High-order encoding schemes for floodlight quantum key distribution

Quntao Zhuang,[1,2,*] Zheshen Zhang,[2,†] and Jeffrey H. Shapiro[2]

[1]*Department of Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[2]*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

Floodlight quantum key distribution (FL-QKD) has realized a 1.3 Gbit/s secret-key rate (SKR) over a 10-dB-loss channel against a frequency-domain collective attack [Quantum Sci. Technol. **3**, 025007 (2018)]. It achieved this remarkable SKR by means of binary phase-shift keying (BPSK) of multiple optical modes. Moreover, it did so with available technology, and without space-division or wavelength-division multiplexing. In this paper we explore whether replacing FL-QKD's BPSK modulation with a high-order encoding can further increase that protocol's SKR. First, we show that going to K-ary phase-shift keying with $K = 32$ doubles—from 2.0 to 4.5 Gbit/s—the theoretical prediction from [Phys. Rev. A **94**, 012322 (2016)] for FL-QKD's BPSK SKR on a 50-km-long fiber link. Second, we show that $2d \times 2d$ quadrature amplitude modulation does not offer any SKR improvement beyond what its $d = 1$ case—which is equivalent to quadrature phase-shift keying—provides.

I. INTRODUCTION

Quantum key distribution [1] (QKD) allows remote parties (Alice and Bob) to create a shared random bit string with unconditional security. Later, they can employ their shared string for one-time-pad (OTP) encryption [2] of messages they wish to keep entirely private from any eavesdropper (Eve). Unfortunately, current QKD systems' Mbit/s secret-key rates (SKRs) [3–7] fall far short of what is needed to make high-speed (Gbit/s) transmission with OTP encryption ready for widespread deployment. Floodlight QKD (FL-QKD) [8–10] is a recent protocol that uses binary phase-shift keying (BPSK) of multiple optical modes and homodyne detection to achieve security against the optimum frequency-domain collective attack. Its initial theoretical study [8] predicted that FL-QKD was capable of Gbit/s SKRs at metropolitan-area distances over single-mode fiber (no space-division multiplexing) in a single-wavelength channel (no wavelength-division multiplexing) without the need to develop any new technology. The initial tabletop experimental demonstration of FL-QKD [9] used 100 Mbit/s modulation to realize a 55 Mbit/s SKR over a 10-dB-loss channel (equivalent to 50 km of low-loss fiber) in a setup that was limited by the bandwidth of its electronics. A subsequent tabletop experiment [10], using GHz-bandwidth electronics, attained a 1.3 Gbit/s SKR over a 10-dB-loss channel using a 7 Gbit/s modulation rate

Why is FL-QKD's SKR so much higher than prior state of the art, even when compared at the same collective-attack security level? It is because FL-QKD takes advantage of multimode encoding, whereas the predominant decoy-state BB84 protocol does not [3], and conventional continuous-variable (CV) QKD protocols require single-mode encoding [4]. Moreover,

the SKR advantage over decoy-state BB84 shown in recent D-dimensional QKD experiments [5–7] comes only from mitigating the SKR-limiting effect of single-photon detectors' dead time, i.e., within each time slot of their D-slot symbols these protocols take no advantage of multimode encoding. Thus the SKRs in *bits/s* for prior state-of-the-art systems are constrained to be no more than the ultimate limit on SKR in *bits per mode*, viz., the PLOB bound [11], SKR $\leqslant -\log_2(1 - \eta)$ bits per mode for a channel with transmissivity η. In contrast, FL-QKD's predicted 2 Gbit/s SKR [8] over a 50-km-long fiber link uses 10 Gbit/s BPSK modulation of 200 modes per symbol making its 10^{-3} bits per mode well below the $-\log_2(1 - \eta) = 0.15$ PLOB bound for $\eta = 0.1$, while still affording the Gbit/s SKRs needed for high-speed OTP encryption.

How can we increase FL-QKD's bits per mode SKR, other things being equal, to further enhance its bits/s SKR? Because FL-QKD relies on homodyne detection, there is a potential answer from classical fiber-optic communication, where a similar problem has been confronted in the context of increasing the spectral efficiency (bits/s Hz = bits per mode) for coherent (homodyne or heterodyne) detection systems [12]. For classical communication the answer is to go to a high-order modulation format, e.g., K-ary phase-shift keying (KPSK) or quadrature amplitude modulation (QAM). Therefore, in this paper we will evaluate the merits of FL-QKD's using those formats. We show that KPSK with $K = 32$ doubles—from 2.0 to 4.5 Gbit/s—the theoretical prediction from Ref. [8] for FL-QKD's BPSK SKR on a 50-km-long fiber link, but we find that $2d \times 2d$-symbol QAM does not offer any SKR improvement beyond what its $d = 1$ case—which is equivalent to quadrature phase-shift keying, i.e., 4PSK—provides.

