PHYSICS

Provably secure and high-rate quantum key distribution with time-bin qudits

Nurul T. Islam,[1]* Charles Ci Wen Lim,[2,3]* Clinton Cahall,[4] Jungsang Kim,[4,5] Daniel J. Gauthier[6]

The security of conventional cryptography systems is threatened in the forthcoming era of quantum computers. Quantum key distribution (QKD) features fundamentally proven security and offers a promising option for quantum-proof cryptography solution. Although prototype QKD systems over optical fiber have been demonstrated over the years, the key generation rates remain several orders of magnitude lower than current classical communication systems. In an effort toward a commercially viable QKD system with improved key generation rates, we developed a discrete-variable QKD system based on time-bin quantum photonic states that can generate provably secure cryptographic keys at megabit-per-second rates over metropolitan distances. We use high-dimensional quantum states that transmit more than one secret bit per received photon, alleviating detector saturation effects in the superconducting nanowire single-photon detectors used in our system that feature very high detection efficiency (of more than 70%) and low timing jitter (of less than 40 ps). Our system is constructed using commercial off-the-shelf components, and the adopted protocol can be readily extended to free-space quantum channels. The security analysis adopted to distill the keys ensures that the demonstrated protocol is robust against coherent attacks, finite-size effects, and a broad class of experimental imperfections identified in our system.

INTRODUCTION

Development of scalable quantum computing platforms is one of the rapidly expanding areas of research in quantum information science (*1*, *2*). With many commercial companies working toward building these platforms, a medium-scale quantum computer capable of demonstrating quantum supremacy over classical computers is in earnest only a few years away. Quantum computers pose a serious threat to the cybersecurity because most of the current cryptosystems, such as the one devised by Rivest, Shamir, and Adleman (known as the RSA)—whose security is based on computational hardness assumptions—can potentially be broken with a powerful quantum computer in practical time scales (*3*, *4*). Quantum key distribution (QKD) with symmetric encryption is one of the very few methods that can provide provable security against an attack aided with a quantum computer (*5*). However, a major limitation of most current QKD systems is that the rate at which the secret key is generated is orders of magnitude lower than the digital communication rates (*6*). This limitation ultimately prevents QKD from being useful for a wide range of communication tasks.

To make QKD more relevant for widespread deployment in communication networks, there has been significant effort to increase the key generation rate of QKD systems, prioritizing metropolitan distances (20 to 80 km) for large-scale implementation of QKD networks (*7*). One of the major breakthroughs was the development of superconducting nanowire single-photon detectors that can detect photons with high efficiency and yet have low dark count rates (*8*). However, these detectors still have a recovery time greater than 10 ns (*9*), thereby limiting the rate at which the secret key can be generated.

High-dimensional quantum states—qudits (dimension $d > 2$) rather than qubits—provide a robust and efficient platform to overcome some of the practical challenges of current QKD systems (*10*, *11*). The efficiency comes from the ability to encode many bits ($\log_2 d$) of information on a single photon. QKD systems using a high-dimensional quantum state space rely on the same degrees of freedom as the qubit-based systems. Nonetheless, the amount of information that can be encoded on each photon can be large even in a realistic situation because the number of bits that can be encoded on each photon is unbounded, scaling as $\log_2 d$.

Fundamentally, QKD systems using a high-dimensional quantum state space have two major advantages over the qubit-based protocols. First, they can increase the effective key generation rate in systems limited by the saturation of the single-photon detectors, often arising from the dead time of the detectors. The dead time refers to the period over which a single-photon detector resets from a previous detection event and thus remains unresponsive to an incident photon. This becomes particularly important in the limit of low channel loss, which corresponds to relatively short distances in standard optical fiber. Second, high-dimensional QKD systems have higher resistance to quantum channel noise, which means that these systems can tolerate a higher quantum bit error rate compared to qubit-based systems (*12*). Specifically, a two-basis $d = 4$ protocol can tolerate a maximum error of 18.9% compared to the 11% error tolerance for $d = 2$ protocols (*12*).

High-dimensional QKD systems have been demonstrated using various degrees of freedom of the photon, such as spatial (*13*–*17*) or time-energy modes (*18*–*23*). Here, we use the photon's temporal degree of freedom because it is relatively unaffected by turbulence in a free-space channel and easily propagates through metropolitan-scale fiber networks. Using a four-dimensional ($d = 4$) state space represented by four distinct time bins and its conjugate state space in the Fourier transform domain, we realize a QKD that generates an ultrahigh secret key rate. We note that our system is built using commercial off-the-shelf components, and therefore, it can be readily realized using equipment found in many existing QKD systems.

