Large-alphabet encoding for higher-rate quantum key distribution

Research Article | Vol. 27, No. 13 | 24 Jun 2019 | OPTICS EXPRESS 17539
Optics EXPRESS

Large-alphabet encoding for higher-rate quantum key distribution

CATHERINE LEE,[1,2] DARIUS BUNANDAR,[1] ZHESHEN ZHANG,[1,3] GREGORY R. STEINBRECHER,[1,2] P. BEN DIXON,[2] FRANCO N. C. WONG,[1] JEFFREY H. SHAPIRO,[1] SCOTT A. HAMILTON,[2] AND DIRK ENGLUND[1,*]

[1]*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[2]*Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, MA 02421, USA*
[3]*Currently with the Department of Materials Science and Engineering, University of Arizona, Tucson, AZ 85721, USA*
[*]*englund@mit.edu*

Abstract: The manipulation of high-dimensional degrees of freedom provides new opportunities for more efficient quantum information processing. It has recently been shown that high-dimensional encoded states can provide significant advantages over binary quantum states in applications of quantum computation and quantum communication. In particular, high-dimensional quantum key distribution enables higher secret-key generation rates under practical limitations of detectors or light sources, as well as greater error tolerance. Here, we demonstrate high-dimensional quantum key distribution capabilities both in the laboratory and over a deployed fiber, using photons encoded in a high-dimensional alphabet to increase the secure information yield per detected photon. By adjusting the alphabet size, it is possible to mitigate the effects of receiver bottlenecks and optimize the secret-key rates for different channel losses. This work presents a strategy for achieving higher secret-key rates in receiver-limited scenarios and marks an important step toward high-dimensional quantum communication in deployed fiber networks.

1. Introduction

Quantum key distribution (QKD) allows two parties, Alice and Bob, to establish provably secure encryption keys at a distance. The keys can be used with symmetric encryption schemes, like the one-time pad, which requires no assumptions about the computational abilities of an adversary. QKD commonly relies on the transmission and detection of single photons to distribute the secret keys, where the secret-key generation rates are often limited by the receiver hardware, which caps the achievable photon detection rate [1]. Under this constraint, for a given maximum detection rate, the secret-key rate can still be increased by optimizing the photonic encoding. The first QKD schemes used photons encoded in two states, such as two different polarization states [2]. Recently, much effort has turned to large-alphabet QKD schemes, which encode photons in a larger set of high-dimensional basis states [3].

Compared to binary-encoded QKD, such large-alphabet schemes can boost secure communication rates by encoding more secure information per detected photon and also exhibit increased resilience to noise and loss [4]. High-dimensional encoding can also provide practical advantages in resource usage or task efficiency for various quantum information processing goals, such as Bell tests [5], quantum gates [6], and quantum error correction [7]. Here, we demonstrate the advantages of high-dimensional encoding using the example of a prepare-and-measure, high-speed, large-alphabet QKD protocol under three different channel losses, including measurements over a deployed telecom fiber. Our proof-of-principle experiments show the feasibility of large-alphabet QKD as a path to achieve higher secret-key rates in certain loss regimes.

High-dimensional encoding is possible in a variety of degrees of freedom, and large-alphabet

#350067 https://doi.org/10.1364/OE.27.017539
Journal © 2019 Received 5 Nov 2018; revised 14 May 2019; accepted 15 May 2019; published 11 Jun 2019