The remainder of the paper is organized as follows. We begin, in Sec. II, by extending the FL-QKD protocol—as presented in Ref. [8] and subsequently realized in Refs. [9,10]—to allow for high-order encoding, using either the KPSK or QAM signal constellations. Next, in Sec. III, we analyze FL-QKD's performance when it employs KPSK with $1 \leqslant \log_2(K) \leqslant 5$ or

---

*quntao@mit.edu
†Present address: Department of Materials Science and Engineering, University of Arizona, Tucson, Arizona 85721, USA.
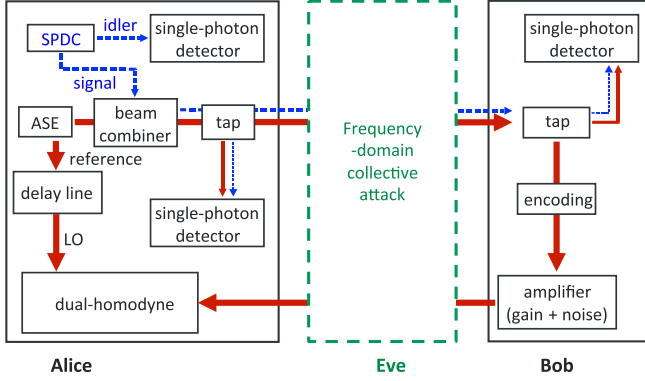
FIG. 1. Quantum channel setup for FL-QKD under frequency-domain collective attack. ASE: amplified spontaneous emission source. SPDC: spontaneous parametric downconverter. LO: local oscillator.
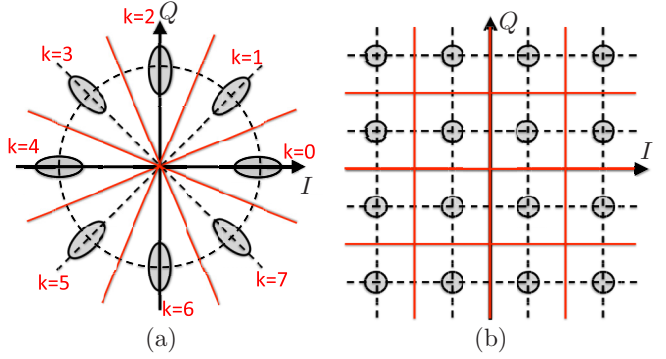

FIG. 2. Signal constellation examples: (a) 8PSK; (b) 4×4 QAM. In both cases the gray shading marks one-standard-deviation regions for Alice's receiver about the $\{\bar{I}_k + i\bar{Q}_k\}$—where $\bar{I}_k + i\bar{Q}_k$ is how Bob's kth transmitted symbol would appear, in a noise-free world, at the output of Alice's dual-homodyne receiver—and the red lines mark the boundaries of her minimum error-probability decision regions. Note that the eccentricity of the elliptical contours shown in (a) originates from the correlation between Alice's LO and the light she receives from Bob. That eccentricity has been exaggerated in (a) to emphasize the rotational symmetry, while in (b) circular contours are shown because, as demonstrated in Appendix B, the contours' eccentricity is negligible for parameter values of interest for FL-QKD.

$2d \times 2d$ square-lattice QAM with $1 \leqslant d \leqslant 4$. We conclude, in Sec. IV, with some discussion and suggestions for future work. Derivation details appear in Appendixes A and B.

II. FL-QKD WITH HIGH-ORDER ENCODING

In FL-QKD with high-order encoding (schematic in Fig. 1), Alice splits the W-Hz bandwidth, flat-top spectrum, high-brightness (many photons per mode) output from an amplified spontaneous emission (ASE) source into a low-brightness ($\ll 1$ photon per mode) signal and a high-brightness reference. To enable channel monitoring, Alice combines her low-brightness ASE with the signal output from a spontaneous parametric down-converter (SPDC)—of the same W-Hz bandwidth flat-top spectrum as the ASE—in an n:1 ASE-to-SPDC ratio with $n \gg 1$. Alice uses a single-photon detector to monitor her SPDC's idler and another single-photon detector to monitor a $\kappa_A \ll 1$ fraction that she taps from her combined ASE-SPDC light, while sending the remainder of that light—whose brightness is $N_S \ll 1$ photon per mode—to Bob. Alice retains her bright reference beam in an optical-fiber delay line—using amplifiers as needed—for use as her dual-homodyne receiver's high-brightness ($N_{LO} \gg 1$ photons per mode) local oscillator (LO).

In the absence of Eve, the fiber link from Alice to Bob is a pure-loss channel with transmissivity $\kappa_S \ll 1$. Eve's presence, however, allows her to control that channel; hence Alice and Bob must perform channel monitoring to bound Eve's information gain. So, prior to his encoding operation, Bob taps a small fraction $\kappa_B \ll 1$ of the light he receives and sends it to a single-photon detector. The outputs from Alice and Bob's single-photon detectors enable them to determine the singles' rates S_I for Alice's idler and S_A (S_B) for Alice's (Bob's) tap, as well as C_{IA} (C_{IB}) and $\tilde{C}_{IA}$ ($\tilde{C}_{IB}$) the time-aligned and time-shifted coincidence rates between Alice's idler and Alice's (Bob's) tap. They use their measurements to (1) verify that Bob receives the photon flux he would get were Eve absent and (2) determine Eve's intrusion parameter, f_E, from [8]

$$f_E = 1 - [(C_{IB} - \tilde{C}_{IB})/S_B]/[(C_{IA} - \tilde{C}_{IA})/S_A]. \quad (1)$$

Alice and Bob's knowing Eve's intrusion parameter quantifies the integrity of the Alice-to-Bob channel and allows them to place an upper bound on Eve's Holevo-information rate for her optimum frequency-domain collective attack. Eve can realize that optimum attack in the form of an SPDC light-injection attack [8], in which case f_E is the fraction of the light entering Bob's terminal that comes from Eve.

To complete his part of the FL-QKD protocol, Bob first takes the light not routed to his channel monitor's single-photon detector and modulates it with a random symbol selected from his signal constellation at an $R = 1/T$ baud symbol rate. In Refs. [8–10], that constellation was BPSK, i.e., Bob randomly applied a 0 rad or π rad phase shift. In the present work, Bob will employ either a KPSK or a square-lattice QAM constellation, as shown in Figs. 2(a) and 2(b), respectively, and detailed in Sec. III. These encodings are easily imposed on the ASE light that Bob receives from Alice by means of commercially available electro-optic modulators, cf. the 7 Gbit/s BPSK modulation applied to 2.24-THz-bandwidth ASE light in the FL-QKD experiment reported in Ref. [10].

