice—suffered a bit-error probability of at least 0.28. Recently, we reported a 500 kbps table-top experimental demonstration of our protocol [9], in which Alice and Bob realized a bit-error probability of $\sim 2\times 10^{-6}$ while Eve's was ∼0.5. This demonstration verified the theory from [8], once experimental nonidealities were accounted for. In addition, it verified a property of even broader potential significance—entanglement's benefit can survive an entanglement-breaking channel—as we now explain.

Our protocol employs the quantum illumination paradigm [10,11], in which Alice produces entangled signal and idler beams via continuous-wave (cw) spontaneous parametric downconversion (SPDC), sending the signal to Bob and retaining the idler. Bob, for his part, imposes message modulation on the signal beam he receives from Alice, amplifies it, and sends it back to her. The amplified spontaneous emission (ASE) noise from Bob's amplifier destroys the entanglement that would otherwise have existed between the beam Alice receives from him and her retained idler. Yet Alice and Bob obtain immunity to passive eavesdropping *only* because Alice started with an entangled source. Indeed, had Alice started with signal and idler beams at the limit of classical cross-correlation, then her error probability would *not* have been much lower than Eve's [9].

The rest of this paper is organized as follows. We begin, in Sect. 2, by reviewing the protocol from [8], and extending its analysis to include an assessment of Alice and Bob's information advantage over an optimal collective attack by a passive eavesdropper. We continue, in Sect. 3, by reviewing the experiment from [9]. Next, in Sect. 4, we show how the secure data rate of our quantum illumination protocol might be increased to ~1 Gbps. Then, in Sect. 5, we introduce a potential means for defeating the principal vulnerability of our protocol, viz., its susceptibility to *active* eavesdropping, in which Eve injects her own light into Bob's terminal. We conclude, in Sect. 6 by summarizing our results and their implications.

2 The Quantum Illumination Protocol and its Performance

The basic setup for our quantum-illumination (QI) communication protocol is shown in Fig. 1. Alice's cw SPDC source is assumed to emit single spatial-mode signal and idler beams[1] having uniform fluorescence spectra over the downconverter's W Hz phase-matching bandwidth, with common brightness (average photon number per mode) N_S photons/sec-Hz. The quadrature components of these beams are maximally entangled in mode pairs, i.e., the signal mode that is blue-detuned (red-detuned) by ω from the signal's center frequency ω_S is entangled with the idler mode that is red-detuned (blue-detuned) by ω from its center frequency ω_I. Thus, for a typical case, each T-sec-long transmission from Alice to Bob comprises $M = TW \gg 1$ of such mode pairs, e.g., the 50 Mbps communication example from [8], which assumed $W = 1$ THz and $T = 20$ ns, had $M = 2 \times 10^4$.[2]

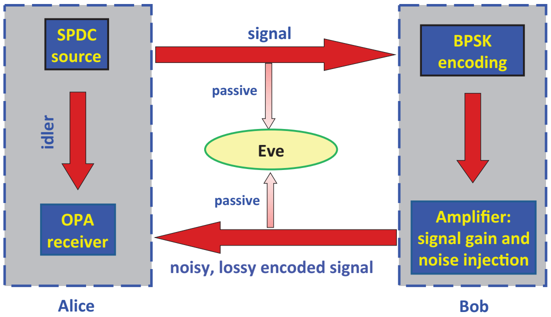

Fig. 1 Basic setup for achieving passive-eavesdropping immunity by means of quantum illumination. SPDC: spontaneous parametric downconversion. BPSK: binary phase-shift keying. OPA: optical parametric amplifier.

Alice sends the signal light to Bob through a pure-loss channel of transmissivity κ, in which propagation loss is accompanied by the minimum (vacuum-state) noise injection needed to preserve free-field commutator brackets. She retains the idler light for subsequent joint measurement with the light that Bob will return to her. Bob applies binary phase-shift keying (BPSK) at rate $R = 1/T$ bps to the light he receives from Alice, passes it through a phase-insensitive amplifier with

[1] We are presuming single spatial-mode operation here, as was done in [8], for compatibility with transmission over single-mode fiber. In Sect. 6 we will comment on the utility of our protocol for line-of-sight links through the atmosphere.

[2] The analysis in [8] assumed, and the experiment in [9] employed, $TW \gg 1$.

gain G_B whose output has ASE noise of brightness N_B photons/sec-Hz, and transmits the output beam back to Alice through a transmissivity-κ pure-loss channel. Eve is assumed to collect all the light lost en route between Alice and Bob and all the light lost en route between Bob and Alice. Moreover, she is afforded an optimum quantum receiver for decoding Bob's message bits—one by one—from a joint measurement on the two light beams she had tapped, even though no known realization exists for that receiver. Alice, however, is only permitted to use the optical parametric amplifier (OPA) receiver from [12], whose error exponent is 3 dB inferior to that of her optimum quantum receiver, because it is the best known-realization receiver for decoding Bob's message. In the OPA receiver, Alice's retained and returned light beams are applied to the idler and signal ports, respectively, of a low-gain ($G_A - 1 \ll 1$) OPA to convert their phase-sensitive cross correlation into intensity modulation of the amplifier's output beams.[3] Alice then decodes Bob's message by direct detection of the light from her OPA's idler-port output. Throughout this section we will assume, as was done in [8], that Alice and Bob have ideal equipment, so that the only losses in their portions of the Fig. 1 setup are those due to propagation through the transmissivity-κ channels that connect their terminals.

The principal analytic results from [8] are the Chernoff bounds [14,15] on the bit-error probabilities of Alice and Eve's optimum (minimum error-probability) quantum receivers, the Bhattacharyya bound on the bit-error probability of Alice's OPA receiver, and the lower bound on the the bit-error probability of Eve's optimum quantum receiver. These bounds, obtained using Pirandola and Lloyd's symplectic-decomposition technique [16], take the following simple asymptotic forms in QI's normal low-brightness ($N_S \ll 1$), very lossy ($\kappa \ll 1$), high-noise ($N_B \gg 1$) operating regime:

$$\Pr(e)^{\rm opt}_{\rm Alice} \le \frac{\exp(-4M\kappa G_B N_S/N_B)}{2}, \tag{1}$$

$$\frac{1-\sqrt{1-\exp(-8M\kappa G_B N_S^2/N_B)}}{2} \le \Pr(e)^{\rm opt}_{\rm Eve} \le \frac{\exp(-4M\kappa G_B N_S^2/N_B)}{2}, \tag{2}$$

and

$$\Pr(e)^{\rm OPA}_{\rm Alice} \le \frac{\exp(-2M\kappa G_B N_S/N_B)}{2}. \tag{3}$$

Note that the Chernoff bounds are exponentially tight in the mode-pair number M, e.g., $-\ln\!\left[2\Pr(e)^{\rm opt}_{\rm Alice}\right]/M$ converges to $4\kappa G_B N_S/N_B$ as $M \to \infty$, when $N_S \ll 1$, $\kappa \ll 1$, and $N_B \gg 1$.