[1]Department of Physics and the Fitzpatrick Institute for Photonics, Duke University, Durham, NC 27708, USA. [2]Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831–6418, USA. [3]Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117583, Singapore. [4]Department of Electrical Engineering and the Fitzpatrick Institute for Photonics, Duke University, Durham, NC 27708, USA. [5]IonQ Inc., 4505 Campus Drive, College Park, MD 20730, USA. [6]Department of Physics, Ohio State University, 191 West Woodruff Avenue, Columbus, OH 43210, USA.
*Corresponding author. Email: nti3@duke.edu (N.T.I.); charles.lim@nus.edu.sg (C.C.W.L.)

RESULTS

Our QKD system is based on a prepare-and-measure scheme, where Alice randomly modulates a continuous-wave laser and attenuates the outgoing photonic wave packets to the single-photon level. The photonic wave packets are then transmitted via an untrusted quantum channel to a distant receiver, called Bob, who uses single-photon detectors or interferometers coupled to single-photon detectors to measure the wave packets in the time or phase bases, respectively. In addition, to deal with the so-called photon number–splitting attacks, we use a practical decoy-state method to estimate the number of single-photon wave packets received by Bob (*24*–*27*). The secret key is calculated using the sifted photon time-of-arrival data, and the amount of extractable secret data is determined using the noise level observed in the sifted phase measurement data. An illustration of our experimental system is shown in Fig. 1.

The quantum eigenstates in a d-dimension time basis are denoted by $|t_n\rangle$ ($n = 0, \ldots, d-1$). Each eigenstate is represented by a photonic wave packet of width $\Delta t = 66$ ps, well localized to a time bin n of width $\tau = 400$ ps within a frame of d contiguous time bins, as shown in Fig. 2A for $d = 4$. For fixed τ, the maximum mutual information per received state between Alice and Bob scales as $(\log_2 d)/d$, assuming that there is no detector saturation. This quantity is identical for $d = 2$ and $d = 4$ but decreases for larger d.

When considering detector saturation in a high-rate system such as ours, the rate scales as $\log_2 d$ if the state (frame) duration τd matches the characteristic detector saturation time (for example, detector dead time), and hence, higher-dimension protocols outperform qubit ($d = 2$) protocols (*23*). Furthermore, higher-dimension protocols have better noise tolerance, resulting in a higher secret key rate as discussed below. In our experimental implementation, we focus on $d = 4$.

To secure the QKD system, we use d-dimension phase states. They are a linear superposition of all the temporal states weighted by a unit-magnitude exponential phase factor given by

$$|f_n\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{\frac{2\pi i n m}{d}} |t_m\rangle \qquad n = 0, \ldots, d-1 \tag{1}$$

and illustrated in Fig. 2A. They take the form of the discrete Fourier transforms of the temporal states and have a multipeaked spectrum with peak spacing $1/\tau$ and width $\sim 1/2\Delta t$, and the carrier frequency of each is shifted with respect to the others. The phase states are mutually unbiased with respect to the temporal states in that states prepared in one basis and measured in the other result in a uniformly uncertain outcome: $|\langle t_n | f_m \rangle|^2 = 1/d$. The bars along the anti-diagonal in Fig. 2B represent the experimentally determined values of these probabilities when a state is prepared and measured in different bases.

At Bob's receiver, a BS is used to randomly direct the incoming quantum photonic wave packets to either a temporal or phase measurement device. We measure the temporal states using high detection efficiency single-photon detectors with a temporal resolution better than 40 ps. The detector efficiency begins to drop when the detection rate exceeds 2 megacounts/s due to the finite detector reset time (section S3). To overcome this issue, we use a 1:4 coupler to randomly direct photons to one of four detectors, allowing us to operate at high rates occurring at lower channel loss.