After his encoding, Bob amplifies his modulated light with a gain $G_B \gg 1$ quantum-limited amplifier whose output ASE has brightness $N_B = G_B - 1$, and sends the modulated and amplified light back to Alice through what, in Eve's absence, is a κ_S-transmissivity fiber. The amplifier's gain will overcome the return-path loss insofar as Alice is concerned, thus making FL-QKD's performance only subject to one-way path loss, despite its being a two-way protocol. Furthermore, the amplifier's ASE will mask Bob's modulation from Eve's passive (listening only) attack. Indeed, Alice's transmitting low-brightness ($N_S \ll 1$) light to Bob precludes Eve's deriving a sufficiently good broadband phase reference—from light she taps from the Alice-to-Bob channel—for retrieving Bob's symbol stream from his noisy transmission to Alice [13]. On

the other hand, Alice's high-brightness ($N_{LO} \gg 1$) broadband LO beam enables her to reliably recover Bob's symbols.

To decode Bob's symbols, Alice uses dual-homodyne reception, i.e., she 50:50 beam splits both the light returned from Bob and her LO, and then makes homodyne measurements of the I (0 rad LO phase shift) and Q ($\pi/2$ rad LO phase shift) in-phase and quadrature components of the returned light, as in classical KPSK or QAM fiber-optic communications. Following Alice's minimum error-probability decoding of Bob's symbol stream from her measured sequence of $I + iQ$ values, Alice and Bob complete the FL-QKD protocol with the usual key reconciliation and privacy amplification steps, using an authenticated classical communication channel.

III. SECRET KEY RATES

Our route to determining FL-QKD's performance when it employs KPSK or QAM parallels what was done in Ref. [8] for FL-QKD using BPSK: we obtain a lower bound on the SKR from

$$\text{SKR}_{\text{LB}} = \beta I_{AB} - \chi_{EB}^{\text{UB}}. \tag{2}$$

Here (1) β is Alice and Bob's reconciliation efficiency; I_{AB} is Alice and Bob's bits/s Shannon-information rate, which they calculate from their measured conditional probability distribution—obtained during reconciliation—for Alice's decoded symbol given Bob's encoded symbol; and (2) χ_{EB}^{UB} is an upper bound on Eve's bits/s Holevo-information rate, which Alice and Bob calculate from their channel monitors' f_E measurement. Also, we are assuming that (1) Eve mounts an SPDC light-injection attack—which, see below, realizes her optimum frequency-domain collective attack on KPSK—with $f_E = 0.01$ intrusion parameter and (2) SKR_{LB} is sufficiently high that a typical QKD session will push deep into the asymptotic regime, i.e., no finite-key correction is needed. Note that I_{AB} does not achieve the Holevo capacity for classical information transmission from Bob to Alice, even in the absence of Eve. That capacity is achieved by Bob's encoding with an ensemble of Gaussian-distributed coherent states and Alice decoding with a joint-detection receiver [14]. Our interest, however, is in high-SKR QKD when Eve may be attacking the quantum channel. Hence we have chosen to use the principal high-order encodings employed in fiber-optic communications. As will be seen below, however, the SKR gains we obtain with these high-order encodings fall far short of what they afford in conventional fiber-optic communications.

The subsections that follow evaluate SKR_{LB} for FL-QKD with KPSK and QAM using the same parameter values that Ref. [8] assumed, thus enabling direct comparisons of FL-QKD's performance using these high-order encodings to the protocol's performance with its original BPSK encoding. These parameter values are as follows. (1) Alice's ASE and SPDC sources operate at 1550 nm wavelength and have $W = 2$ THz bandwidth. (2) Alice's transmission to Bob has a 99:1 ASE-to-SPDC ratio, and its brightness, N_S, is chosen, for each propagation distance, to maximize SKR_{LB}. (3) Alice and Bob are connected by L-km-long single-mode fibers with 0.2 dB/km loss. (4) Alice and Bob use 1% taps for their channel monitors. (5) Bob's symbol rate is $R = 10$ Gbaud ($T = 0.1$ ns symbol duration) [15]. (6) Bob's amplifier has gain $G_B = 10^4$.

(6) Alice's LO is undegraded with brightness $N_{LO} = 10^4$ and her receiver has an $\eta = 0.9$ homodyne efficiency. (7) Alice and Bob's reconciliation efficiency is $\beta = 0.94$.

Before proceeding to our SKR_{LB} evaluations, there is an important point to make about Alice's homodyne-measurement statistics. With our assumed $T = 0.1$ ns symbol duration and $W = 2$ THz source bandwidth, there are $M = TW = 200$ modes per symbol in Bob's transmission to Alice. In this $M \gg 1$ regime, the central limit theorem implies that Alice's I and Q values for each received symbol are jointly Gaussian random variables given the value of Bob's transmitted symbol. Furthermore, the means, variances, and covariance of I and Q—which fully characterize their joint conditional distribution—can be obtained from the value of the transmitted symbol and the conditional covariance matrix of the return and reference beams' M independent identically distributed (iid) return-LO mode pairs.