Equations (1)–(3) clearly show Alice's error-probability advantage over Eve in that Alice's SPDC source is operated at low brightness, $N_S \ll 1$. Thus Alice's error exponent—even with the OPA receiver—is far superior to Eve's. This N_S versus N_S^2 behavior of Alice and Eve's Chernoff-bound error exponents arises from Alice's signal and idler beams being emitted with a phase-sensitive cross correlation that is at the ultimate quantum limit, which is proportional to $\sqrt{N_S(N_S+1)}$,

[3] The low-gain OPA is a downconverter to which non-vacuum signal and idler inputs are applied. That it converts phase-sensitive cross correlation between those inputs into intensity modulation of the idler output follows from standard coupled-mode analysis [13]. The low-gain condition maximizes the resulting signal-to-noise ratio on the idler output by suppressing the ASE noise present on the returned light.

whereas the light beams available to Eve have a phase-insensitive cross correlation that is bounded by the classical limit, which is proportional to N_S. The latter is much weaker than the former because $N_S \ll 1$. Interestingly, as noted in [8] and demonstrated in [9], this entanglement-derived error-probability advantage is present despite Bob's ASE noise having destroyed the entanglement between the two light beams available to Alice's receiver.[4]

Figure 2, reproduced from [8], plots the bounds for Alice's optimum quantum and OPA receivers and Eve's optimum quantum receiver, versus the number of mode pairs (the time-bandwidth product for a single bit) M, for the following example: $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$, with $G_A = 1 + N_S/\sqrt{\kappa N_B}$. These results were obtained from exact evaluation of the procedure from [16], i.e., *without* passage to the asymptotic regime in which Eqs. (1)–(3) apply. We see that the *upper* bound on the error probability of Alice's OPA receiver can be orders of magnitude lower than the *lower* bound on the error probability of Eve's optimum quantum receiver. For example, at $M = 2 \times 10^4$, corresponding to a 50 Mbps data rate when the SPDC source's phase-matching bandwidth is 1 THz, we have $\Pr(e)^{\rm opt}_{\rm Alice} < 5.1\times10^{-7}$, while $0.28 < \Pr(e)^{\rm opt}_{\rm Eve} < 0.46$. So, if propagation is through fiber with 0.2 dB/km loss, then—because we have neglected all other losses and nonidealities—the preceding performance can be achieved over a 50-km-long fiber link.[5]

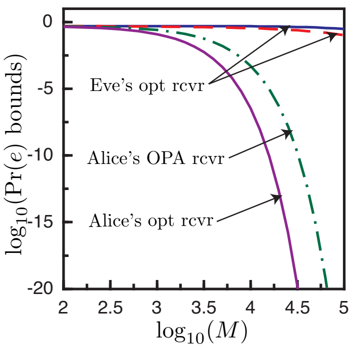

Fig. 2 Bit-error probability bounds versus mode-pair number (time-bandwidth product for a single bit) M. All curves assume $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$. Solid curves: Chernoff bounds for Alice and Eve's optimum quantum receivers. Dashed curve: lower bound for Eve's optimum quantum receiver. Dot-dashed curve: Bhattacharyya bound for Alice's OPA receiver with $G_A = 1 + N_S/\sqrt{\kappa N_B}$.

So far we have only examined the bit-error probability advantage that Alice and Bob have over their passive-eavesdropping adversary. Using these results to bound Alice and Bob's Shannon information advantage over Eve's then quantifies

[4] The ASE threshold for entanglement breaking is $N_B^{\rm thresh} = \kappa G_B$. Because phase-insensitive amplifiers must obey $N_B \geq G_B - 1$, any $\kappa \leq (G_B - 1)/G_B$ will make the channel entanglement-breaking. For $G_B \gg 1$, this condition will always be satisfied in long-distance communication.

[5] The impact of nonidealities, such as idler-storage loss, will be addressed explicitly in Sect. 3, when we review our proof-of-principle experiment from [9].

their security with respect to an optimal *individual* attack by a passive eavesdropper. In [17], however, we showed how to lower bound the information advantage that they enjoy against an optimal *collective* attack by this passive eavesdropper, i.e., the difference between Alice and Bob's Shannon information and Eve's Holevo information, hence providing a considerably stronger security guarantee. But, before developing those collective-attack results, we will consider the bit-error probability bounds for some alternative operating regimes, because they provide important physical insights into the behavior of our QI protocol.

Our QI protocol for passive-eavesdropping immunity—like its predecessor for QI target detection—operates in the low-brightness, very-lossy, high-noise regime. Could it also work in the absence of noise ($N_B = 0$) or at high source-brightness ($N_S \geq 1$)? These questions are answered in Fig. 3. Here we see that at low source-brightness ($N_S = 0.004$) when Bob does not use an amplifier ($G_B = 1$ and $N_B = 0$) Eve's optimum quantum receiver outperforms Alice's. This is because Eve is collecting the lion's share of the light propagating in each direction between Alice and Bob. It is consistent with Nair's result [18] showing that quantum illumination provides an insignificant performance advantage over coherent-state operation when both are used to detect a weakly-reflecting target in the absence of background noise. Figure 3 also shows that the high-brightness ($N_S = 1, G_B = N_B = 10^4$) Chernoff bounds for Alice and Eve's receivers are much closer to each other than are their low-brightness counterparts from Fig. 2. This is due to the convergence of the $\propto\sqrt{N_S(N_S+1)}$ quantum limit on phase-sensitive cross correlation to the $\propto N_S$ classical limit on phase-insensitive cross correlation that occurs when $N_S \gg 1$. In short, Fig. 3 verifies that the preferred operating regime for our QI communication protocol is one with low source brightness and high background noise. Staying within that regime, we now turn to Alice and Bob's information advantage when a passive eavesdropper mounts an optimum collective attack.

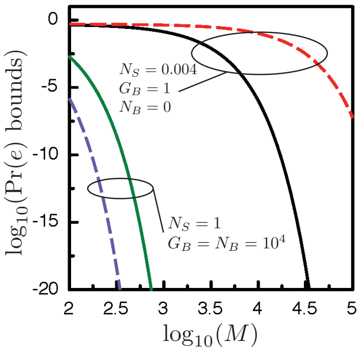

Fig. 3 Chernoff bounds versus mode-pair number (time-bandwidth product for a single bit) M, in the no-noise and high-brightness regimes. All curves assume optimum quantum reception and $\kappa = 0.1$. Solid curves: Eve's receivers. Dashed curves: Alice's receivers.

Alice and Bob's information advantage, $\mathit{\Delta} I_{AB}$, in bits/channel-use satisfies

$$\mathit{\Delta} I_{AB} = I_{AB} - \chi_E, \tag{4}$$

i.e., it is the difference between Alice and Bob's Shannon information and Eve's Holevo information. We will assume that Bob's message bits are equally likely to be 0 or 1, so that I_{AB} is given by

$$I_{AB} = 1 - H_B(\Pr(e)_{\text{Alice}}), \tag{5}$$

in terms of the binary entropy function $H_B(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ and Alice's bit-error probability. Eve's Holevo information is

$$\chi_E = S(\hat{\rho}_E) - \sum_{k=0}^{1} S(\hat{\rho}_{E_k})/2, \tag{6}$$

where $S(\hat{\rho}) = -\text{Tr}[\hat{\rho}\log_2(\hat{\rho})]$ is the von Neumann entropy, $\hat{\rho}_E$ is Eve's unconditional density operator for the light beams she has tapped, and $\hat{\rho}_{E_k}$ is her conditional density operator for those beams when Bob's message bit is k. Because I_{AB} is monotonically decreasing with increasing $\Pr(e)_{\text{Alice}}$, Eq. (3) gives us the lower bound (LB)

$$I_{AB} \geq I_{AB}^{\text{LB}} = 1 - H_B[\exp(-2M\kappa G_B N_S/N_B)/2], \tag{7}$$

when Alice uses an OPA receiver with $G_A = 1 + N_S/\sqrt{\kappa N_B}$ and operation is in the low-brightness, very-lossy, high-noise regime. Because the $\{\hat{\rho}_{E_k}\}$ are zero-mean Gaussian states, their von Neumann entropies are easily found [16], but $\hat{\rho}_E$, although zero-mean, is *not* Gaussian. Moreover, it has an enormous number of temporal modes, half of which (the modes tapped from the Bob-to-Alice channel) have very high average photon numbers, and all of which are correlated in phase by virtue of Bob's BPSK modulation. Nevertheless, because $\hat{\rho}_E$'s Wigner covariance matrix, $\boldsymbol{\Lambda}_E$, is diagonal, its von Neumann entropy cannot exceed $S_{\text{therm}}(\boldsymbol{\Lambda}_E)$, the von Neumann entropy of a thermal state with the same covariance matrix. Thus we have the upper bound (UB)

$$\chi_E \leq \chi_E^{\text{UB}} = S_{\text{therm}}(\boldsymbol{\Lambda}_E) - \sum_{k=0}^{1} S(\hat{\rho}_{E_k})/2, \tag{8}$$

whence

$$\Delta I_{AB} \geq \Delta I_{AB}^{\text{LB}} = I_{AB}^{\text{LB}} - \chi_E^{\text{UB}}. \tag{9}$$