Optics EXPRESS

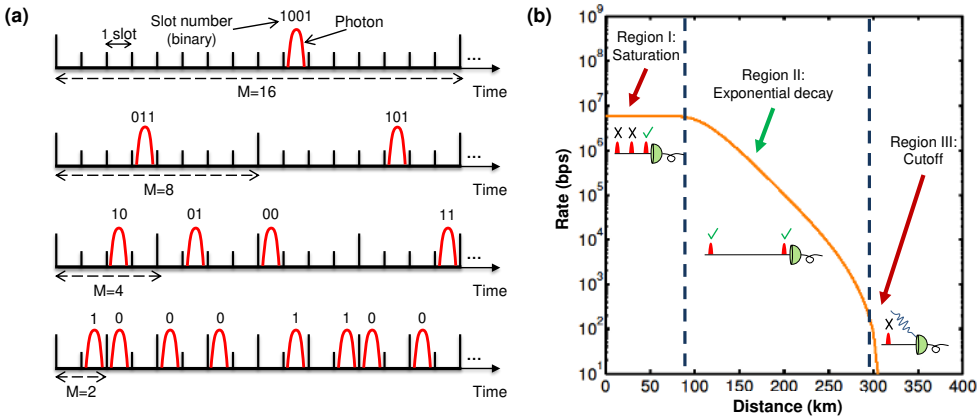

Fig. 1. (a) In high-dimensional temporal encoding (pulse position modulation), information is encoded in the position of an optical pulse within M slots, depicted here for alphabet size $M \in \{2, 4, 8, 16\}$. For a fixed slot duration, the alphabet size and the transmitted pulse rate are inversely proportional. (b) Representative plot of secret-key rate versus channel length for a traditional two-dimensional QKD protocol, assuming a 5 Gbps modulation rate, a 0.2 dB/km channel loss, a 1 kcps background count rate, a 93% detector efficiency, and a 100 ns detector reset time after each detection event. These detector performance characteristics were chosen to correspond with the high efficiency telecom band single photon detection system reported in [22], and the effects of detector reset time on observed count rate were modeled following [37]. Three regions are denoted: I. At short distances, 0-90 km (or correspondingly, low losses, 0-18 dB), the secret-key rate is limited by detector saturation. II. For higher losses (normal operation), the secret-key rate decays exponentially with distance. III. At even higher losses (> 300 km), a cutoff is reached when Bob's received photon rate becomes comparable to his detectors' background count rate. At this point, the error rate grows and the secret-key rate drops abruptly.

QKD has been demonstrated using position-momentum [8], spatial modes in multicore fibers [9, 10], time-energy [11–16], and orbital angular momentum (OAM) modes [17–19], as well as combinations of polarization and OAM modes [20]. Of these, time-energy encoding is appealing for its compatibility with a large portion of existing telecommunications infrastructure — which lowers the barriers to widespread adoption of QKD. Indeed, the time-energy correlations are robust over transmission in both fiber and free-space channels and are preserved when passing through wavelength-division multiplexing.

In high-dimensional temporal encoding, the time-slot position of a pulse within a multi-time-slot symbol-frame determines its coded symbol. Classically, this encoding is known as pulse position modulation (PPM), and combined with single-photon detection, it achieves near-optimal performance in terms of bits per detected photon [21]. A pulse coded into a symbol comprising M time slots can convey up to $\log_2 M$ bits of information, as illustrated in Fig. 1(a). The rate of transmitted symbols, R_T, is ideally $R_T = R_c/M$, where R_c is the system clock rate. Assuming constant R_c, PPM exhibits a trade-off between the alphabet size M and R_T: an increase in the former directly corresponds to a decrease in the latter. We take advantage of this trade-off to maximize the secret-key rate in the presence of receiver saturation.

Figure 1(b) is a representative plot of secret-key rate versus channel length for binary encoding with realizable parameters. Three regimes of distance/loss are indicated. In normal operation (Region II), the secret-key rate decreases exponentially with distance until the received photon flux is comparable to the background counts of the detector(s). In this regime, binary encoding works

Optics EXPRESS

well and high-dimensional encoding does not offer any performance benefit. At distances/losses beyond the exponential rate-loss cutoff point (Region III), the correlations between sender and receiver are masked by the background and no secure keys can be generated. However, at short distances, i.e., low losses (Region I), the secret-key rate is limited when some component of the receiver hardware — such as the single-photon detectors or the readout electronics — is saturated by the incoming photon flux, as illustrated in Fig. 1(b). In this regime, which extends to approximately 90 km for these parameters, high-dimensional encoding can be used to increase the secret-key rate above the maximum binary-encoded rate.

Here we focus on using high-dimensional encoding to maximize secret-key rates over metropolitan-area distances of tens of kilometers. This work is complementary to previous research which has tended to focus on extending the range of QKD links well beyond tens of kilometers to inter-city lengths of hundreds of kilometers [23–26]: deployed QKD networks will include a variety of links, including long distance inter-city links, as well as shorter, metropolitan-area-scale links. Each link type will potentially have different optimal operating points and technologies.

2. High-dimensional prepare-and-measure QKD experiment

To demonstrate high-rate, large-alphabet QKD, we focus on dispersive-optics QKD (DO-QKD) [27], a high-dimensional QKD protocol based on time-energy encoding, with basis transformations produced by group velocity dispersion (GVD). We previously proved the security of this scheme against arbitrary collective attacks [27] and implemented the scheme using entangled photon pairs in the laboratory [14]. Recent theoretical work has extended the security to hold against general attacks [28]. The present work is a prepare-and-measure (P&M), decoy-state version of DO-QKD.

In P&M DO-QKD, Alice and Bob derive shared information from timing correlations between the prepared pulse time and the measured pulse time. This information can be derived when Alice and Bob prepare and measure using the same basis. When they use different bases, the correlations are degraded and provide no shared information. Decoy states provide protection against photon number splitting (PNS) attacks [29–31].

