Enhancing the secure key rate in a quantum-key-distribution system using discrete-variable, high-dimensional, time-frequency states

Nurul T. Islam[1], Clinton Cahall[2], Andrés Aragoneses[1], Charles Ci Wen Lim[3], Michael S. Allman[4], Varun Verma[4], Sae Woo Nam[4], Jungsang Kim[2], and Daniel J. Gauthier[5]

[1]Department of Physics and the Fitzpatrick Institute for Photonics, Duke University, Durham, North Carolina 27708, USA
[2]Department of Electrical and Computer Engineering and the Fitzpatrick Institute for Photonics, Duke University, Durham, North Carolina 27708, USA
[3]Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, USA
[4]National Institute of Standards and Technology (NIST), 325 Broadway, Boulder, Colorado 80305, USA
[5]Department of Physics, The Ohio State University, 191 West Woodruff Ave., Columbus, Ohio 43210 USA

ABSTRACT

High-dimensional (dimension $d > 2$) quantum key distribution (QKD) protocols that encode information in the temporal degree of freedom promise to overcome some of the challenges of qubit-based ($d = 2$) QKD systems. In particular, the long recovery time of single-photon detectors and large channel noise at long distance both limit the rate at which a final secure key can be generated in a low-dimension QKD system. We propose and demonstrate a practical discrete-variable time-frequency protocol with $d = 4$ at a wavelength of 1550 nm, where the temporal states are secured by transmitting and detecting their dual states under Fourier transformation, known as the frequency-basis states, augmented by a decoy-state protocol. We show that the discrete temporal and frequency states can be generated and detected using commercially-available equipment with high timing and spectral efficiency. In our initial experiments, we only have access to detectors that have low efficiency (1%) at 1550 nm. Together with other component losses, our system is equivalent to a QKD system with ideal components and a 50-km-long optical-fiber quantum channel. We find that our system maintains a spectral visibility of over 99.0% with a quantum bit error rate of 2.3%, which is largely due to the finite extinction ratio of the intensity modulators used in the transmitter. The estimated secure key rate of this system is 7.7×10^4 KHz, which should improve drastically when we use detectors optimized for 1550 nm.

Keywords: quantum key distribution, high-dimensional quantum states, time-delay interferometers

1. INTRODUCTION

Quantum key distribution (QKD) exploits quantum properties of single-photon wavepackets to transmit secret keys between two distant users (Alice and Bob) in the presence of an eavesdropper (Eve) who has access to technology only limited by the laws of physics.[1] In the original proposal by Bennet and Brassard (famously known as BB84),[2] information is encoded in the polarization degree-of-freedom of a single photon wavepacket, allowing users to extract a maximum of one secret bit per photon. Most current QKD systems are qubit-based ($d = 2$) variants of the original scheme, where only up to one secret bit is impressed on a photon using various degrees-of-freedom such as polarization, phase, orbital angular momentum, or time.

Further author information:
N. T. I.: E-mail: nti3@duke.edu

Quantum Information Science and Technology II, edited by Mark T. Gruneisen, Miloslav Dusek, John G. Rarity,
Proc. of SPIE Vol. 9996, 99960C · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2241429

For QKD systems operating over relatively short distances where the channel loss is low, the secret key rate is limited by the saturation of single-photon detectors in the receiver. Detector saturation arises from the so-called detector "dead time," the time over which the detector is not responsive to a photon after a detection event. In greater detail, consider a QKD system where Alice encodes information on photonic wavepackets every period of the system master clock (every time slot). To avoid missing photon detection events, the clock period needs to be longer than the detector dead time, thus limiting the overall system photon rate and the secure key rate. The advent of cryogenic-based superconducting single-photon nanowire detectors has significantly improved the detector recovery time, but the detected photon rate is still limited to 25-100 MHz.[3] In comparison, the temporal window required to create a photonic state can be less than 1 ps so that the the number of photonic states that can be generated is $\sim 10^4$ times greater than can be detected directly.