Figure 4 plots the preceding information bounds versus the mode-pair number M for our standard example: $N_S = 0.004$, $\kappa = 0.1$, $G_B = N_B = 10^4$. In this figure the lower bound on Alice and Bob's Shannon information is obtained from exact evaluation of the Bhattacharyya bound for her OPA receiver's error probability—assuming $G_A = 1 + N_S/\sqrt{\kappa N_B}$—rather than using the asymptotic formula from Eq. (7). We see from this figure that $\Delta I_{AB}^{\text{LB}}$ exceeds 0.88 bits/channel-use at its peak. For a 1 THz phase-matching bandwidth, this implies that Alice and Bob's maximum information advantage in bits/sec, $\max(W\Delta I_{AB}^{\text{LB}}/M)$, exceeds 100 Mbps, suggesting that QI might bring secure communication rates up to Gbps with more complete system optimization. Moreover, if the only loss encountered in Fig. 1 is propagation through 0.2 dB/km fiber, then this secure rate is achievable on a 50-km-long link. Lest we become wildly optimistic in this regard, we will devote the next section to a review of our proof-of-principle experiment. That review will make the experimental challenges in realizing QI's theoretically-predicted potential explicit. In Sect. 4 we will return to considering how high a secure rate can be supported by our QI protocol over application-relevant propagation distances.

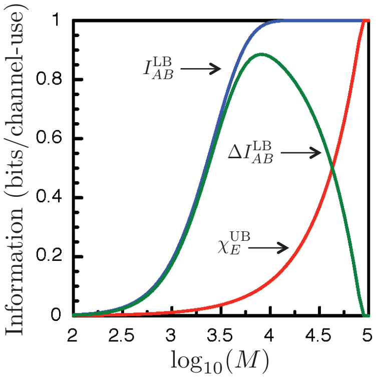

Fig. 4 Lower bound on Alice and Bob's Shannon information for an OPA receiver with $G_A = 1 + N_s/\sqrt{\kappa N_B}$, upper bound on Eve's Holevo information for a collective passive-eavesdropping attack, and the resulting lower bound on Alice and Bob's information advantage, all plotted versus mode-pair number (time-bandwidth product for a single bit) M. The curves assume $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$.

3 Proof-of-Principle Experiment

The setup for our proof-of-principle experiment is shown in Fig. 5 [9]. Alice's SPDC source uses a 20-mm type-0 phase-matched MgO-doped periodically-poled lithium niobate (MgO:PPLN) crystal that is cw pumped at 780 nm, producing signal and idler outputs at 1550 nm and 1570 nm. A coarse wavelength-division multiplexer (CWDM) separates the signal and idler and bandlimits them to 16 nm ($W \approx 2$ THz). The $T = 2\,\mu$s bit duration at 500 kbps 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.

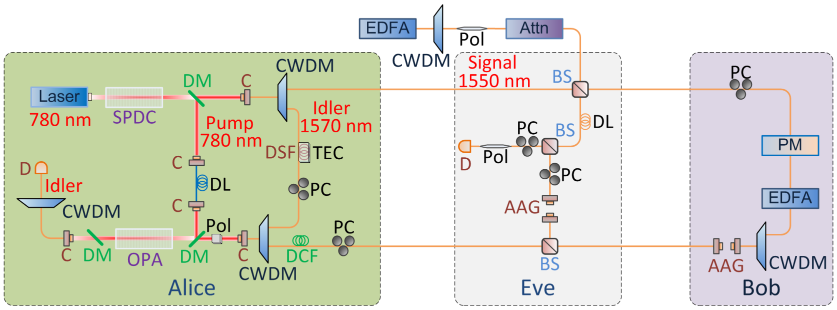

Fig. 5 Experiment setup. SPDC: spontaneous parametric downconverter; DM: dichroic mirror; C: collimator; CWDM: coarse wavelength-division multiplexer; BS: beam splitter; Attn: attenuator; EDFA: erbium-doped fiber amplifier; DL: delay line; PC: polarization controller; PM: phase modulator; AAG: adjustable air gap; Pol: polarizer; DCF: dispersion-compensating fiber; DSF: dispersion-shifted fiber; TEC: thermoelectric cooler; OPA: optical parametric amplifier; D: detector. Reproduced from [9], Fig. 1.

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 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.[6] The modulated light is fed to an erbium-doped fiber amplifier (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 bandlimit 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. 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 (SCS) which stabilizes the relative phases between the OPA pump, Alice's retained idler, and the modulated light she receives from Bob. The SCS 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-

[6] We will use bit-error rate and bit-error probability interchangeably. The former term is commonly used in describing experiments, whereas the latter is preferred for the theory.

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 implemented 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 interfering 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 [17] for details)

$$\mathrm{BER}_A = Q\left(\frac{\sqrt{M}\zeta_A\sqrt{N_S(N_S+1)}}{\sigma^{\rm tot}_{A_+} + \sigma^{\rm tot}_{A_-}}\right) \tag{10}$$

$$\mathrm{BER}_E = Q\left(\frac{\sqrt{M}\zeta_E N_S}{\sigma^{\rm tot}_{E_+} + \sigma^{\rm tot}_{E_-}}\right). \tag{11}$$

Here: Q is the tail integral of the standard Gaussian probability density, $Q(x) = \int_x^\infty dy\, \frac{e^{-y^2/2}}{\sqrt{2\pi}}$; $\zeta_A\sqrt{N_S(N_S+1)}$ ($\zeta_E N_S$) is the modulation-depth signature of Bob's message bit seen by Alice (Eve), where ζ_A (ζ_E) is a transmission efficiency; and $\sigma^{\rm tot}_{A_\pm}$ ($\sigma^{\rm tot}_{E_\pm}$) are Alice's (Eve's) per-mode noise standard deviations for bit values 0 and 1. The transmission efficiencies include 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 per-mode noise standard deviations include their fundamental quantum-noise terms, and technical noise arising from the OPA's pump-power fluctuations, the APD's excess-noise factor, and the detection system's electronics.

Figure 6, reproduced from [9], shows the results of our experiment. The dashed and solid blue curves are theory for BER_A when Alice uses 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 sub-optimal 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. 6 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. 6 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.

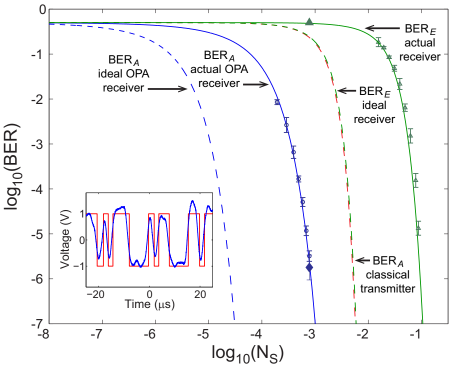

Fig. 6 BER$_A$ and BER$_E$ versus source brightness N_S for 500 kbps communication. Inset: 25 bits of OPA-receiver detector output (blue) and Bob's corresponding modulation waveform (red). See text for more information.