The general protocol architecture is pictured in Fig. 2. Alice's transmitter generates a sequence of PPM-encoded pulses that will become the raw key. The transmitter prepares signal-intensity states, with probability P_μ, by attenuating the optical pulses to an average intensity of μ photons/pulse, and the transmitter also prepares decoy-intensity states, with probability $P_\nu = 1 - P_\mu$, by attenuating the optical pulses to an average intensity of ν photons/pulse.

The transmitter prepares these pulses either in the time basis, with probability P_T, by sending them directly across the communication channel, or in the energy basis, with probability $P_E = 1 - P_T$, by applying sufficiently strong GVD to the pulse in order to stretch the pulse across many time-slots within the PPM symbol-frame, before sending the stretched pulse across the communication channel.

At the other end of the communication channel, Bob's receiver measures either in the time basis — by sending the photons directly to a time-resolving single-photon detection system — or in the energy basis — by applying GVD of equal magnitude but opposite strength as used by Alice before sending the photons to a time-resolving single-photon detection system. We assume that Bob's basis choice probabilities are the same as Alice's.

The protocol's security proof requires that for each transmitted pulse, the choices of preparation basis and transmission intensity must be random to an eavesdropper, Eve, but known to Alice. Similarly, the protocol's security proof also requires that for each received pulse, the choice of measurement basis must be random to Eve but known to Bob. However, to increase the probability that Alice and Bob both choose the same basis, we can set $P_T > 1/2$; i.e., Alice and Bob both preferentially choose the time basis. Under this asymmetric basis selection, the protocol

remains secure against Eve if the timing correlations are analyzed separately for each basis [32].

After the prepared pulse times and basis choices, as well as the measured pulse times and basis choices, are recorded, Alice and Bob convert the measurement results into shared secret keys through a series of classical post-processing steps. First, Alice and Bob demodulate their PPM streams, giving each a sequence of symbols. They then perform sifting — they publicly announce their basis choices in order to post-select only the symbols that are encoded and decoded using the same basis and therefore should be strongly correlated. Alice then announces the transmitted intensities in order to divide the post-selected symbols into signal-intensity and decoy-intensity symbols. Some of the symbols — all of the energy basis, signal-intensity symbols; an equal number of randomly selected time basis, signal-intensity symbols; and all of the decoy-intensity symbols from both bases — are publicly announced in order to estimate timing correlations and symbol-error rates (SERs), which are used to calculate the maximum information accessible to Eve [31, 33]. The SER is the high-dimensional analog of the quantum bit error rate (QBER) in binary-encoded QKD; it is the fraction of symbols that were encoded and decoded using the same basis but whose values do not match. The remaining signal-intensity symbols are input to first an error-correction code, and then to a privacy amplification code, both of which sacrifice a portion of the symbol sequence, resulting in a shorter, error-free sequence of symbols shared between Alice and Bob and secret from any eavesdropper, up to an agreed upon probability of failure ε_s [33–35].

The secret key rate K, in bits/s, is the product of the detected photon rate R_p, in counts/s, and the secure photon information efficiency r, in bits. The value of R_p is ultimately limited by the receiver saturation rate. The value of r is a function of the alphabet size M, the SER — which depends upon the pulse width and real-world system fluctuations and disturbances, the operating point choices of $\{P_\mu, P_\nu, P_T, P_E\}$, the efficiency of the error correction code, and the agreed-upon value of ε_s. The details of how these factors determine r are discussed in the Appendix and also in [27, 31, 33]. The value of M is, in turn, limited by the worst timing resolution of either the transmitter or the receiver system. The operating point that optimizes the secret-key rate K achieves a complex balance between the conflicting goals of sharing maximum information between Alice and Bob and sharing minimum information with Eve — while operating within the constraints of the system hardware and real-world system fluctuations and disturbances.

3. Experimental system and demonstration

The implemented transmitter used a superluminescent diode (InPhenix) with tens of nanometers of optical bandwidth which was filtered to 25 GHz (0.2 nm), centered at 1559 nm, by a tunable bandpass filter. This continuous beam was modulated by a lithium niobate electro-optic modulator (JDSU) controlled by a PPM sequence produced by a 12.5 GHz pulse pattern generator (PPG; Anritsu). Preparing in the time-basis was performed by using this output pulse sequence, whereas preparing in the energy-basis was performed by inserting a dispersion module with 10,000 ps/nm of GVD (Proximion). Preparing in the signal or decoy intensities consisted of manually adjusting a variable optical attenuator (VOA; JDSU) to give $\mu = 0.5$ photons/pulse for signal intensities, or $\nu = 0.05$ photons/pulse for decoy intensities. These intensity values were chosen to maximize R_p while maintaining security. An optical circulator was included at the output of Alice's transmitter for protection against Trojan horse attacks [36].