One solution to this problem is to use the temporal degree-of-freedom for encoding information, analogous to classical pulse-position modulation. Here, the photon is placed in a single time bin within a window (frame) of d contiguous time bins and the mean photon number is adjusted so that there is approximately one photon per frame. The frame and time-bin size is then adjusted to just reach detector saturation, allowing the extraction of $\log_2 d$ bits of information per detected photon in comparison to other protocols operating at the detector saturation limit that attempt to fill every time slot. Another advantage of the temporal degree-of-freedom is that many standard classical communication components can be used in the QKD system.

In the opposite limit of high quantum channel loss, high-dimension protocols also have an advantage. In particular, the extractable secure key rate can be larger for a high-dimension protocol as compared to a qubit protocol.[4] In fact, at large errors, there may be no extractable secure key for qubit protocols whereas some key can be obtained from the higher-dimension approaches.

There has been several recent proposals and demonstrations of high-dimension QKD systems using various photonic degree-of-freedom, including orbital angular momentum[5] and time-frequency in discrete[6–10]- and continuous-variable schemes.[11–13] Here, we implement a discrete-variable time-frequency scheme,[7] where Alice encodes high-dimension symbols using photonic states in temporal bins, and the presence of an eavesdropper is monitored by transmitting and receiving states in the discrete Fourier transform (frequency) domain. In the rest of the paper, we first describe the protocol (Sec. 2) and the experimental setup used to realize the protocol (Sec. 3). In Sec. 4, we discuss and evaluate the performance of our setup. Finally in Sec. 5, we conclude with a brief summary.

2. TWO-BASIS ASYMMETRIC TIME-FREQUENCY PROTOCOL

In our protocol, Alice prepares photonic quantum states in discrete time-bins of width τ, where each state occupies up to d time bins that we refer to as frame. The single-photon states are prepared in either the temporal or frequency basis, where the temporal states consist of a narrow temporal width wavepacket localized to one of the d time bins given by $|\Psi_{t_n}\rangle = a_n^\dagger|0\rangle$, where $n = 0, 1, ..., d-1$ and $|0\rangle$ is the vacuum state. The frequency states are multi-peaked wavepackets extending over the entire frame of d time bins and expressed as a superposition of temporal states with phase coefficients for each wavepacket peak given by the discrete Fourier transform. Specifically, they are defined through the relation[14]

$$|\Psi_{f_n}\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \exp\left(\frac{2\pi i n m}{d}\right) |\Psi_{t_m}\rangle. \qquad n = 0, ..., d-1 \tag{1}$$

In a practical implementation, both the temporal and frequency states can be generated by modulating a weak coherent laser source using electro-optic intensity modulators to create the narrow-width wavepackets. A phase modulator can be used to impose the required phases when creating the frequency states. To overcome loss-dependent eavesdropping strategies, such as photon number splitting attacks that arise from multi-photon components of the weak coherent pulses, the so-called decoy state method can be used to set a lower bound on the single-photon detection rate and an upper bound on the single-photon error rate. These estimates thus allow us to optimize contributions from states that contain only one photon.[15,16]

Detection of the frequency states can be performed by appropriately delaying the temporal wavepackets within a frame and interfering them in the same temporal mode. This can be accomplished by using active optical

switches, optical delay lines, and phase shifters, although at the expense of a more complicated experimental setup.[17] An alternative method involves using $d-1$ passive unequal path (delay) interferometers (DI) and placing them in a tree-like multi-stage arrangement.[7] In a DI, an incoming beam of light is split into two equal parts using a 50-50 beamsplitter. The beams are directed along two different paths and interfered at a second beamsplitter, where the path difference is denoted by ΔL, resulting in a time delay $\Delta t = c/\Delta L$ where c is the speed of light.

The tree of DIs used to measure the frequency states is arranged so that interferometers in each stage have the same time-delay and each successive stage has interferometers with half the time-delay as the previous stage. See Fig. 1(a) for the measurement of frequency states with $d = 4$. The last stage of the tree has $d/2$ interferometers whose time-delay is equal to τ. The phases of the interferometers are set such that there is a one-to-one correspondence between each frequency state and one output port of the last-stage interferometers.