The filled blue diamond in Fig. 6 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 source was 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,[7] 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 when $N_B \geq N_B^{\text{thresh}} = 2.14 \times 10^3$, so our measured $N_B = 1.46 \times 10^4$ was 8.3 dB above the threshold for classicality.[8]

The open green triangles in Fig. 6 were obtained using attenuated ASE from an EDFA source, whose statistics mimic those of Alice's SPDC source but at brightness levels unobtainable therefrom with our available pump power. 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. 6 at the same BER values quantifies Alice and Bob's entanglement-derived communication advantage when Alice and Eve both use realistic receivers.

These experimental results validate the theory proposed in [8]. In [9] we relied on that validation to evaluate Alice and Bob's information advantage over Eve's collective attack for the paper's experimental scenario. The evaluation showed they could realize more than 0.8 bits/channel-use advantage in this 500 kbps system. In the next section we return to the question raised at the end of Sect. 3: how high a secure rate can QI provide over a propagation distance of real application interest?

[7] The dc level is removed prior to amplification. The equivalent dc level for the inset in Fig. 6 is ∼33 V.

[8] The classicality threshold employed here accounts for the nonidealities in the experimental system, see [17].

4 Pushing the QI Protocol to Higher Rate-Distance Product

Let us return to the Fig. 1 setup for QI communication, this time with Alice using a downconverter with $W = 2\,\mathrm{THz}$ and $N_S = 0.01$. The following system nonidealities will be included:[9] (1) Alice suffers 10% coupling loss between her SPDC source and the Alice-to-Bob fiber, 10% coupling loss between the Bob-to-Alice fiber and her OPA, and her detection system, although shot-noise limited, has 80% detection efficiency. (2) Alice stores her idler in a 40-km-long optical fiber whose $0.2\,\mathrm{dB/km}$ loss equals that of the 20-km-long fibers connecting Alice to Bob and Bob to Alice. (4) Bob has 10% coupling loss between the Alice-to-Bob fiber and his BPSK modulator, and 10% coupling loss between his EDFA and the Bob-to-Alice fiber.

We have calculated Alice and Bob's Shannon information, in bits/sec, from

$$I_{AB} = R[1 + \mathrm{BER}_A \log_2(\mathrm{BER_A}) + (1 - \mathrm{BER}_A) \log_2(1 - \mathrm{BER_A})], \tag{12}$$

where $R = 1/T$ is Bob's modulation rate. To find BER_A, we used the Gaussian-approximation expression from Eq. (10), which is valid for $M \gg 1$.[10] In terms of the parameters given in Table 1, BER_A is given by that equation with $M = W/R$,

$$\zeta_A = 4\kappa_d \sqrt{G_A(G_A - 1)\kappa_I \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A}, \tag{13}$$

and

$$\sigma^{\mathrm{tot}}_{A_\pm} = \sqrt{N^\pm_A (N^\pm_A + 1)}, \tag{14}$$

where

$$\begin{aligned} N^\pm_A = {} & \kappa_d G_A \kappa_I N_S + \kappa_d (G_A - 1) + \kappa_d (G_A - 1)\kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S \\ & + \kappa_d (G_A - 1)\kappa'_A \kappa_2 \kappa'_B N_B \pm \zeta_A \sqrt{N_S(N_S + 1)}. \end{aligned} \tag{15}$$

See [17] for a full derivation.

Figure 7 shows Alice and Bob's Shannon information, I_{AB} from Eq. (12), the upper bound

$$\chi^{\mathrm{UB}}_E = R\left[S_{\mathrm{therm}}(\boldsymbol{\Lambda}_E) - \sum_{k=0}^{1} S(\hat{\rho}_{E_k})/2\right], \tag{16}$$

on the Eve's Holevo information, in bits/sec, for a collective passive-eavesdropping attack, and the resulting lower bound on Alice and Bob's information advantage, $\Delta I^{\mathrm{LB}}_{AB} = I_{AB} - \chi^{\mathrm{UB}}_E$. These quantities are plotted versus Bob's modulation rate R. Note that the minimum number of mode pairs for this figure occurs at $R = 10\,\mathrm{Gbps}$, for which $M = 200$, ensuring the validity of Eq. (10). Two initial points worth noting about this figure are the following: (1) The overlapping straight-line behavior of I_{AB} and χ^{UB}_E at low modulation rates is due to both Alice and Eve's having near-perfect data, making their respective information rates equal

[9] All other nonidealities will be neglected, e.g., Alice's dispersion compensation will be taken to be perfect.

[10] For the parameter values given below, we have found that this approximation has 0.23% error at $M = 200$—the M value associated with $R = 10\,\mathrm{Gbps}$—by comparison with the exact results for that M value. That exact analysis shows that increasing R to $2\,\mathrm{Tbps}$ (reducing M to 1) does not appreciably increase $\Delta I^{\mathrm{LB}}_{AB}$ beyond the value shown in Fig. 7 for $R = 10\,\mathrm{Gbps}$.

Parameter	Symbol	Value
Alice's fluorescence bandwidth	W	2 THz
Alice's source brightness	N_S	0.01
Alice's signal transmissivity	κ_A	0.90
Alice-to-Bob transmissivity	κ_1	0.40
Bob's pre-EDFA transmissivity	κ_B	0.90
Bob's EDFA gain	G_B	10^4
Bob's EDFA per-mode ASE	N_B	10^4
Bob's post-EDFA transmissivity	κ'_B	0.90
Bob-to-Alice transmissivity	κ_2	0.40
Alice's return transmissivity	κ'_A	0.90
Alice's idler transmissivity	κ_I	0.16
Alice's OPA gain -1	$G_A - 1$	2.51×10^{-3}
Alice's detection efficiency	κ_d	0.8

Table 1 System parameters assumed in calculating the information-advantage results shown in Fig. 7.

to Bob's modulation rate. (2) Once Eve's Holevo-information upper bound falls below 1 bit/channel-use, its value in bits/sec becomes constant, because the former is proportional to M, the latter equals the former multiplied by $R = W/M$, and the phase-matching bandwidth W is a constant. Of greater significance, however, is the fact that $\Delta I_{AB}^{\rm LB}$ exceeds 1 Gbps at $R = 10$ Gbps. In this regard, some discussion of our assumed parameters is definitely germane.

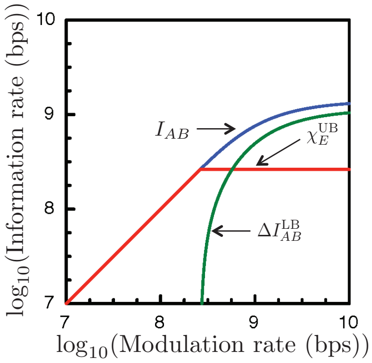

Fig. 7 Alice and Bob's Shannon information for an OPA receiver with $G_A = 1 + \kappa_I N_s/\sqrt{\kappa_2 N_B}$, upper bound on Eve's Holevo information for a collective passive-eavesdropping attack, and the resulting lower bound on Alice and Bob's information advantage, all plotted versus Bob's modulation rate. The curves assume the parameters given in Table 1.