A. FL-QKD performance with KPSK encoding

In FL-QKD with KSPK encoding, Bob applies a $2\pi k/K$ rad phase shift to the light remaining after his monitor tap, where k (his symbol to be encoded) is equally likely to be any integer between zero and $K - 1$. As a result, given Bob's transmitted symbol k, the joint distribution for Alice's I and Q has the rotational symmetry shown in Fig. 2(a). Specifically, $p(I, Q \mid k)$ is a Gaussian, whose mean $\langle I + iQ \rangle = \bar{I}_k + i\bar{Q}_k$ has phase angle $2\pi k/K$ and a k-independent magnitude, and whose covariance matrix is such that

$$\tilde{I}_k \equiv I \cos(2\pi k/K) + Q \sin(2\pi k/K), \tag{3}$$

$$\tilde{Q}_k \equiv -I \sin(2\pi k/K) + Q \cos(2\pi k/K) \tag{4}$$

are statistically independent with k-independent variances $\sigma_{\tilde{I}}^2 > \sigma_{\tilde{Q}}^2$. (See Appendix A for the details.)

The preceding statistics make it easy to determine Alice's minimum error-probability rule for decoding Bob's transmitted symbol from her $I + iQ$ measurement. Because Bob sends each possible symbol with equal probability, the minimum error-probability rule reduces to making a maximum-likelihood decision as to which symbol was sent [16]. Because the conditional statistics of I and Q are Gaussian and rotationally symmetric, the maximum-likelihood decision rule is minimum-distance decoding: Alice decodes her measured $I + iQ$ as the symbol whose $\bar{I}_k + i\bar{Q}_k$ is closest to that measured value. As shown in Fig. 2(a), this means that the decision region, $\mathcal{D}_k$, in the $I + iQ$ plane wherein Alice decodes symbol k is

$$\mathcal{D}_k = \{I + iQ : -\pi k/K \leqslant \theta < \pi k/K\}, \tag{5}$$

where $|I + iQ|e^{i\theta}$ is the polar-coordinate form of $I + iQ$.

Using the $\{\mathcal{D}_k\}$, together with the equiprobable nature of Bob's encoding and the jointly Gaussian conditional distributions $\{p(I, Q \mid k)\}$, we can numerically evaluate the conditional probabilities $\Pr(\tilde{k} \mid k)$ for Alice to decode her $I + iQ$ value as $\tilde{k}$, given that Bob sent symbol k, via

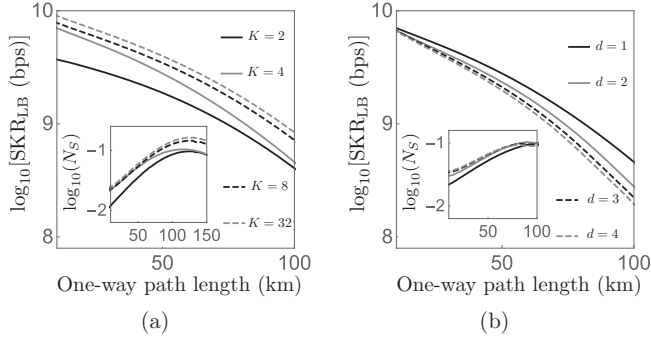$$\Pr(\tilde{k} \mid k) = \int \int_{\mathcal{D}_{\tilde{k}}} dI \, dQ \, p(I, Q \mid k). \tag{6}$$

FIG. 3. SKR lower bounds for FL-QKD vs one-way path length L, with insets showing the optimized brightness N_S of Alice's transmission to Bob. The assumed parameter values are given in the text. (a) SKR_{LB} with KPSK for $1 \leqslant \log_2(K) \leqslant 5$. (b) SKR_{LB} with $2d \times 2d$ square-lattice QAM for $1 \leqslant d \leqslant 4$.

Alice and Bob's Shannon-information rate then follows from

$$I_{AB} = R \left\{ \sum_{k=0}^{K-1} \sum_{\tilde{k}=0}^{K-1} \frac{\Pr(\tilde{k} \mid k)}{K} \log_2 \left[\frac{K \Pr(\tilde{k} \mid k)}{\sum_{k'=0}^{K-1} \Pr(\tilde{k} \mid k')} \right] \right\}. \tag{7}$$

At this point, we can obtain SKR_{LB} from Eq. (2) once we have an upper bound on Eve's Holevo-information rate, χ_{EB}^{UB}, when she mounts an SPDC light-injection attack. In that attack, Eve injects signal light from her own W-Hz bandwidth, flat-top spectrum, low-brightness SPDC source into the Alice-to-Bob channel, so that it will get modulated and amplified by Bob and then transmitted on the Bob-to-Alice channel. Eve also stores her SPDC source's idler light for use as a reference and then—making use of that reference, plus the light she has tapped from the Alice-to-Bob channel, and the light she taps from the Bob-to-Alice channel—Eve makes the collective quantum measurement that maximizes her Holevo-information rate.

In Ref. [8] it was shown that Eve's SPDC light-injection attack realizes her optimum frequency-domain collective attack when Bob uses BPSK encoding. It turns out that this is still true when Bob uses KPSK encoding, because KPSK's signal constellation is rotationally symmetric. This makes Eve's conditional state, given Bob transmits symbol k, a Gaussian state with a k-independent von Neumann entropy. It also makes her unconditional state identical to what prevails when Bob uses BPSK. Consequently, applying the χ_{EB}^{UB} derivation from Ref. [8]'s Appendix C to FL-QKD with KPSK requires only that in the final χ_{EB}^{UB} formula—Eq. (C56) of that Appendix—the maximum allowable value for χ_{EB}^{UB} be increased from $R \log_2(2) = R$ to $R \log_2(K)$, i.e.,

$$\chi_{EB}^{\text{UB}} = R \min\{M \kappa_S N_S [f_E / \ln(2) - f_E \log_2(f_E \kappa_S N_S) + (1 - f_E) N_S \log_2(1 + 1/N_S)], \log_2(K)\}. \tag{8}$$

This result omits $O(\kappa_S^{3/2})$ and $O(N_B^{-1/2})$ terms that were included in our numerical evaluations but are too long to display here.