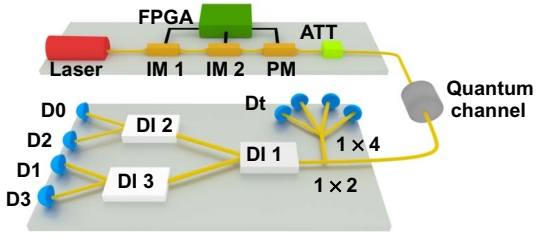

Fig. 1. Schematic of the experimental setup. At Alice's transmitter, the quantum photonic states (signal and decoy) are created using a frequency-stabilized continuous laser (Wavelength Reference, Clarity-NLL-1550-HP) operating at 1550 nm, which passes through three intensity modulators (only two are shown for clarity) and one phase modulator (all intensity and phase modulators are from EOSpace). The entire system is controlled by serial pattern generators realized with a field-programmable gate array (FPGA; Altera Stratix V 5SGXEA7N2F40C2), operating at a 10-GHz clock rate. In greater detail, a 5-GHz sine-wave generator phase locked to the FPGA drives an intensity modulator (not shown), which creates a periodic train of 66-ps-duration (full width at half maximum) optical pulses. These pulses pass through an intensity modulator (IM 1), which is driven by the FPGA-based pattern generator to define the data pattern for either the time-bin or phase states. A second intensity modulator (IM 2), driven by an independent FPGA channel, adjusts the amplitude of the phase and decoy states relative to the primary time-bin signal states. Finally, the states pass through an FPGA-driven phase modulator (PM) to encode the different phase states. The time-bin basis and the phase basis are chosen with probabilities of 0.90 and 0.10, respectively. An attenuator (ATT) reduces the level of the states to the single-photon level. An additional attenuator is used to simulate the loss of the quantum channel. At Bob's receiver, the incoming signals are split using a 90/10 beam splitter (BS) to direct 90% of the states to the temporal basis measurement system and 10% to the phase basis system. For both measurement bases, we use commercially available superconducting nanowire single-photon detectors (Quantum Opus), and the detection events are recorded with a 50-ps-resolution time-to-digital converter (Acqiris U1051A, Agilent), which is synchronized with Alice's clock over a public channel.

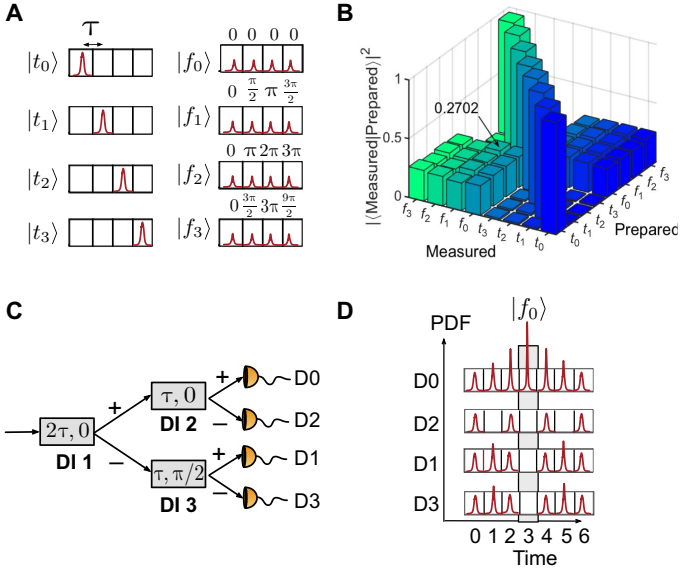

Fig. 2. Time-bin and phase states for $d = 4$ and the phase-state measurement scheme. (**A**) Temporal (left) and phase (right) states for $d = 4$, with the phases determined from Eq. 1. (**B**) Probability of detection when each input state is measured in both bases. (**C**) Measuring the phase states with a cascaded interferometric tree, where the relative time delay of the first unequal-path delay-line interferometer (DI 1) is twice the delay of DI 2 and DI 3. The phase of DI 3 is set to $\pi/2$. (**D**) Expected photon probability distribution at the output of the interferometers when the phase state $|f_0\rangle$ is injected into the system.

A novel feature of our QKD system is the phase-state measurement device (*18*, *28*), as shown in Fig. 2C. Each output of the interferometers is uniquely related to one of the phase states. As illustrated in Fig. 2D, the relevant time bin for observing interference is the central time bin (time bin 3), and when a phase state $|f_n\rangle$ is incident in the interferometric setup, the central time bin emerging from detector *Dn*, $n \in \{0, 3\}$, experiences constructive interference from the superposition of all *d* wave packets and destructive interference in all other outputs. We use commercial delay interferometers that are designed to be field-deployable and hence require no active path-length stabilization.

Security of the protocol

The security of our QKD system is derived using a recently developed technique based on entropic uncertainty relations for qudits (*29*–*31*). Unlike previous analyses for high-dimensional QKD, our approach gives finite-key bounds for mutually unbiased states and is secure against general (coherent) attacks. To extract a secret key from the single-photon states, we use a three-intensity decoy-state method to estimate the single-photon statistics observed in the data. We thereby obtain a bound on the extractable secret key length in terms of the measured data, as quantified by Eq. 2 in Materials and Methods.

Extractable secure key rate and error rates

Incorporating all our experimental and theoretical tools, we realize a QKD system that can generate record-high secret key rates. Our achieved secret key rate as a function of channel loss is shown in Fig. 3A. For comparison to previous studies (Table 1), we also represent the channel loss in terms of an equivalent length of optical fiber at telecommunication wavelengths (0.2 dB/km). At a channel loss of 4 dB (equivalent to a 20-km-long optical fiber), we can achieve an extractable secret key rate of 26.2 megabits/s, which is the highest secret key rate reported at this quantum channel loss. For this case, the error rate in the temporal and phase bases is 4.5% and 4.8%, respectively, as shown in Fig. 3B. We also obtain record-high secret key rates for other channel conditions up to a loss of 16.6 dB (83 km), as illustrated in Table 1.