Of the system parameters in Table 1, the values for W, N_S, G_B, N_B, and G_A are easily obtained, and those for κ_1, κ_2, and κ_I are just the transmissivities for 0.2 dB/km single-mode fibers that are 20 km (for κ_1 and κ_2) and 40 km (for κ_I) in length. The κ_A, κ_B, κ'_B and κ'_A values—which account for the coupling losses inside Alice and Bob's terminals—are admittedly aggressive, but Bob's having a BPSK modulator capable of operation at up to 10 Gbps is not. The biggest challenge, however, is clearly the photodetector. It should be a photon-number resolving single-photon detector[11] that has negligible dark counts with 10 GHz bandwidth and high quantum efficiency at telecom wavelengths. Recent progress with tungsten-silicide (WSi) superconducting nanowire single-photon detectors (SNSPDs) [19] has shown that *most* of these requirements—everything but photon-number resolution and 10 GHz bandwidth—could be had, at the cost of employing cryogenics. Furthermore, the authors of that work speculate that large arrays of such detectors could be developed which preserve the desirable features they demonstrated in a single-element device. With such arrays, our requirements for photon-number resolution and 10 GHz bandwidth could be satisfied by spreading the light beam to be detected over the array. A preliminary demonstration of this concept has already been reported with a four-element NbN SNSPD [20], but we would need a much larger array, like the ones that might be developed for astronomy.

On the other side of the ledger, we should note the one assumption underlying Fig. 7 that is conservative, rather than aggressive, namely that Eve captures all the light lost in the Alice-to-Bob and Bob-to-Alice channels. It would be much more realistic to assume that Eve inserts a tap into each fiber, making it appear to Alice and Bob that their installed fibers have slightly more loss than 0.2 dB/km.[12] Under this more realistic assumption, it turns out that Alice and Bob's performance advantage increases, but not dramatically, given the parameter values we have assumed. For example, suppose that Eve inserts a 1 dB tap in the Alice-to-Bob fiber close to Alice's terminal, and a 1 dB tap in the Bob-to-Alice channel close to Bob's terminal. Then, with the other parameters as specified in Table 1 and Bob's modulator running at 10 Gbps, $\mathit{\Delta} I_{AB}^{\rm LB}$ increases from its 1.04 Gbps value from Fig. 7 to 1.15 Gbps. Surprisingly, this story changes if we increase Alice's source brightness. With $N_S = 0.04$, we get $\mathit{\Delta} I_{AB}^{\rm LB} = 742$ Mbps at $R = 10$ Gbps when Eve gets all the light that is lost in transmission, but we find $\mathit{\Delta} I_{AB}^{\rm LB} = 2.68$ Gbps at that R value when Eve makes 1 dB taps of the two fibers that connect Alice and Bob.

While waiting for SNSPD technology to advance to the level needed to fulfill the requirements of the QI system we have just considered, let us turn our attention to a more readily realizable setup for high-rate operation. We will continue with the parameters from Table 1, but with $N_S = 0.04$ instead of 0.01, and, as justified below, $\kappa_I = 0.9$. Also, we will modify the basic QI communication architecture to use dense wavelength-division multiplexing. Thus Bob will pass the 2-THz-bandwidth light he receives from Alice through a dense wavelength-division multiplexer (DWDM), whose outputs will be a set of 40 channels, each of $W_c = 40$ GHz bandwidth with 10 GHz guard bands between adjacent channels. Bob will then impress independent rate R_c bps BPSK modulation on each of these individual channels, recombining the modulated light beams with another DWDM prior to optical amplification and transmission back to Alice. Alice's receiver independently homodyne detects the 40 channels of idler and the 40 channels of returned light she obtains after each 2-THz-bandwidth beam has been passed

[11] At $R = 10$ Gbps, Alice's OPA receiver detects an average of 15.3 photons/bit when Bob send a 0, and 11.2 photons/bit when Bob sends a 1.

[12] Of course, if Alice and Bob use optical time-domain reflectometers (OTDRs) to monitor the integrity of their fiber links, they should be able to detect the presence of a discrete loss element at an unexpected location. We shall ignore that possibility for now.

through a DWDM.[13] With $R_c = 300\,\text{Mbps}$ modulation on each channel, Alice and Bob's *total* information advantage (over all 40 channels) is at least 2.89 Gbps.[14] In comparison with the previous single-channel system—which required an SNSPD array to achieve a Gbps information advantage—the DWDM system can rely on existing 40 GHz PIN-diode homodyne receivers. The price paid by the DWDM approach is one of complexity: Bob needs 40 BPSK modulators and Alice needs homodyne detectors for 40 idler and 40 returned-light channels, each equipped with an analog-to-digital converter fast enough to accommodate the 40-GHz-bandwidth output [21].[15]

5 Thwarting Active Eavesdropping

Our QI communication protocol is vulnerable to *active* eavesdropping, in which Eve shines her own light into Bob's terminal and decodes what comes back from him. We recognized that vulnerability in [8], where we suggested that: (1) Alice and Bob should monitor the physical integrity of their communication channels, e.g., with OTDRs if they are communicating via fiber links; (2) Bob should check that the received power level and frequency distribution at his terminal are what he expects; and (3) Alice should verify that the bit-error probability at her terminal is what she expects. Later [22], we analyzed these suggestions for reducing active-eavesdropping vulnerability, showing that an appreciable gap between Alice and Eve's bit-error probabilities could be created, but not nearly as much as what we have shown for defeating passive eavesdropping. In this section we will introduce a more effective procedure for thwarting active eavesdropping, one which relies on basis encoding together with power monitoring. The one aspect of our prior work regarding active eavesdropping that we will retain is the following. Bob will use optical filtering to preclude Eve's attacking him with illumination wavelengths outside the band employed by Alice.

The new setup is shown in Fig. 8. The changes from Fig. 1 are in Bob's modulator and Alice's receiver. Alice and Bob have agreed in advance on the following B choices for the BPSK phase-shifts that he will employ to represent his $k = 0$ or 1 bit values: for $0 \le b \le B-1$, Bob will use

$$\theta_k^{(b)} = \begin{cases} (4b+1)\pi/2B, & \text{for } k = 0 \\ [\theta_0^{(b)} + \pi]\text{modulo}(2\pi), & \text{for } k = 1, \end{cases} \tag{17}$$

where $B > 1$ is an odd integer.[16] Figure 9 shows the $\{\theta_k^{(b)}\}$ for $B = 5$.

Bob transmits his nth bit to Alice using basis b_n, which he draws from the pseudorandom sequence, $\{b_n : 0 \le b_n \le B-1\}$, that he and Alice have shared

[13] Because the idler is now detected immediately, rather than stored in a fiber, $\kappa = 0.9$ can be used, representing a coupling efficiency from the SPDC source to the homodyne detector.

[14] The upper bound on the bit-error rate for an individual homodyne detector—from which a lower bound on Alice and Bob's Shannon information is obtained—is derived in Appendix A. The derivation of the upper bound on Eve's Holevo information is the same as previously described.

[15] One could also carp that the coupling efficiencies in Table 1 need to be augmented to account for the coupling efficiencies of the DWDMs that are employed.

[16] The $\{\theta_k^{(b)}\}$ are thus a version of Yuen's alpha-eta scheme [23].