The receiver used superconducting-nanowire single-photon detectors (SNSPDs), made of niobium nitride (NbN), capable of detecting hundreds of millions of photons per second with 68% detection efficiency and dark count rates of several thousand per second [37]. The timing resolution was 50 – 100 ps. The receiver timing resolution limits the minimum time-slot duration that the transmitter can use. The SNSPD system had a single optical fiber coupled to four interleaved nanowires, which were individually read out by a commercial time-to-digital converter (Picoquant Hydraharp 400). This interleaved nanowire structure is functionally equivalent to a

passive 1x4 optical splitter followed by four individual detectors. The time-to-digital converter had a dead time of 70 − 80 ns per channel, which gave the receiver system a saturated detected pulse rate of about 50 MHz. Measurements in the time basis were performed by sending the received pulses directly to the SNSPD system, whereas measurements in the energy basis were performed by inserting a dispersion compensation module with -10,000 ps/nm of GVD (Proximion) just before the SNSPD system. The insertion loss of the dispersion compensation module was 4 dB. There were some additional losses, totaling 6 dB, in the receiver due to lossy optical connectors and the blocking effects of high photon flux on the SNSPDs.

The system performance was characterized over three channel configurations, referred to as: the back-to-back configuration, the fiber-spool configuration, and the deployed-fiber configuration. The back-to-back configuration had the transmitter and the receiver in the same laboratory, connected by a short patch cable with 0.1 dB loss. The fiber-spool configuration had the transmitter and the receiver in the same laboratory, connected by a 41-km spool of standard SMF-28 single-mode fiber with 7.6 dB loss. The deployed-fiber configuration had the transmitter and the receiver located in physically separate laboratories, connected by a 43-km span of deployed telecom fiber with 12.7 dB loss.

This deployed fiber channel is one of pair of dark fibers running parallel to each other between MIT and Lincoln Laboratory, as illustrated in Fig. 2. This channel was subject to significant real-world temperature fluctuations and acoustic perturbations which introduced relative timing drifts between the transmitter and the receiver, thereby degrading the DO-QKD protocol performance by obscuring the timing correlations. This effect was mitigated by including out-of-band, periodic optical synchronization pulses sent from the transmitter and detected at the receiver with a linear photodiode to act as a shared timing reference.

In the fiber-spool and deployed-fiber configurations, the long fibers introduce additional GVD, which degrades the timing correlations between Alice's prepared pulses and Bob's measured pulses. This GVD is precompensated using a spool of dispersion-compensating fiber in the transmitter.

Four different PPM alphabet sizes were used, $M \in 4, 8, 16, 32$. For all M, the time-slots were 240 ps long, corresponding to a system clock rate of $R_c = 4.17$ GHz, which was chosen to be approaching the maximum clock rate supported by the receiver system. The high-speed capabilities of the transmitter allowed the actual optical pulses contained within the time-slots to be 50 ps long, which reduced the SER by mitigating the effects of intersymbol interference. Each symbol-frame comprised the alphabet M time-slots followed by two empty guard time-slots. The transmitted symbol rate was then $R_c/(M + 2)$, and the detected frame rate was the product of the transmitted symbol rate, the average transmitted photon number, and the channel transmission.

The DO-QKD secret-key rate capabilities of the three channel configurations were characterized by taking large data sets for the two preparation bases, the two measurement bases, and the two pulse intensities, separately. An optimized secret-key rate capability was then determined for a combined data set, consisting of 10^9 received pulses, by numerically optimizing the values of P_μ and P_T to maximize the secret-key rate. This analysis used security parameter $\varepsilon_s = 10^{-10}$ and a multi-layer low-density parity-check (LDPC) code [38] for error reconciliation.

4. Results

In the back-to-back configuration, the maximum secret-key rate capability was 23 Mbps with $M = 16$. In the fiber-spool configuration, the maximum secret-key rate capability was 5.3 Mbps with $M = 8$. In the deployed-fiber configuration, the maximum secret-key rate capability was 1.2 Mbps with $M = 4$. Table 1 summarizes the optimum rate cases for the three channel configurations.