Figure 3(a) plots KPSK's SKR_{LB} versus one-way path length L for $1 \leqslant \log_2 K \leqslant 5$ when, for each L value, Alice's source brightness N_S is chosen to maximize SKR_{LB} and

the other system parameters as given earlier in this section, i.e., they are the same as those employed in Ref. [8]. We see that at 50 km path length going from BSPK to 32PSK increases the SKR from 2 Gbit/s to 4.5 Gbit/s. The inset in Fig. 3(a) plots the optimized N_S versus L. As required to defeat Eve's passive eavesdropping attack on BPSK [8,10,13], we see that $N_S \ll 1$ prevails at all distances shown for that case. Somewhat higher brightnesses—but still satisfying $N_S < 1$ at all distances—are optimum as K increases, because Eve's decoding a higher-order KPSK requires her to have a higher-quality phase reference, something that is still inaccessible to her at those N_S values. As an interesting side note, we point out that the convergence with increasing L of Fig. 3(a)'s SKR_{LB} 4PSK curve to its BPSK curve—a behavior that can be shown analytically—is due to the resulting decrease in Alice's signal-to-noise ratio and the structure of those two signal sets.

B. FL-QKD performance with QAM encoding

In FL-QKD with $2d \times 2d$ square-lattice QAM, Bob first selects a symbol from $0 \leqslant k \leqslant K_q - 1 \equiv 4d^2 - 1$ in an equiprobable manner. He then intensity and phase modulates the light remaining after his channel-monitor tap to encode that symbol so that, in a noise-free world, it would appear as $\bar{I}_k + i\bar{Q}_k$—the center of the kth gray-shaded region in Fig. 2(b)—at the output of Alice's dual-homodyne receiver [17].

Our first task is to use the Gaussian approximation for Alice's I and Q values' conditional distribution to determine Alice's minimum error-probability decision rule. Finding that decision rule, without further approximation, is made difficult by the symbol-dependent conditional variances and covariance of I and Q. In Appendix B, however, we show that for the parameter values of interest, it is reasonable to take I and Q to be statistically independent, given Bob's transmitted symbol is k, with mean values $\bar{I}_k$ and $\bar{Q}_k$, and equal symbol-independent variances, σ^2.

With the preceding approximation for QAM's conditional measurement statistics, $p(I, Q \mid k)$, finding FL-QKD's minimum error-probability decision rule reduces to the one for classical fiber-optic communication with QAM: decoding an equiprobable QAM symbol from its observation in additive white Gaussian noise. The minimum error-probability decision rule for that problem is minimum-distance decoding, i.e., the decision region, $\mathcal{D}_k$, for symbol k is

$$\mathcal{D}_k = \{I + iQ : \arg\min_{k'} |(I - \bar{I}_{k'}) + i(Q - \bar{Q}_{k'})| = k\}, \tag{9}$$

as shown in Fig. 2(b).

So, to evaluate Alice and Bob's Shannon-information rate, we use QAM's $p(I, Q \mid k)$ and its $\mathcal{D}_{\tilde{k}}$ to calculate $\Pr(\tilde{k} \mid k)$ from Eq. (6) for $0 \leqslant k, k' \leqslant K_q - 1$. The desired Shannon-information rate is then found from

$$I_{AB} = R \left\{ \sum_{k=0}^{K_q-1} \sum_{\tilde{k}=0}^{K_q-1} \frac{\Pr(\tilde{k} \mid k)}{K_q} \log_2 \left[\frac{K_q \Pr(\tilde{k} \mid k)}{\sum_{k'=0}^{K_q-1} \Pr(\tilde{k} \mid k')} \right] \right\}. \tag{10}$$

Now, to complete our goal of finding FL-QKD's SKR_{LB} for operation with $2d \times 2d$ square-lattice QAM when Eve mounts an SPDC light-injection attack, we need to get χ_{EB}^{UB}

for that attack. Eve's Holevo-information rate upper bound can be obtained in a manner similar to the case of BPSK. Indeed, the derivation in Appendix C of Ref. [8] is directly applicable with only minor changes. This applicability is due to Eve's conditional state, given Bob transmits his kth symbol, still being Gaussian, and her unconditional state still having a Wigner covariance matrix that is diagonal. Hence Ref. [8]'s Appendix C provides the upper bound we are seeking if we (1) take account of the k-dependent nature of Eve's conditional state in evaluating the average of her conditional-states' von Neumann entropies, (2) bound her unconditional state's von Neumann entropy by the von Neumann entropy of a thermal state with the same Wigner covariance matrix, and (3) use $R \log_2(K_q)$, instead of R, as the upper limit of her Holevo-information rate. (See Appendix B for the details.)

Figure 3(b) plots QAM's SKR_{LB} versus one-way path length L for $1 \leqslant d \leqslant 4$ when, for each L value, Alice's source brightness N_S is chosen to maximize SKR_{LB} and the other system parameters are the same as those employed in Ref. [8] and for KPSK. The inset in this figure shows the optimized N_S value versus L; as expected, low-brightness operation is maintained to ward off Eve's passive-eavesdropping attack. What may not be expected for QAM, however, is the following behavior. Unlike what we saw for KPSK—where increasing K led to increasing SKR, albeit with diminishing returns, for $1 \leqslant \log_2(K) \leqslant 5$—the best QAM performance, for $1 \leqslant d \leqslant 4$, occurs when $d = 1$. But $d = 1$ square-lattice QAM is merely quadrature phase-shift keying (QPSK = 4PSK) rotated by $\pi/4$ rad, so we conclude that QAM, at least in its square-lattice form, offers no SKR benefit to FL-QKD [18].