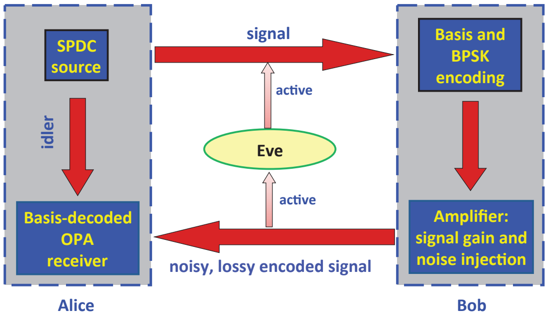
SPDC source
idler
Basis-decoded OPA receiver
Alice
signal
active
Eve
active
noisy, lossy encoded signal
Basis and BPSK encoding
Amplifier: signal gain and noise injection
Bob

Fig. 8 Setup for thwarting active eavesdropping by means of quantum illumination with basis encoding. SPDC: spontaneous parametric downconversion. BPSK: binary phase-shift keying. OPA: optical parametric amplifier.

in advance. Ideally, the $\{b_n\}$ would be a truly random sequence, constructed from a shared one-time pad, but Alice and Bob will need $\log_2(B) > 1$ bits of one-time pad for each bit Bob wants to send, rendering that ideal approach infeasible. On the other hand, because our QI protocol runs at very high rates, Alice and Bob can use a conventional cryptosystem—say the Advanced Encryption Standard (AES)—which they rekey very frequently. Note that our original QI protocol already requires Alice and Bob to have an initial shared secret, which they use to authenticate each other, i.e., to preclude Eve's mounting an impersonation or man-in-the-middle attack.[17] Thus in augmenting our QI protocol with basis encoding, we can assume that the initial portion of the $\{b_n\}$ sequence is a shared random key. In what follows we will be optimistic, and assume that the $\{b_n\}$ can be modeled as statistically independent, uniformly distributed random variables whose values are known to Alice but not to Eve. Alice then has no difficulty decoding Bob's message: she knows the $\{b_n\}$ sequence, so she uses her own phase modulator to convert the $\{\theta_k^{(b_n)}\}$ basis for the nth bit into the $\{0, \pi\}$ basis prior to parametric amplification. Hence Alice's bit-error probability and Alice and Bob's Shannon information are unchanged from what we have presented above, except for any insertion loss of Alice and Bob's phase modulators. Eve's situation is more complicated.

When Alice and Bob do not employ basis encoding—and do not even take steps to detect the presence of an active eavesdropper—the best active-eavesdropping attack we know of has Eve injecting signal light from her own downconverter into Bob, and using her own OPA receiver to decode his message bits from her retained idler and the light she has tapped from the Bob-to-Alice channel. Basis encoding prevents Eve from exploiting that approach, because OPA reception is only optimally sensitive to one basis at a time, and if she divides her retained and returned light between B OPA receivers—to cover all the bases—her performance degrades rapidly with increasing B. Consequently, we will assume that Eve illuminates Bob's terminal with cw coherent-state (laser) light. Note that unless Eve can employ spread-spectrum modulation to match the ∼THz bandwidth of Alice's SPDC source, the high brightness of Eve's illumination should be easily detected

[17] This authentication requirement is no different from what is needed in QKD protocols.

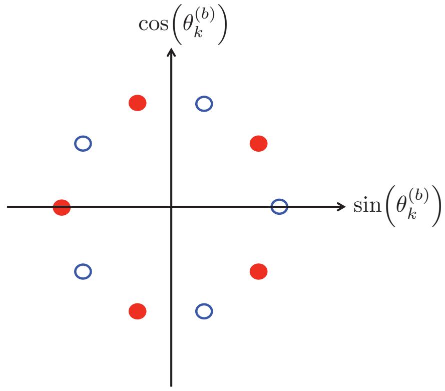
$\cos\left(\theta_k^{(b)}\right)$
$\sin\left(\theta_k^{(b)}\right)$

Fig. 9 Bob's phase shifts, $\{\theta_k^{(b)} : k = 0, 1, \text{ and } 0 \le b \le B-1\}$, for $B = 5$. Open circles are for $k = 0$, filled circles are for $k = 1$.

by Bob, as we will discuss later. Eve's best receiver—with an explicit realization—uses optical heterodyne detection. Furthermore, because we have been unable to evaluate Eve's Holevo information—or obtain a sufficiently tight upper bound on it—we will confine our information-advantage analysis to an individual attack, by restricting our attention to the difference between the Alice and Bob's Shannon information and Eve's. For this initial active-eavesdropping analysis, we will return to an idealized scenario in which the only losses present are those due to propagation through the $\kappa = 0.1$ fibers connecting Alice and Bob, and Eve collects all the light lost in propagation from Bob to Alice. (Because she is injecting her own light into the Alice-to-Bob channel, the amount of Alice's light that she could collect from that fiber is irrelevant here.)

Figure 10(a) compares the bit-error probability bounds for Alice's OPA receiver (assuming a $W = 2\,\text{THz}$ phase-matching bandwidth and an $R = 100\,\text{Mbps}$ modulation rate) and Eve's heterodyne receiver when $B = 7$ basis encoding is used and there is an active-eavesdropping attack. (See Appendix B for derivations of the bounds on $\Pr(e)_{\text{Eve}}$.) The curves are plotted versus N_{in}, the average photon-number per bit that either Alice or Eve deliver to Bob's terminal:

$$N_{\text{in}} = \begin{cases} WN_S\kappa/R, & \text{for Alice} \\ N_E(1-\kappa), & \text{for Eve,} \end{cases} \tag{18}$$

where N_E is the average photon-number per bit emitted by Eve's laser. We see that the Bhattacharyya upper bound on $\Pr(e)_{\text{Alice}}$ is orders of magnitude below the lower bound on the error probability for Eve's heterodyne receiver when $N_{\text{in}} \ge 3$.

Figure 10(b) plots the lower bound on Alice and Bob's Shannon information that follows from $\Pr(e)_{\text{Alice}}^{\text{UB}}$ in Fig. 10(a), the upper bound on Eve's Shannon information that follows from that figure's $\Pr(e)_{\text{Eve}}^{\text{LB}}$, and the lower bound on Alice and Bob's information advantage, $\Delta I_{AB}^{\text{LB}} = I_{AB}^{\text{LB}} - I_E^{\text{UB}}$. We see that an information advantage as high as 0.98 bits/channel-use is obtainable in this idealized scenario, i.e., as much as 98 Mbps for our $R = 100\,\text{Mbps}$ modulation rate.

There is something implicit in the remarks we have just made about Fig. 10 that must be made explicit. Our comments above are, of course, correct if Alice

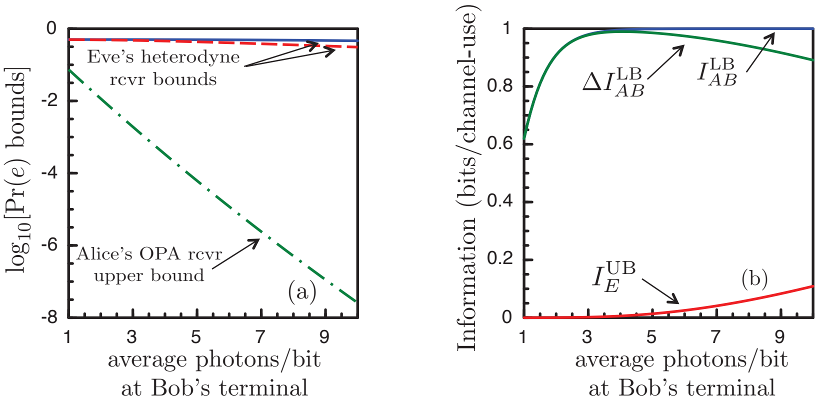

Fig. 10 (a) Bit-error probability bounds for operation with $B = 7$ basis encoding and active eavesdropping. Solid curve: Chernoff bound for Eve's heterodyne receiver. Dashed curve: lower bound for Eve's heterodyne receiver. Dot-dashed curve: Bhattacharyya bound for Alice's OPA receiver with $G_A = 1+N_S/\sqrt{\kappa N_B}$. (b) Lower bound on Alice and Bob's Shannon information, $I_{AB}^{\rm LB}$; upper bound on Eve's Shannon information, $I_E^{\rm UB}$; and lower bound on Alice and Eve's information advantage, $\Delta I_{AB}^{\rm LB}$. (Note that $I_{AB}^{\rm LB}$ lies almost directly under $\Delta I_{AB}^{\rm LB}$ until it asymptotes at $I_{AB}^{\rm LB} = 1$.) The curves in (a) and (b) are plotted versus the average photon-number per bit that Alice and Eve individually deliver to Bob's terminal. All curves assume the only losses in the system are due to propagation through the $\kappa = 0.1$ fibers connecting Alice and Bob. Alice's performance assumes a 2 THz phase-matching bandwidth and a 100 Mbps modulation rate.