Figure 3(a) plots these experimental results along with theoretical secret-key rates as functions of channel loss. In Fig. 3(a), there is a data point and theoretical curve corresponding to the optimal

Optics EXPRESS

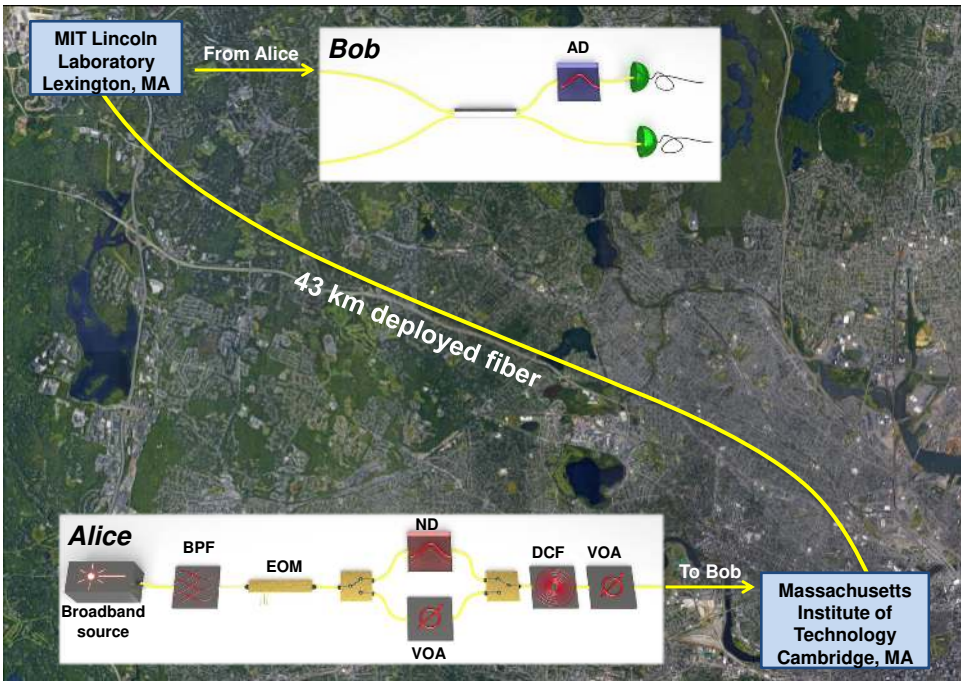

Fig. 2. Map showing node locations and approximate path of the installed 43-km deployed-fiber testbed used in this work. Overlaid are Alice's transmitter, located in Cambridge, MA, and Bob's receiver, located in Lexington, MA. BPF: bandpass filter. EOM: electro-optic modulator. VOA: variable attenuator. ND: normal GVD. AD: anomalous GVD. DCF: dispersion-compensating fiber.

alphabet size for each of the three channel configurations. The three channel configurations each had slightly different measured timing correlation values and each theoretical curve was computed using the corresponding measured values; thus, we should not directly compare the curves to determine the universally optimal alphabet size for a given loss. For a given channel configuration, however, we can determine the optimal alphabet size. To further illustrate this point, Fig. 3(a) also includes a theoretical curve showing the performance for $M = 2$ over the deployed fiber channel. For these channel losses and timing correlation values, choosing $M = 4$ outperforms $M = 2$. Figure 3(b) displays the secret-key rate capabilities obtained for each alphabet size in the three test cases, showing that the optimal alphabet size increases as the loss decreases.

5. Discussion

High-dimensional encoding can improve the rate or efficiency of quantum information processing, compared to binary encoding. Here, we have used high-dimensional encoding in quantum key distribution to mitigate the effects of receiver bottlenecks. For receiver-limited scenarios, such as relatively low-loss metro-scale fiber links, high-dimensional DO-QKD allows us to increase the realizable secret-key rate by adjusting the alphabet size.

The optimal M to maximize the secret-key rate depends most strongly on Bob's received photon rate, which is in turn a function of channel loss and also of the transmitted symbol rate. If Bob had an ideal receiver, the highest secret-key rate would be obtained for the fastest transmitted

Optics EXPRESS

Table 1. Summary of the maximum secret-key rates obtained in the three channel configurations.

	Back-to-back	41-km fiber spool	43-km deployed fiber
Loss (dB)	0.1	7.6	12.7
Slot duration (ps)	240	240	240
M	16	8	4
K (bps)	23×10^6	5.3×10^6	1.2×10^6
r (bit/pulse)	1.40	0.88	0.50
Time SER (%)	6.5	4.8	4.9
Energy SER (%)	7.1	4.9	5.3
P_T	0.99	0.93	0.88
P_μ	0.99	0.94	0.90