IV. DISCUSSION

We have shown that 32PSK can increase FL-QKD's SKR on a 50-km-long fiber channel from 2.0 Gbit/s to 4.5 Gbit/s, but that square-lattice QAM offers no SKR improvement beyond its 4-ary case, which is equivalent to 4PSK. Therefore, the first thing to discuss is the reason for this behavior, which contrasts sharply with QAM's ability to provide substantial capacity increases in classical fiber-optic communication by virtue of its higher spectral efficiency.

It is easy to see why FL-QKD with KPSK suffers diminishing returns with increasing K. Because $N_S < 1$ is maintained to ensure security against Eve's passive-eavesdropping attack, the $\{\bar{I}_k + i\bar{Q}_k\}$ become more tightly packed around a circle of limited radius in the I, Q place with increasing K. Thus, because the one-standard-deviation noise regions about these points do *not* change with K, increasing K makes it harder for Alice to reliably decode Bob's transmitted symbols, hence limiting Alice and Bob's SKR gain with increasing K.

Alice's transmitting at low brightness, so that Eve cannot obtain a suitable high-quality broadband phase reference to decode Bob's KPSK, defeats passive eavesdropping. For $2d \times 2d$ square-lattice QAM with $d > 1$, however, the situation is different. Now, Bob's symbols vary in both intensity and phase. So, even without a suitable high-quality broadband phase reference, Eve's passive-eavesdropping attack can provide some intensity information about Bob's symbols. Moreover, as is the case for KPSK, Alice faces increasing difficulty in discriminating between Bob's different QAM symbols with

increasing d, because those symbols lie within a limited-radius circle in the I, Q plane, and they are each surrounded by fixed-radius one-standard-deviation noise regions. The result is that $d = 1$ is the best of the $2d \times 2d$ square-lattice QAM constellations insofar as FL-QKD's SKR is concerned.

In conclusion, FL-QKD—whether with its original BPSK encoding or with its high-order KPSK encoding—currently offers something that no other QKD protocol does: Gbit/s SKRs over metropolitan-area distances with available technology and without space-division or wavelength-division multiplexing. Hence FL-QKD could make OTP encryption of high-data-rate traffic possible over such distances. Two issues that remain to be addressed before widespread use of FL-QKD might occur are as follows.

The first issue arises because FL-QKD is an interferometric protocol, which implies that proper functioning of Alice's dual-homodyne receiver requires that the roundtrip Alice-to-Bob-to-Alice fiber link be stabilized in time delay to <1 ps and in phase to <0.2 rad for BPSK and even more finely for KPSK. It turns out, however, that the BPSK-level challenge has been overcome by MIT Lincoln Laboratory, which has recently reported success in stabilizing the 86-km-roundtrip fiber link between its Lexington Massachusetts location and the Cambridge Massachusetts MIT campus [19]. Performing a field test of FL-QKD on such a stabilized, deployed-fiber channel is the next experimental step that ought to be taken in FL-QKD's development. In support of such a field test, extending our SKR analysis to include the impact of imperfect phase stabilization is an important future task.

The second issue to be addressed concerns FL-QKD's existing security proof's being limited to frequency-domain collective attacks in the asymptotic domain, as opposed, e.g., to decoy-state BB84's coherent-attack security proof with a finite-key correction [3]. Toward this end, a recent theoretical study [20] elaborates the use of limited entanglement-assisted channel capacity to prove that Gaussian attacks are the optimum for a broad class of two-way QKD protocols. We have used that result to establish a framework that could provide the desired coherent-attack security proof for FL-QKD [21]. Completing that security proof is the essential next step in FL-QKD's theoretical development.

APPENDIX A: DETAILS FOR KPSK ENCODING

In this Appendix we shall supply details for FL-QKD with KPSK encoding that were omitted from Sec. III A, viz., we will derive the means, variances, and covariance of I and Q conditioned on Bob's having transmitted the kth symbol from his KPSK alphabet. Then, we will verify the rotational invariance claimed in Sec. III A, by proving that $\tilde{I}_k$ and $\tilde{Q}_k$ from

Eqs. (3) and (4) are statistically independent, given k, and we will find their k-independent conditional variances, $\sigma_{\tilde{I}}^2 > \sigma_{\tilde{Q}}^2$.

Our work in this Appendix will draw heavily upon the BPSK theory for FL-QKD that was established in Ref. [8]. In that paper's Appendix A, it was shown that the returned and LO light entering Alice's receiver for a particular symbol transmission comprise a collection of $M = TW$ iid mode pairs with photon annihilation operators $\{\hat{a}'_{B_m} : 1 \leqslant m \leqslant M\}$ and $\{\hat{a}'_{R_m} : 1 \leqslant m \leqslant M\}$, respectively. Under Eve's SPDC light-injection attack, and assuming Bob has transmitted his kth symbol, the results from Ref. [8]'s Appendix A—generalized to account for KPSK signaling—show that the $\hat{a}'_{B_m}$ and $\hat{a}'_{R_m}$ modes are in a zero-mean, jointly Gaussian state that is completely characterized by its nonzero second moments:

$$\langle \hat{a}_{B_m}'^\dagger \hat{a}'_{B_m} \rangle = \kappa_S [G_B(1 - \kappa_B)\kappa_S N_S + N_B] \equiv n_B, \quad \text{(A1)}$$

$$\langle \hat{a}_{R_m}'^\dagger \hat{a}'_{R_m} \rangle = N_{\text{LO}}, \quad \text{(A2)}$$

$$\langle \hat{a}_{B_m}'^\dagger \hat{a}'_{R_m} \rangle = e^{-2\pi i k/K} c_{RB}, \quad \text{(A3)}$$

where

$$c_{RB} \equiv \kappa_S [G_B(1 - \kappa_B)(1 - f_E)N_S N_{\text{LO}} n/(n+1)]^{1/2}. \quad \text{(A4)}$$