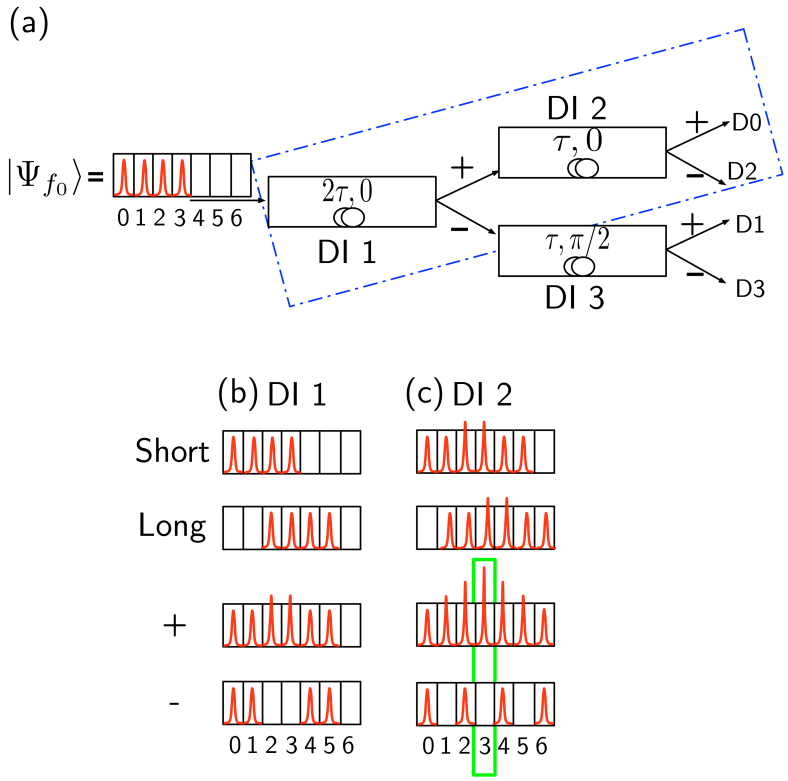

Figure 1. (a) Illustration of tree-like arrangement required for detection of frequency states in $d = 4$. (b) Illustration of the photonic wavepacket $|\Psi_{f_0}\rangle$ propagating through DI 1, and (c) DI 2. The shape of the interference patterns represent the probability density of the wavepacket at the output ports the interferometers. The delay and phase is given for each DI in (a). The green rectangle indicates the time bin in the output wavepacket where interference of all four peaks of the input wavepacket interfere either constructively (the + output port of DI 2) or destructively (the − output port of DI 2).

As an example, we illustrate in Fig. 1 the measurement of the frequency state $|\Psi_{f_0}\rangle$ with $d = 4$. For simplicity, we only trace the propagation of the state along one branch of the tree (blue dashed lines in Fig. 1(a)), where the wavepacket at the + output port of DI 1 propagates through DI 2. A similar argument can be used to explain the propagation through the other branches.

Figures 1(b) and (c) illustrate wavepackets at different stages of the tree as they propagate through interferometers DI 1 and DI 2. In DI 1, the part of the wavepacket propagating through the long arm of the interferometer is shifted by 2τ relative to the part that propagates through the short arm (Fig. 1(b)). At the final beamsplitter, the two parts recombine and there is constructive (destructive) interference in the middle two time bins (2, 3) at the + (−) output port of the interferometer. The wavepackets occupying the outer time bins

(0,1,4,5) do not interfere. The two wavepackets at the + and − output ports of the interferometers are then directed towards the next stage interferometers.

The wavepacket at the + output of DI 1 propagates through DI 2 where the relative delay is τ as shown in Fig. 1(c). In this case, the part of the wavepacket propagating through the long arm of DI 2 is shifted by τ relative to the part propagating through the shorter arm. When the wavepackets combine at the final beamsplitter, there is constructive (destructive) interference in the five middle time bins. The wavepackets in time bin 0 and 6 do not interfere. The interference pattern as observed after the final beamsplitter is shown in Fig. 1(c).