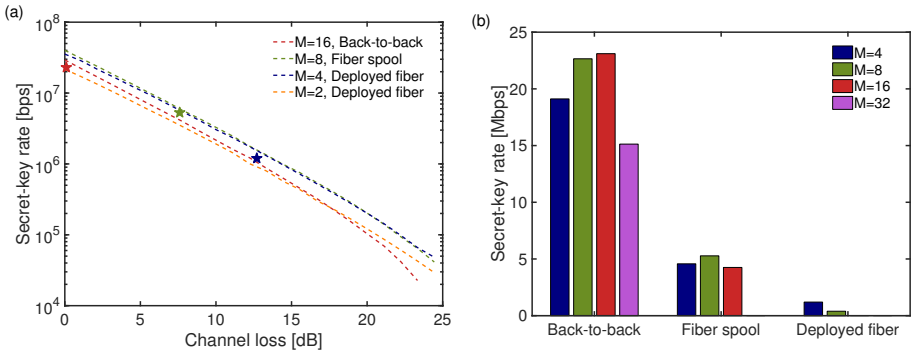

Fig. 3. (a) Experimental (stars) and theoretical (dashed curves) secret-key rates versus channel loss. Colors correspond to optimal alphabet size M for each of the channel configurations. Each theoretical curve is based on the experimental parameters (e.g., detector timing jitter) observed in the corresponding the channel configuration. The theoretical secret-key rate for $M = 2$ over the deployed fiber channel is also plotted for reference. (b) Experimental secret-key rates for all alphabet sizes of each channel configuration. Loss increases from left to right. The optimal M increases as loss decreases. For experimental convenience, we did not increase the alphabet size once it became apparent that doing so would not increase the secret-key rate.

symbol rate, which occurs for $M = 2$. However, Bob's receiver hardware is usually rate-limited. The limit may be due to the single-photon detectors themselves; for instance, SNSPDs exhibit reset times ranging from a few nanoseconds [37,39–41] to several tens of nanoseconds [22,41,42], depending on the choice of superconductor. The readout electronics can also limit the receiver count rate, as is the case for the commercial time-tagger in our system and also for the high-rate BB84 demonstration of [1]. When Bob's receivable photon rate is limited, increasing M to values greater than two allows Alice and Bob to effectively produce secret keys even during the reset time. Thus, at short distances and correspondingly low losses, we can expect a bottleneck due to

the maximum count rate of Bob's receiver. In this receiver-limited regime, it is advantageous to increase M to encode as much information as possible in each detected photon while keeping the receiver near saturation. Our receiver saturated at received photon rates around 50 Mcps, but the transmitted symbol rate for $M = 2$ was greater than 1 Gcps. For the channel configurations we examined, the channel losses were insufficient to prevent the receiver from saturating at such high transmitted symbol rates. To prevent saturation, we also needed to reduce the transmitted symbol rates by increasing M, and Fig. 3(b) demonstrates that the optimal M increased as channel loss decreased.

It should be noted that although we did not perform fast basis or intensity switching in our demonstration, the addition of such steps would not affect the demonstrated rate capabilities of the system. At the transmitter, basis switching can be done by adding a fast switch; any loss incurred can be compensated by adjusting the transmitter's variable attenuator. Intensity switching can be done by programming the transmitter's variable attenuator. At the receiver, basis switching can be done by adding a passive beamsplitter and a second detector unit. Additionally, our transmitted PPM sequence relied upon a predetermined pseudorandom stream, allowing us to fully characterize our system. The use of a high-quality random number generator would not affect the demonstrated rate capabilities of the system. Finally, the magnitude of the applied GVD should vary with M in order to stretch the pulse across the full temporal duration of the symbol-frame. For these proof-of-principle experiments, we were limited to a single pair of normal/anomalous GVD elements whose magnitude, 10,000 ps/nm, is approximately the median required value for the M considered in our demonstration.

An alternate strategy to mitigate the effects of the receiver's dead time involves using either a passive splitter or an active switching system [43,44] to distribute the incoming photons between a larger number of single-photon detectors. However, this approach can be resource-intensive, as it requires multiple detectors and readout channels and, for the active case, a switching system that is both fast and low-loss. The switching rate must match the incoming photon rate, and the loss must be low enough such that the resulting secret-key rate is higher than what could be obtained using high-dimensional encoding. Switches with both of these characteristics are not available. Additionally, it is likely that practical, deployed systems will be subject to size, weight, power, and cost constraints, further making the alternate strategy of adding a bank of detector systems unfeasible. In contrast, high-dimensional encoding does not significantly increase the receiver hardware complexity or cost because the high-dimensional decoding is performed by software.

The high-dimensional time-energy encoding investigated here offers the ability to optimize the secret-key rate by varying the alphabet size M in response to both receiver capabilities and channel loss. This is most beneficial when Bob's receiver is saturated, which often occurs over metropolitan-area distances of tens of kilometers. We have demonstrated the secret-key rate capabilities of a high-dimensional, prepare-and-measure QKD protocol over different channel losses, both in the laboratory and over a 43-km deployed telecom fiber, and shown that as the channel loss decreases, the optimal alphabet size increases. These proof-of-principle experiments demonstrate the benefits of a QKD scheme designed to adapt to the constraints of a particular link implementation, representing a strategy for optimizing high-rate secure quantum communication in metropolitan areas.