Alice 50:50 beam splits her returned and LO modes to provide the following inputs for the I and Q channels of her dual-homodyne receiver:

$$\hat{a}_{B_m}'^{(I)} = (\hat{a}'_{B_m} + \hat{a}_{V_{B_m}})/\sqrt{2}, \quad \text{(A5)}$$

$$\hat{a}_{B_m}'^{(Q)} = (\hat{a}'_{B_m} - \hat{a}_{V_{B_m}})/\sqrt{2}, \quad \text{(A6)}$$

$$\hat{a}_{R_m}'^{(I)} = (\hat{a}'_{R_m} + \hat{a}_{V_{R_m}})/\sqrt{2}, \quad \text{(A7)}$$

$$\hat{a}_{R_m}'^{(Q)} = (\hat{a}'_{R_m} - \hat{a}_{V_{R_m}})/\sqrt{2}, \quad \text{(A8)}$$

where the $\{\hat{a}_{V_{B_m}}, \hat{a}_{V_{R_m}}\}$ are in their vacuum states. The I and Q outputs of Alice's dual-homodyne receiver are then the results of the quantum measurements

$$\hat{I} = \sum_{m=1}^{M} (\hat{a}_{+m}'^{(I)\dagger} \hat{a}_{+m}'^{(I)} - \hat{a}_{-m}'^{(I)\dagger} \hat{a}_{-m}'^{(I)}), \quad \text{(A9)}$$

$$\hat{Q} = \sum_{m=1}^{M} (\hat{a}_{+m}'^{(Q)\dagger} \hat{a}_{+m}'^{(Q)} - \hat{a}_{-m}'^{(Q)\dagger} \hat{a}_{-m}'^{(Q)}), \quad \text{(A10)}$$

where

$$\hat{a}_{\pm m}'^{(I)} \equiv \sqrt{\eta}(\hat{a}_{B_m}'^{(I)} \pm \hat{a}_{R_m}'^{(I)})/\sqrt{2} + \sqrt{1 - \eta}\,\hat{v}_{\pm m}^{(I)}, \quad \text{(A11)}$$

$$\hat{a}_{\pm m}'^{(Q)} \equiv \sqrt{\eta}(\hat{a}_{B_m}'^{(Q)} \pm i\hat{a}_{R_m}'^{(Q)})/\sqrt{2} + \sqrt{1 - \eta}\,\hat{v}_{\pm m}^{(Q)}, \quad \text{(A12)}$$

with η being her receiver's homodyne efficiency and the $\{\hat{v}_{\pm m}^{(I)}, \hat{v}_{\pm m}^{(Q)}\}$ modes being in their vacuum states.

Straightforward calculations now yield the following expressions for the conditional means, variances, and covariance of I and Q, given that Bob's transmitted symbol was k:

$$\bar{I}_k = M\eta \cos(2\pi k/K) c_{RB}, \quad \text{(A13)}$$

$$\bar{Q}_k = M\eta \sin(2\pi k/K) c_{RB}, \quad \text{(A14)}$$

$$\sigma_{I_k}^2 = M\eta [\eta \cos(4\pi k/K) c_{RB}^2 + n_B + N_{\text{LO}}(1 + \eta n_B)]/2, \quad \text{(A15)}$$

$$\sigma_{Q_k}^2 = M\eta [-\eta \cos(4\pi k/K) c_{RB}^2 + n_B + N_{\text{LO}}(1 + \eta n_B)]/2, \quad \text{(A16)}$$

$$\sigma_{I_k Q_k} = M\eta^2 \sin(4\pi k/K) c_{RB}^2/2. \quad \text{(A17)}$$

Finally, we can prove our rotational invariance claim for the conditional statistics of I and Q. Using Eqs. (3) and (4), together with the conditional moments we have just obtained, gives us the desired result: $p(\tilde{I}_k, \tilde{Q}_k \mid k)$ is a Gaussian distribution that is completely characterized by the following moments:

$$\langle \tilde{I}_k \rangle = M\eta c_{RB}, \quad \text{(A18)}$$

$$\langle \tilde{Q}_k \rangle = 0, \quad \text{(A19)}$$

$$\sigma_{\tilde{I}_k}^2 = M\eta [\eta c_{RB}^2 + n_B + N_{\text{LO}}(1 + \eta n_B)]/2, \quad \text{(A20)}$$

$$\sigma_{\tilde{Q}_k}^2 = M[-\eta c_{RB}^2 + n_B + N_{\text{LO}}(1 + \eta n_B)]/2, \quad \text{(A21)}$$

$$\sigma_{\tilde{I}_k \tilde{Q}_k} = 0. \quad \text{(A22)}$$

Here, the Gaussian nature of $p(\tilde{I}_k, \tilde{Q}_k \mid k)$ follows from $p(I, Q \mid k)$'s being Gaussian, and the statistical independence of $\tilde{I}_k$ and $\tilde{Q}_k$ given k was sent then follows from their being uncorrelated ($\sigma_{\tilde{I}_k \tilde{Q}_k} = 0$). We also see that $\tilde{I}_k$ and $\tilde{Q}_k$ have k-independent variances, $\sigma_{\tilde{I}}^2 > \sigma_{\tilde{Q}}^2$, given k was sent.