At the + output port of DI 2, the wavepacket occupies 7 time bins, with the highest photon detection probability in the central time bin. On the other hand, in the − output port of DI 2, there is destructive interference in alternative time bins and a zero probability of photon detection in the central time bin. It is important to note that the central time bin represents the interference of all wavepacket peaks in the incident state. The other time bins, except the outer most ones, represent the interference of only a subset of peaks and can provide information about the coherence of certain peaks in the incident wavepacket. However, in this protocol we consider them as inconclusive events that arise due to inefficiency of our measurement system. Therefore, a successful measurement of state $|\Psi_{f_0}\rangle$ occurs when a detection event is observed in the central time bin at the + output of DI 2. An error in the measurement of the state $|\Psi_{f_0}\rangle$ corresponds to a detection event in the central time bin at any other output ports. A similar analysis shows that a successful measurement of frequency state $|\Psi_{f_n}\rangle$ corresponds to a detection event in the central time bin of detector n. Any spurious event that results from loss of coherence will be detected by observing events in the central time bin of the other detectors.

In order to quantify the error due to spurious events, the visibility of the interference can be calculated based on photon events observed at different output ports of DI 2 and DI 3. For the incident state $|\Psi_{f_n}\rangle$, the visibility of the interference is defined as

$$\mathcal{V} = \frac{P_n - P_e}{P_n + P_e}, \tag{2}$$

where P_n is the probability of observing the detection event in the central time bin of a frame in detector n and P_e is the probability of detecting the photon in the central bin in any other detector. The probabilities can be calculated based on the observed statistics of the interference. The interference pattern represents the probability density function of the photon's occupation. Therefore, the area under the interference pattern represents the probability of photon occupation.

The visibility is an important system parameter for this protocol because it is related to the quantum bit-error rate for measurements of the frequency basis. It estimates the mutual information that an eavesdropper has on the shared quantum states between Alice and Bob. Any loss of visibility, whether due to the intrinsic error of the measurement device or due to noise in the quantum channel, is assumed to be due to the eavesdropper. Therefore, it is important that we can obtain a high visibility to maximize the secure key rate.

3. EXPERIMENTAL SYSTEM

The secure rate per photon is the most important figure of merit for a QKD system, which depends on parameters such as the quantum bit-error rate and hence on the interferometer visibility. The main source of quantum bit error in a temporal encoding scheme arise from detecting photons in the wrong time-bin, which can be due to imperfect interference in the interferometer from optical misalignment or non-ideal beamsplitters, photonic wavepackets that have a duration larger than or comparable to τ, detector jitter larger than or comparable to τ, detector dark counts, and photons entering the quantum channel from other sources. Here, we address generating temporally brief wavepackets and reducing the detector jitter.

The transmitter of our time-frequency QKD system creates 66-ps-duration pulses using a continuous-wave laser (Wavelength Reference Clarity-NLL-1550-HP) modulated by three intensity modulators (EOSpace, 12 GHz-bandwidth) as shown in Fig. 2. The first intensity modulator (IM 1) is driven by a 5 GHz sine-wave generator that creates a pulse train of 66 ps in 400-ps-duration temporal bins. The second intensity modulator (IM2) is driven by a 10 GHz (100 ps) custom-built random pattern generator based on a field-programmable gate array

(FPGA, Altera Stratix V), which is used to carve the temporal and frequency states from the periodic pulse train. The third intensity modulator (IM 3) is used as an optical switch to reduce the intensity of the signal states for a small fraction (7.1%) of the signals to generate the so-called decoy states.[15] Finally, all states (signal and decoy) are attenuated to single-photon level and the mean photon numbers per state are set to ∼0.5 for the signal states and ∼0.1 for the decoy states.

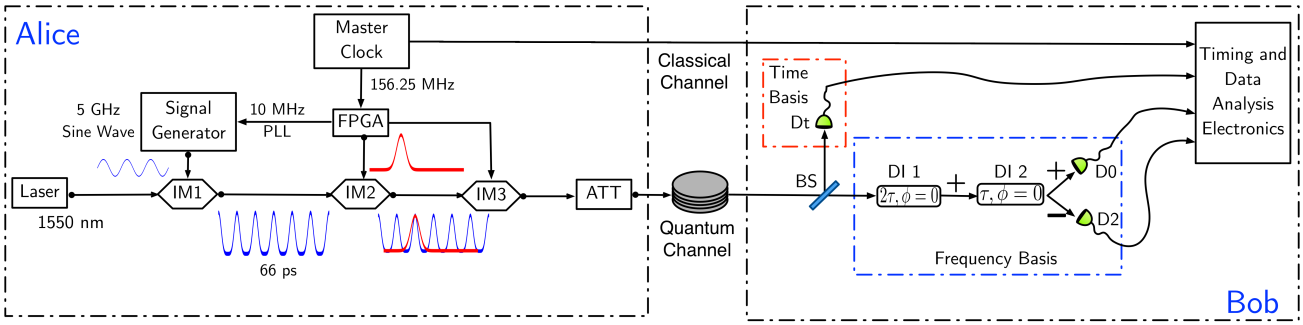

Figure 2. A schematic of the experimental setup that is used for the generation and detection of temporal and frequency states. Since only one frequency state is created, the detection of the frequency state can be performed with only one branch of the interferometric tree as indicated with the blue box.