and Eve are constrained to keep their $N_{\rm in}$ values in the range $1 \le N_{\rm in} \le 5$. That is certainly not a problem for Alice; her bit-error probability and Shannon information are already at excellent values below $N_{\rm in} = 5$. But Eve has no reason to be so constrained unless Alice and Bob can force her to comply. Here is where Bob's power monitoring comes in. Suppose Alice operates at $N_{\rm in} = 4$. By diverting a small fraction—say 5%—of the light he receives at his terminal's input to a power monitor, Bob can estimate $N_{\rm in}$ and abort communication when he senses $N_{\rm in} \ge 5$. In particular, if his power monitor is a high-efficiency, shot-noise limited detector with a 0.4 μs integration time—corresponding to 400 bits at the 100 Mbps modulation rate—then $N_{\rm in} = 5$ is sufficient to yield a 20 dB signal-to-noise ratio with 5% power diversion. Unless Eve attenuates Alice's light while injecting her own, Bob's power monitor will force Eve to keep her $N_{\rm in} < 1$, at which point her Holevo information would be at most 7.4×10^{-5} bits/channel-use. In fact, in this scenario Bob would have an easier time constraining Eve to $N_{\rm in} < 1$, because her $N_{\rm in} = 1$ laser signal with 40 GHz spread-spectrum modulation will be 11 dB brighter than Alice's $N_{\rm in} = 4$ signal with 2 THz bandwidth.[18] Eve could cut the Alice-to-Bob connection, to maximize the light she can inject into Bob, but $N_{\rm in} = 5$ will give her at most 0.014 bits/channel-use about Bob's message, and cutting the

[18] Note that Fig. 10 applies even if Eve could use spread spectrum over the full 2 THz optical bandwidth of Bob's terminal. Also note that Alice and Bob could increase the number of bases they employ, leading to an increase in the power that Eve must inject to glean information from her active attack, and thus reducing the amount of time Bob needs to detect her intrusion with his power monitor.

Alice-to-Bob fiber will quickly be detected by Alice in that she will no longer be receiving meaningful data, even if Eve attempts an impersonation attack.

6 Conclusions

At this point we have accomplished the objectives laid out in our introduction. In Sect. 2 we reviewed the quantum illumination protocol that is immune to passive eavesdropping, extending its initial analysis [8], which only addressed Alice and Bob's bit-error probability advantage, to include their information advantage over a passive eavesdropper's collective attack. For the idealized scenario considered therein, that information advantage could exceed 0.88 bits/channel-use, equaling more than 100 Mbps at the modulation rate giving that bits/channel-use value with the assumed 1 THz phase-matching bandwidth. In Sect. 3 we reviewed our proof-of-principle experiment [9] that validated the theory from [8], and introduced the system nonidealities that the earlier theory paper had neglected. In Sect. 4 we made an initial attempt at pushing Alice and Bob's information advantage to the Gbps regime while including realistic to aggressive values for system parameters. With future development of very large WSi SNSPD arrays, Gbps advantages might be possible over 20-km-long fiber connections. Alternatively, a DWDM architecture might deliver similar capability in a 40-channel system. Finally, in Sect. 5, we introduced a new approach to thwarting active eavesdropping: combining alpha-eta basis encoding with power monitoring at Bob's terminal. So far, this scheme relies on a pseudorandom sequence to choose the basis for each successive bit transmitted by Bob, and so it lacks the assurance that its security rests on fully quantum-mechanical principles. Nevertheless, there is some possibility that quantum data-locking might provide stronger assurance than what we have already demonstrated, cf. the recent works on quantum enigma machines and data-locking capacity [25, 26].

Going forward there is much to be done on QI-based secure communication with passive-eavesdropping immunity. On the system analysis front, the full-range of parameter optimization—which we have not done—should be performed to determine the best operating point for high-rate, high-security operation and to delineate the limit on the secure-rate×distance figure of merit. On the experimental side, high data-rate long-distance operation should be demonstrated with or without DWDM. For active eavesdropping, further analysis of our basis-encoded scheme might lead to an understanding of vulnerability to a collective attack, although that would implicitly assume truly-random basis selection, as we did in Sect. 5 for Eve's individual attack. Here, enigma-machine theory might provide some security assurance without that unwarranted assumption. In addition, an experiment to demonstrate the effectiveness of basis-encoding protection would be worth doing.

Finally, we might forego fiber links in favor of operation over line-of-sight paths through the atmosphere. The QI system would obviously fail when clouds or fog obscure the path, and random refractive-index fluctuations known as atmospheric turbulence would have to be contended with in clear weather.[19] The additional

[19] See [27,28] for the effects of turbulence on the sift and error probabilities of Bennett-Brassard 1984 QKD, and [29,30] for an assessment of the ultimate quantum limits on optical communication through turbulence at high photon and spectral efficiencies.

adaptive optics that might be needed to compensate for many of the ill-effects of atmospheric turbulence will be added implementation burden. But Alice and Bob's ability to observe their propagation paths, and control their telescopes' fields of view, could make it highly difficult for Eve to accomplish active eavesdropping. Furthermore, there are many interesting applications—especially those involving mobile platforms—where fiber connections will never be available but line-of-sight paths are available. It is therefore of considerable importance to understand how our QI communication protocol might work in such scenarios.

Appendix A

Here we shall derive the bit-error rate for a single channel of the homodyne receiver that Alice uses in the QI-DWDM setup from Sect. 4. We will assume $R_c \ll W_c$. Then, given the value, k, of Bob's message bit, the outputs from Alice's idler and returned-light homodyne detectors during the $T_c = 1/R_c$ duration bit interval can be regarded as a set of $M_c = W_c/R_c$ statistically independent, identically distributed, zero-mean, 2-D Gaussian random-vector modes $\{\mathbf{x}_m : 1 \leq m \leq M_c\}$[20] with common covariance matrix

$$\Lambda_0^{\text{hom}} = \frac{1}{4}\begin{bmatrix} 2N_{R_S}+1 & C_{R_SR_I} \\ C_{R_SR_I} & 2N_{R_I}+1 \end{bmatrix} \tag{19}$$

when $k = 0$, and

$$\Lambda_1^{\text{hom}} = \frac{1}{4}\begin{bmatrix} 2N_{R_S}+1 & -C_{R_SR_I} \\ -C_{R_SR_I} & 2N_{R_I}+1 \end{bmatrix} \tag{20}$$

when $k = 1$. In these expressions:

$$N_{R_S} = \kappa_d\kappa'_A\kappa_2\kappa'_B(G_B\kappa_B\kappa_1\kappa_A N_S + N_B), \tag{21}$$

$$N_{R_I} = \kappa_d\kappa_I N_S, \tag{22}$$

and

$$C_{R_SR_I} = 2\kappa_d\sqrt{\kappa'_A\kappa_2\kappa'_B G_B\kappa_B\kappa_1\kappa_A\kappa_I N_S(N_S+1)}. \tag{23}$$

When Bob's message bits are equally-likely to be 0 or 1, the minimum error-probability decision rule reduces to the following threshold test:

$$\sum_{m=1}^{M_c} x_{m_R}x_{m_I} \underset{\text{decide 1}}{\overset{\text{decide 0}}{\gtrless}} 0. \tag{24}$$

[20] The two components of $\mathbf{x}_m$ are the outputs from the returned-light and idler homodyne detectors for the mth mode: $\mathbf{x}_m = \begin{bmatrix} x_{m_R} & x_{m_I} \end{bmatrix}^T$.