A. Secure photon information efficiency

In this appendix, we briefly describe the secure photon information efficiency r. The secure photon information efficiency quantifies Alice and Bob's information advantage over Eve, who we assume can mount arbitrary collective attacks. In the asymptotic regime of infinitely long

Optics EXPRESS

keys, the secure photon information efficiency for DO-QKD with decoy-state analysis is

$$r_{\infty,\text{decoy}} = \beta I(A;B) - (1 - F_\mu^{\text{LB}}) \log_2 M - F_\mu^{\text{LB}} \chi^{\text{UB}}(A;E), \tag{1}$$

where $\beta I(A;B)$ is Alice and Bob's reconciled mutual information, F_μ^{LB} is a lower bound on the fraction of Bob's detection events that came from a single-photon transmission by Alice, and $\chi^{\text{UB}}(A;E)$ is an upper bound on Eve's Holevo information [27, 31, 45]. By measuring the covariance matrix associated with the correlation between prepared pulse time and measured pulse time [27, 45] and by monitoring the quantum channel using weak-intensity decoy states [29–31], Alice and Bob can bound the information accessible to Eve. Any information that Alice and Bob share in excess of this bound will be secure. The decoy state measurements contribute to the estimation of both F_μ^{LB} and $\chi^{\text{UB}}(A;E)$.

In the more realistic regime of finite-length keys, Eq. (1) is true except with a finite failure probability that corresponds to the predetermined security parameter ε_s [33–35]. Operationally, ε_s is the tolerated failure probability of the entire protocol, where failure means that at the conclusion of the protocol and unbeknownst to Alice and Bob, Eve holds information about the output key. In practice, the failure probability quantifies the effects of finite sample sizes on error correction, privacy amplification, and parameter estimation [35]. The parameters related to decoy states are also affected in the finite-key regime [33]. Table 2 lists numerical values of these security-related parameters for the three channel configurations.

Table 2. Numerical values of security-related parameters for the three channel configurations.

	Back-to-back	41-km fiber spool	43-km deployed fiber
ε_s	10^{-10}	10^{-10}	10^{-10}
F_μ^{LB}	0.63	0.55	0.54
$\chi^{\text{UB}}(A;E)$ (bit/pulse)	0.24	0.12	0.05

We also note that recent theoretical work has extended the security of DO-QKD to hold against general attacks [28].

Funding

U.S. Air Force (FA8721-05-C-0002 and/or FA8702-15-D-0001); Air Force Office of Scientific Research Multidisciplinary University Research Initiative (FA9550-14-1-0052); Air Force Research Laboratory RITA (FA8750-14-2-0120); Office of Naval Research CONQUEST (N00014-16-C-2069).

Acknowledgments

Distribution statement A. Approved for public release: distribution unlimited. This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering. D.E. and D.B. acknowledge partial support from the Air Force Office of Scientific Research Multidisciplinary University Research Initiative (FA9550-14-1-0052) and the Air Force Research Laboratory RITA program (FA8750-14-2-0120). D.B. also acknowledges partial support from the Office of Naval Research CONQUEST program (N00014-16-C-2069)

and the Samsung Advanced Institute of Technology. C.L. thanks David Caplan and Nivedita Chandrasekaran for helpful discussions.