On Bob's side, we split the signal using a 50-50 beamsplitter to passively select either a temporal or a spectral measurement. The temporal measurement is performed with a superconducting nanowire single-photon detector optimized for a wavelength of 710 nm as part of a different research project. At the wavelength of 1550 nm used here, the efficiency of the detector is ∼ 1%. The photon time of arrival is measured by passing the electrical signal produced by the detector is sent to a time-to-digital converter (PicoHarp300), which is synchronized with Alice's pattern generator using the classical channel. For the frequency measurement, the photonic state go through two interferometers (Kylia), DI 1 of 1.25 GHz free-spectral range, corresponding to a time-delay of 800 ps and DI 2 of 2.5 GHz, corresponding to a time-delay of 400 ps. The detectors and time-taggers sensing the photons emanating from the interferometers are also synchronized using the classical channel.

For the purpose of an initial experimental demonstration, we only send a fixed pattern of signal states with τ= 400 ps, where Alice prepares all possible temporal and only one frequency state, $|\Psi_{f_0}\rangle$. The states (either temporal or frequency) are generated at a repetition rate of 156.25 MHz, although it can be increased upto 625 MHz in the future experiments. We note that this protocol is still secure against the most general eavesdropping attack even though we only send one frequency state as recently demonstrated in for $d = 2$.[18] The extension of this proof to $d = 4$ is beyond the scope of this paper and will be reported elsewhere.

4. RESULTS AND DISCUSSION

To determine the performance of our QKD system, we characterize the system at a loss simulating a 50 km distance in a fiber-based quantum channel assuming a fiber loss coefficient of 0.2 db/km. Figure 3 (a-d) shows the time-of-arrival of the all temporal states $|\Psi_{t_0}\rangle, |\Psi_{t_1}\rangle, |\Psi_{t_2}\rangle, |\Psi_{t_3}\rangle$ at a loss equivalent to 50 km distance. In Fig. 3(e) we show an example time-of-arrival histogram of the frequency state $|\Psi_{f_0}\rangle$ just before the cascade of delay interferometers and the observed interference pattern as observed in the + (blue) and − (red) output ports of the interferometer in Fig. 3(f).

Based on the time-of-arrival of the temporal states and by calculating the fraction of light in the neighboring time-bins relative to the expected time-bin, we determine a system quantum bit error rate, e_T of 2.3%. A large fraction (∼ 1%) of the error is due to the finite extinction ratio of the intensity modulator, which can be improved in the future. In addition, the carving of the sine-wave modulated pulse train using the 100-ps-duration electrical pulses generated by the FPGA pattern generator results in a leakage of photons into the neighboring bins. We estimate about 1% of the quantum bit error is due to this leakage. Finally, the intrinsic jitter (60 ps) and the dark