The upper bound on Alice's bit-error probability that we used in Sect. 4 is the Bhattacharyya bound,

$$\Pr(e)^{\mathrm{UB}}_{\mathrm{Alice}} \leq \frac{1}{2}\left[\int d\mathbf{x}\,\sqrt{\frac{\exp\left[-\frac{1}{2}\mathbf{x}^T(\varLambda_0^{-1}+\varLambda_1^{-1})\mathbf{x}\right]}{2\pi|\varLambda_0|^{1/2}|\varLambda_1|^{1/2}}}\,\right]^{M_c} \tag{25}$$

$$= \frac{1}{2}\left(\sqrt{1-\frac{C^2_{R_SR_I}}{(2N_{R_S}+1)(2N_{R_I}+1)}}\right)^{M_c}. \tag{26}$$

Appendix B

Here we show how the bit-error probability bounds for Eve's heterodyne receiver, plotted in Fig. 10(a), were obtained. The upper bound is a Chernoff bound,[21]

$$\Pr(e)^{\mathrm{UB}}_{\mathrm{Eve}} = \frac{1}{2}\int d\mathbf{x}\,\sqrt{p(\mathbf{x}\mid 0)p(\mathbf{x}\mid 1)}, \tag{27}$$

and the lower bound is

$$\Pr(e)^{\mathrm{LB}}_{\mathrm{Eve}} = \frac{1-\sqrt{1-\left(\int d\mathbf{x}\,\sqrt{p(\mathbf{x}\mid 0)p(\mathbf{x}\mid 1)}\right)^2}}{2}, \tag{28}$$

where $p(\mathbf{x} \mid k)$ for $k = 0, 1$ is the conditional probability density function for the normalized, complex-valued output $\mathbf{x}$ from bit-interval matched filtering of Eve's heterodyne photocurrent.[22] For our basis-encoded system, Eve's conditional probability densities are

$$p(\mathbf{x}\mid k) = \sum_{b=1}^{B-1}\frac{\exp\left(-\left|\mathbf{x}-(-1)^k\sqrt{(1-\kappa)N_{\mathrm{in}}}\,e^{i\theta_k^{(b)}}\right|^2/(1-\kappa)N_B\right)}{B\pi(1-\kappa)N_B}, \text{ for } k=0,1. \tag{29}$$

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography, public key distribution, and coin tossing. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984. pp. 175–179. IEEE, New York (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67,** 661–663 (1991)
3. Grosshans F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88,** 057902 (2002)
4. Peev, M., *et al.*: The SECOQC quantum key distribution network in Vienna. New J.Phys. **11,** 075001 (2009)
5. Sasaki, M., *et al.*: Field test of quantum key distribution in the Tokyo QKD network. Opt. Express **19,** 10387–10409 (2011)

[21] The symmetry of the $\{\theta_k^{(b)}\}$ make the Chernoff and Bhattacharyya bounds coincide.

[22] In other words, the real and imaginary parts of $\mathbf{x}$ are the in-phase (I) and quadrature (Q) components of standard coherent communications.

6. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28,** 656–715 (1949)
7. Gallager, R.G.: Information Theory and Reliable Communication. chap. 3. Wiley, New York (1968)
8. Shapiro, J.H.: Defeating passive eavesdropping with quantum illumination. Phys. Rev. A **80,** 022320 (2009)
9. Zhang, Z., Tengner, M., Zhong, T., Wong, F. N. C., and Shapiro, J. H.: Entanglement's benefit survives an entanglement-breaking channel. Phys. Rev. Lett. **111,** 010501 (2013)
10. Lloyd, S.: Enhanced sensitivity of photodetection via quantum illumination. Science **321,** 1463–1465 (2008)
11. Tan, S.-H., Erkmen, B. I., Giovannetti, V., Guha, S., Lloyd, S., Maccone, L., Pirandola, S., Shapiro, J. H.: Quantum illumination with Gaussian states. Phys. Rev. Lett. **101**, 253601 (2008)
12. Guha, S., Erkmen, B. I.: Gaussian-state quantum-illumination receivers for target detection. Phys. Rev. A **80,** 052310 (2009)
13. Louisell, W.: Radiation and Noise in Quantum Electronics. chap. 7. McGraw-Hill, New York (1964)
14. Audenaert, K. M. R., Calsamiglia, J., Muñoz-Tapia, R., Bagan, E., Masanes, Ll., Acin, A., Verstraete, V.: Discriminating states: The quantum Chernoff bound. Phys. Rev. Lett. **98,** 160501 (2007)
15. Calsamiglia, J., Muñoz-Tapia, R., Masanes, Ll., Acin, A., Bagan, E.: Quantum Chernoff bound as a measure of distinguishability between density matrices: Application to qubit and Gaussian states. Phys. Rev. A **77,** 032311 (2008)
16. Pirandola, S., Lloyd, S.: Computable bounds for the discrimination of Gaussian states. Phys. Rev. A **78,** 012331 (2008)
17. Zhang, Z., Tengner, M., Zhong, T., Wong, F. N. C., Shapiro, J. H.: Supplemental Material for Phys Rev. Lett. **111,** 010501 (2013). http://link.aps.org/supplemental/10.1103/PhysRevLett.111.010501
18. Nair, R.: Discriminating quantum-optical beam-splitter channels with number-diagonal signal states: Applications to quantum reading and target detection. Phys. Rev. A **84,** 032312 (2011)
19. Marsili, F., Verma, V. B., Stern, J. A., Harrington, S., Lita, A. E., Gerrits, T., Vayshenker, I., Baek, B., Shaw, M. D., Mirin, R. P., Nam, S. W.: Detecting single infrared photons with 93% system efficiency. Nature Photon. **7,** 210–214 (2013)
20. Rosenberg, D., Kerman, A. J., Molnar, R. J., Dauler, E. A.: High-speed and high-efficiency superconducting nanowire single photon detector array. Opt. Express **21,** 1440–1447 (2013)
21. Bower, P., Dedic, I.: High speed converters and DSP for 100G and beyond. Optical Fiber Technol. **17,** 464–471 (2011)
22. Xu, W., Shapiro, J. H.: Defeating active eavesdropping with quantum illumination. in Quantum Communication Measurement and Computing (QCMC). Ralph, T., Lam, P. K., eds. AIP Conf. Proc. No. 1363. AIP, New York (2011)
23. Barbosa, G. A., Corndorf, E., Kumar, P., Yuen, H. P.: Secure communication using mesoscopic states. Phys. Rev. Lett. **90,** 227901 (2003)
24. Stinson, D. R.: Cryptography: Theory and Practice. Chapman and Hall, Boca Raton (2006)
25. Lloyd, S.: Quantum enigma machines. arXiv:1307.0380 [quant-ph]
26. Guha, S., Hayden, P., Krovi, H., Lloyd, S., Lupo, C., Shapiro, J. H., Takeoka, M., Wilde, M. M.: Quantum enigma machines and the locking capacity of a quantum channel. arXiv:1307.5368 [quant-ph]
27. Shapiro, J. H.: Near-field turbulence effects on quantum key distribution. Phys. Rev. A **67,** 022309 (2003)
28. Shapiro, J. H.: Scintillation has minimal impact on far-field Bennett-Brassard 1984 protocol quantum key distribution. Phys. Rev. A **84,** 032340 (2011)
29. Chandrasekaran, N., Shapiro, J. H.: Photon information efficient communication through atmospheric turbulence—Part I: Channel model and propagation statistics. submitted to J. Lightw. Technol.
30. Chandrasekaran, N., Shapiro, J. H., Wang, L.: Photon information efficient communication through atmospheric turbulence—Part II: Bounds on ergodic classical and private capacities. submitted to J. Lightw. Technol.