APPENDIX B: DETAILS FOR QAM ENCODING

Here we shall supply details for FL-QKD with QAM encoding that were omitted from Sec. III B, i.e., the conditional means, variances, and covariance of I and Q, where we again rely on results from Ref. [8]'s Appendix A.

Suppose that Bob encodes his kth symbol on the light remaining after his channel monitor's tap by imposing a transmissivity $0 < \kappa_q \leqslant 1$ attenuation and a $0 \leqslant \theta_q < 2\pi$ phase shift that are chosen in accord with where the kth symbol appears in his $2d \times 2d$ square-lattice QAM constellation. Conditioned on that symbol being sent, and assuming that Eve has mounted an SPDC light-injection attack, the returned and LO light that enters Alice's receiver are again comprised of M iid $\{\hat{a}'_{B_m}, \hat{a}'_{R_m}\}$ mode pairs that are each in a zero-mean, jointly Gaussian state that is completely characterized by its nonzero second moments:

$$\langle \hat{a}_{B_m}'^\dagger \hat{a}'_{B_m} \rangle = \kappa_S [G_B(1 - \kappa_B)\kappa_q \kappa_S N_S + N_B] \equiv n_{B_q},$$
$$\langle \hat{a}_{R_m}'^\dagger \hat{a}'_{R_m} \rangle = N_{\text{LO}},$$
$$\langle \hat{a}_{B_m}'^\dagger \hat{a}'_{R_m} \rangle = \sqrt{\kappa_q} e^{-i\theta_q} c_{RB}. \quad \text{(B1)}$$

It is now a relatively simple matter to show that

$$\bar{I}_k = M\eta \sqrt{\kappa_q} \cos(\theta_q) c_{RB}, \quad \text{(B2)}$$

$$\bar{Q}_k = M\eta \sqrt{\kappa_q} \sin(\theta_q) c_{RB} \quad \text{(B3)}$$

are the conditional-mean values and

$$\sigma_{I_k}^2 = M\eta\big[\eta\kappa_q c_{RB}^2 \cos(2\theta_q) + n_{B_q} + N_{\text{LO}}(1 + \eta n_{B_q})\big]/2,$$
(B4)

$$\sigma_{Q_k}^2 = M\eta\big[-\eta\kappa_q c_{RB}^2 \cos(2\theta_q) + n_{B_q} + N_{\text{LO}}(1 + \eta n_{B_q})\big]/2,$$
(B5)

$$\sigma_{I_k Q_k}^2 = M\eta^2 \kappa_q c_{RB}^2 \sin(2\theta_q)/2$$
(B6)

are the conditional variances and covariance of Alice's I and Q values when Bob transmits his kth symbol.

To simplify finding Alice's minimum error-probability decision regions—and hence the calculation of Alice and Bob's Shannon-information rate—we note that the parameter values assumed in Sec. III imply that

$$N_{\text{LO}} \gg \kappa_q c_{RB}^2 \sim \kappa_q \kappa_S^2 G_B N_S N_{\text{LO}}$$
$$> n_{B_q} \sim \kappa_q \kappa_S N_B \gg 1.$$
(B7)

Using these relations simplifies Eqs. (B4)–(B6) to $\sigma_{I_k}^2 \approx M\eta^2 N_{\text{LO}} n_{B_q}/2$, $\sigma_{Q_k}^2 \approx M\eta^2 N_{\text{LO}} n_{B_q}/2$, and $\sigma_{I_k Q_k} \approx 0$, thus justifying the white Gaussian noise assumption made in Sec. III B.

---

[1] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).

[2] C. E. Shannon, Bell. Syst. Tech. J. **28**, 656 (1949).

[3] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Frölich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Opt. Express **21**, 24550 (2013).

[4] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Opt. Express **23**, 17511 (2015).

[5] T. Zhong *et al.*, New J. Phys. **17**, 022002 (2015).

[6] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, arXiv:1611.01139 [quant-ph].

[7] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, 1701491 (2017).

[8] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **94**, 012322 (2016).

[9] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **95**, 012332 (2017).

[10] Z. Zhang, C. Chen, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, Quantum Sci. Technol. **3**, 025007 (2018).

[11] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).

[12] R. J. Essiambre and R. W. Tkach, Proc. IEEE **100**, 1035 (2012).

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

[14] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).

[15] Unlike [8], we shall not reduce Bob's symbol rate to ensure that Alice's symbol error probability does not exceed 0.1. For the parameter values we have assumed, however, Alice's symbol error probability remains below 0.1 for $L \leqslant 50$ km.

[16] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering* (Wiley, New York, 1965).

[17] The corner points in the Fig. 2(b) signal constellation are produced with just phase shifts. The remaining points require attenuation, with those that do not lie on the I axis requiring phase shifts as well.

[18] This point is further underscored by our not having proved that Eve's SPDC light-injection attack realizes her optimum frequency-domain collective attack on $2d \times 2d$ square-lattice QAM for $d > 1$.

[19] M. E. Grein, M. L. Stevens, N. D. Hardy, and P. B. Dixon, CLEO 2017 Tech. Digest, paper FTu4F.6.

[20] Q. Zhuang, E. Y. Zhu, and P. W. Shor, Phys. Rev. Lett. **118**, 200503 (2017).

[21] Q. Zhuang, Z. Zhang, N. Lütkenhaus, and J. H. Shapiro, arXiv:1805.10314 [quant-ph].