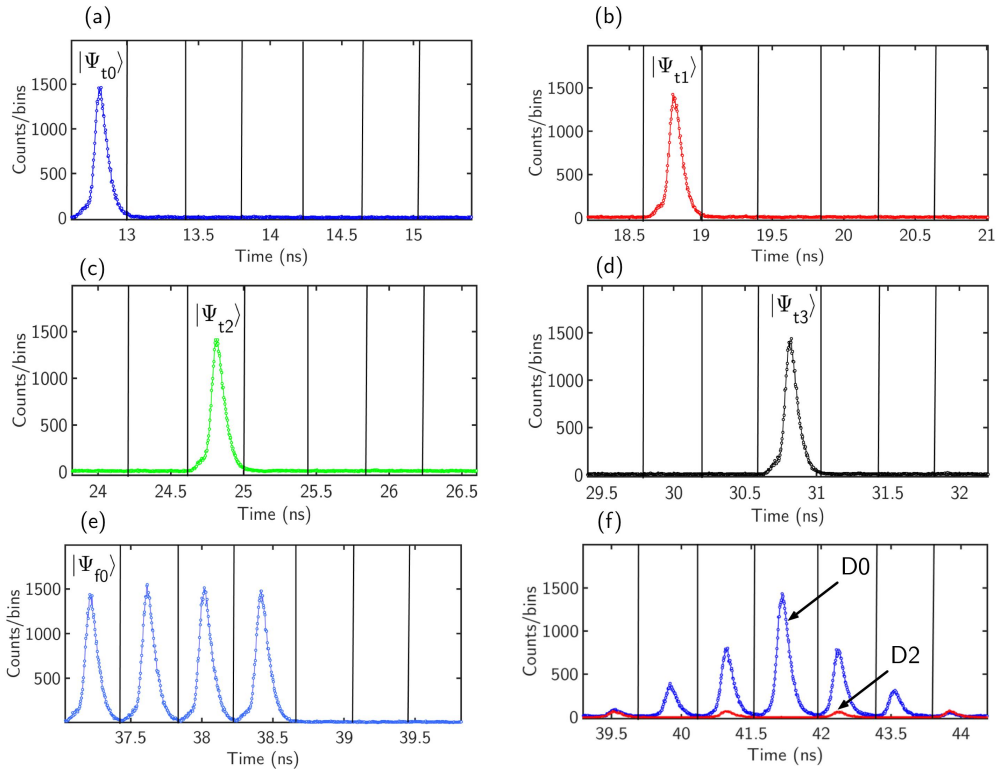

Figure 3. Timing histogram of (a-d) the temporal states $|\Psi_{t_0}\rangle, |\Psi_{t_1}\rangle, |\Psi_{t_2}\rangle, |\Psi_{t_3}\rangle$ as observed in the detector Dt, (e) frequency state $|\Psi_{f_0}\rangle$ at the input of DI 1 and (f) output ports of of DI 2 as observed in detector D0 and D2.

count (10 counts/minute) of the single-photon detectors contribute less than 0.1% error to the overall system error rate.

To determine the visibility of interference, we calculate the area under the interference peaks observed in the + and - output ports of DI 2 within one time bin and estimate the probability of detecting a photon in either port of the interferometer. Based on the probabilities, we use Eq. 2 and determine the visibility of the single-photon the $|\Psi_{f_0}\rangle$ to be 99.0% at the simulated distance of 50 km.

The total system error rate and the visibility are then used to estimate an upper bound on the secure key rate per photon of 1.6 bits/photon using the expression $R = \log_2 2 - 2H(e_T) = 1.6$, where $H(x)$ is the Shannon entropy for $d = 4$ at a quantum bit error rate of x.[19] With a measured detection rate of 4.8×10^4 Hz and raw key rate of 9.6×10^4 Hz, we estimate an upper bound for secure key rate of 7.7×10^4 Hz, which is mainly limited due to the low efficiency of our single-photon detectors and the low repetition rate of the transmitter. This is an upper bound because we do not take into account the effects of sending only one frequency state, the finite-key contribution and the overall error correction efficiency.

5. CONCLUSION

In conclusion, we investigate experimentally a discrete-variable scheme for high-dimensional time-frequency QKD and verify that the detection of single-photon frequency states can be performed using a cascade of time-delay interferometers. We observe an overall system error rate of 2.3% and a visibility of 99.0% at a loss equivalent to a 50-km-long optical fiber quantum channel, resulting in an overall upper bound for the photon efficiency of 1.6 bits per detected photon. We observe a secure key rate is 7.7×10^4 Hz at this distance, which is mainly limited due to the low efficiency of our single-photon detectors. This will improve significantly with high-efficiency detectors, and using a higher repetition rate of the transmitter.

6. ACKNOWLEDGMENT

We gratefully acknowledge the ONR MURI program on Wavelength-Agile Quantum Key Distribution in a Marine Environment, Grant # N00014-13-1-0627.

REFERENCES

[1] Barnett, S., [*Quantum Information*], Oxford Master Series in Physics, OUP Oxford (2009).