References

1. L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Room temperature single-photon detectors for high bit rate quantum key distribution," Appl. Phys. Lett. **104**, 021101 (2014).
2. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, 1984), pp. 175–179.
3. H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," Phys. Rev. A **61**, 062308 (2000).
4. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using *d*-level systems," Phys. Rev. Lett. **88**, 127902 (2002).
5. A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson, "Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities," Nat. Phys. **7**, 677–680 (2011).
6. B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, "Simplifying quantum logic using higher-dimensional Hilbert spaces," Nat. Phys. **5**, 134–140 (2009).
7. S. Muralidharan, C.-L. Zou, L. Li, J. Wen, and L. Jiang, "Overcoming erasure errors with multilevel systems," New J. Phys. **19**, 013026 (2017).
8. S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, "Quantum key distribution session with 16-dimensional photonic states," Sci. Rep. **3**, 2316 (2013).
9. G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. Connolly, A. Przysiezna, E. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, "High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers," Phys. Rev. A **96**, 022317 (2017).
10. Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," npj Quantum Information **3**, 25 (2017).
11. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states," Phys. Rev. Lett. **84**, 4737–4740 (2000).
12. I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," Phys. Rev. Lett. **98**, 060503 (2007).
13. J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith, "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion," Opt. Express **21**, 15959–15973 (2013).
14. C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, "Entanglement-based quantum communication secured by nonlocal dispersion cancellation," Phys. Rev. A **90**, 062331 (2014).
15. T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," New J. Phys. **17**, 022002 (2015).
16. N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Science Advances **3**, e1701491 (2017).
17. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," New J. Phys. **8**, 75 (2006).
18. M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," Phys. Rev. A **88**, 032305 (2013).
19. M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," New J. Phys. **17**, 033033 (2015).
20. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," Optica **4**, 1006–1010 (2017).
21. B. S. Robinson, A. J. Kerman, E. A. Dauler, R. J. Barron, D. O. Caplan, M. L. Stevens, J. J. Carney, S. A. Hamilton, J. K. Yang, and K. K. Berggren, "781 Mbit/s photon-counting optical communications using a superconducting nanowire detector," Opt. Lett. **31**, 444–446 (2006).
22. F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," Nat. Photon. **7**, 210–214 (2013).

Optics EXPRESS

23. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," New J. Phys. **11**, 075003 (2009).
24. S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," Opt. Lett. **37**, 1008–1010 (2012).
25. B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nat. Photon. **9**, 163–168 (2015).
26. B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," Optica **4**, 163–167 (2017).
27. J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, "High-dimensional quantum key distribution using dispersive optics," Phys. Rev. A **87**, 062322 (2013).
28. M. Y. Niu, F. Xu, J. H. Shapiro, and F. Furrer, "Finite-key analysis for time-energy high-dimensional quantum key distribution," Phys. Rev. A **94**, 052323 (2016).
29. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
30. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
31. D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, "Practical high-dimensional quantum key distribution with decoy states," Phys. Rev. A **91**, 022336 (2015).
32. H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," J. Cryptology **18**, 133–165 (2005).
33. H. Bao, W. Bao, Y. Wang, C. Zhou, and R. Chen, "Finite-key analysis of a practical decoy-state high-dimensional quantum key distribution," J. Phys. A: Mathematical and Theoretical **49**, 205301 (2016).
34. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).
35. C. Lee, J. Mower, Z. Zhang, J. Shapiro, and D. Englund, "Finite-key analysis of high-dimensional time–energy entanglement-based quantum key distribution," Quantum Inf. Process. **14**, 1005–1015 (2015).
36. M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical security bounds against the trojan-horse attack in quantum key distribution," Phys. Rev. X **5**, 031030 (2015).
37. D. Rosenberg, A. J. Kerman, R. J. Molnar, and E. A. Dauler, "High-speed and high-efficiency superconducting nanowire single photon detector array," Opt. Express **21**, 1440–1447 (2013).
38. H. Zhou, L. Wang, and G. Wornell, "Layered schemes for large-alphabet secret key distribution," in *Proceedings on Information Theory and Applications Workshop (ITA)* (IEEE, 2013), pp. 1–10.
39. A. J. Kerman, E. A. Dauler, W. E. Keicher, J. K. W. Yang, K. K. Berggren, G. Gol'tsman, and B. Voronov, "Kinetic-inductance-limited reset time of superconducting nanowire photon counters," Appl. Phys. Lett. **88**, 111116 (2006).
40. A. J. Kerman, D. Rosenberg, R. J. Molnar, and E. A. Dauler, "Readout of superconducting nanowire single-photon detectors at high count rates," J. Appl. Phys. **113**, 144511 (2013).
41. E. A. Dauler, M. E. Grein, A. J. Kerman, F. Marsili, S. Miki, S. W. Nam, M. D. Shaw, H. Terai, V. B. Verma, and T. Yamashita, "Review of superconducting nanowire single-photon detector system design options and demonstrated performance," Opt. Eng. **53**, 081907 (2014).
42. R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater, D. Oblak, S. W. Nam, and W. Tittel, "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors," Opt. Express **22**, 24497–24506 (2014).
43. S. A. Castelletto, I. P. Degiovanni, V. Schettini, and A. L. Migdall, "Reduced deadtime and higher rate photon-counting detection using a multiplexed detector array," J. Mod. Opt. **54**, 337–352 (2007).
44. V. Schettini, S. V. Polyakov, I. P. Degiovanni, G. Brida, S. Castelletto, and A. L. Migdall, "Implementing a multiplexed system of detectors for higher photon counting rates," IEEE J. Sel. Top. Quantum Electron. **13**, 978–983 (2007).
45. Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, "Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry," Phys. Rev. Lett. **112**, 120506 (2014).