[2] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," in [*International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984*], 175–179 (1984).

[3] 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., et al., "Detecting single infrared photons with 93% system efficiency," *Nature Photonics* **7**(3), 210–214 (2013).

[4] Leach, J., Bolduc, E., Gauthier, D. J., and Boyd, R. W., "Secure information capacity of photons entangled in many dimensions," *Phys. Rev. A* **85**, 060304 (Jun 2012).

[5] Mirhosseini, M., Magaa-Loaiza, O. S., OSullivan, M. N., Rodenburg, B., Malik, M., Lavery, M. P. J., Padgett, M. J., Gauthier, D. J., and Boyd, R. W., "High-dimensional quantum cryptography with twisted light," *New Journal of Physics* **17**(3), 033033 (2015).

[6] Ali-Khan, I., Broadbent, C. J., and Howell, J. C., "Large-alphabet quantum key distribution using energy-time entangled bipartite states," *Phys. Rev. Lett.* **98**, 060503 (Feb 2007).

[7] Brougham, T., Barnett, S. M., McCusker, K. T., Kwiat, P. G., and Gauthier, D. J., "Security of high-dimensional quantum key distribution protocols using franson interferometers," *Journal of Physics B: Atomic, Molecular and Optical Physics* **46**(10), 104010 (2013).

[8] Gauthier, D. J., Wildfeuer, C. F., Guilbert, H., Stipcevic, M., Christensen, B. G., Kumor, D., Kwiat, P., McCusker, K. T., Brougham, T., and Barnett, S., "Quantum key distribution using hyperentangled time-bin states," in [*The Rochester Conferences on Coherence and Quantum Optics and the Quantum Information and Measurement meeting*], *The Rochester Conferences on Coherence and Quantum Optics and the Quantum Information and Measurement meeting* , W2A.2, Optical Society of America (2013).

[9] Brougham, T., Wildfeuer, C. F., Barnett, S. M., and Gauthier, D. J., "The information of high-dimensional time-bin encoded photons," (2015).

[10] Islam, N. T., Cahall, C., Aragoneses, A., Lim, C. C., Allman, M. S., Verma, V., Nam, S. W., Kim, J., and Gauthier, D. J., "Discrete-variable time-frequency quantum key distribution," in [*Conference on Lasers and Electro-Optics*], *Conference on Lasers and Electro-Optics* , FTh3C.3, Optical Society of America (2016).

[11] Mower, J., Zhang, Z., Desjardins, P., Lee, C., Shapiro, J. H., and Englund, D., "High-dimensional quantum key distribution using dispersive optics," *Phys. Rev. A* **87**, 062322 (Jun 2013).

[12] Nunn, J., Wright, L. J., Söller, C., Zhang, L., Walmsley, I. A., and Smith, B. J., "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion," *Opt. Express* **21**, 15959–15973 (Jul 2013).

[13] Zhang, Z., Mower, J., Englund, D., Wong, F. N. C., and Shapiro, J. H., "Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry," *Phys. Rev. Lett.* **112**, 120506 (Mar 2014).

[14] Cerf, N. J., Bourennane, M., Karlsson, A., and Gisin, N., "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.* **88**, 127902 (Mar 2002).

[15] Lo, H.-K., Ma, X., and Chen, K., "Decoy state quantum key distribution," *Phys. Rev. Lett.* **94**, 230504 (Jun 2005).

[16] Lim, C. C. W., Curty, M., Walenta, N., Xu, F., and Zbinden, H., "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A* **89**, 022307 (Feb 2014).

[17] Gleim, A. V., Egorov, V. I., Nazarov, Y. V., Smirnov, S. V., Chistyakov, V. V., Bannik, O. I., Anisimov, A. A., Kynev, S. M., Ivanova, A. E., Collins, R. J., Kozlov, S. A., and Buller, G. S., "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using bb84 protocol with a strong reference," *Opt. Express* **24**, 2619–2633 (Feb 2016).

[18] Tamaki, K., Curty, M., Kato, G., Lo, H.-K., and Azuma, K., "Loss-tolerant quantum cryptography with imperfect sources," *Phys. Rev. A* **90**, 052314 (Nov 2014).

[19] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M., "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, 1301–1350 (Sep 2009).