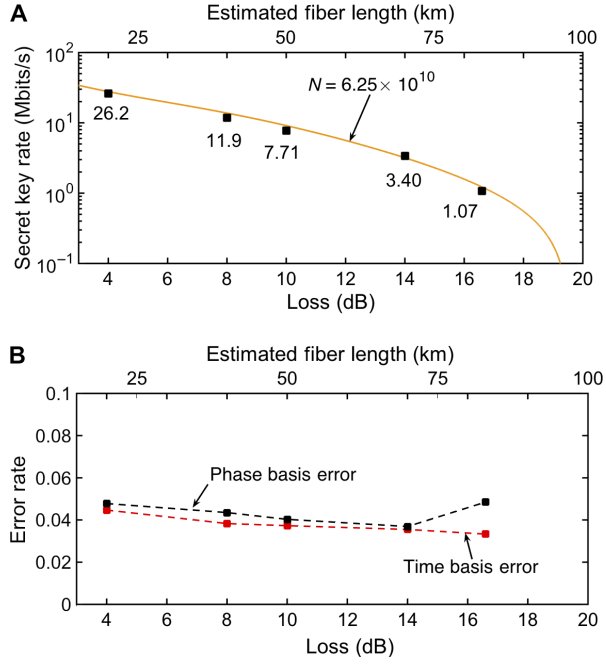

Fig. 3. Observation of high-rate and secure QKD. (**A**) Experimentally achievable secret key rates as a function of the channel loss for the case when the number of signals transmitted by Alice is $N = 6.25 \times 10^{10}$ (100-s-duration communication session). The orange solid line is the simulated secret key rate. For the simulation, we set the probabilities of sending signal, decoy, and vacuum intensities to 0.8, 0.1, and 0.1, respectively. The intrinsic error rate in the time and phase basis is set to 0.03 and 0.025, respectively. (**B**) Experimentally observed quantum bit error rate in temporal and phase basis signal states as a function of channel loss.

There are several factors contributing to the error rates in our system, such as leakage in the intensity modulators, which could be reduced in future experiments by using several modulators in series. In addition, because of high photon count rates at low channel loss, the quantum bit error rate increases as a result of ringing in the electrical readout signal (section S5), which can be reduced using an improved readout circuit. Reducing these errors will increase the secure key rate; for example, a reduction in the total error rate by a factor of 2 below what we observe (~5%) will increase the secret key rate by approximately a factor of 1.2.

Comparison with simulated secret key rate

The solid curve in Fig. 3A is the simulated secret key rate obtained using experimentally observed parameters (see Materials and Methods). At the highest channel loss considered in the experiment (16.6 dB, 83 km), the detection rate is low enough that the detectors operate at their highest detection efficiency (>70%). As the loss decreases, the detectors experience increasingly lower detection efficiency because of the finite detector reset time. To account for this, we characterize the efficiency as a function of detection rate and incorporate this information in the security analysis (section S3).

From the simulation, we see that the secret key rate drops rapidly beyond a loss of 18 dB (90 km). This drop mainly occurs due to finite-key effects arising from our use of a fixed data collection interval for all data points. In this case, the total data received by Bob go down for higher channel loss, which increases the statistical uncertainty about the phase error rate (see Materials and Methods).

DISCUSSION

We can obtain such high secret key rates due to multiple factors. First, for low-loss channels, the rate is ultimately limited by detector saturation. A high-dimensional protocol such as ours allows us to extract more bits per received photon at detector saturation in comparison to a qubit ($d = 2$) protocol, essentially doubling the secret key rate for our $d = 4$ protocol. In principle, the dimension of the photonic states can be increased beyond $d = 4$ to enhance the secret key rate. This requires $2d - 1$ interferometers, which will increase the cost and complexity of the system. Also, it will increase the number of spurious events when performing a phase basis measurement, thereby increasing the total data collection time needed to overcome finite-key length effects. Second, we use high-efficiency superconducting nanowire detectors that have a relatively short reset time in comparison to other detectors operating in the telecommunication band, such as Geiger-mode avalanche photodiodes (*32*). Third, our detectors have nearly constant jitter (<40 ps) and low dark counts (100 to 200 counts/s) independent of detection rate, resulting in a nearly constant quantum bit error rate as a function of loss seen in Fig. 3B. Fourth, we match τ to be only somewhat larger than the detector jitter, allowing us to run at a high system clock rate of 2.5 GHz.

Recently, a high-dimensional QKD system using orbital angular momenta of photons was implemented in a free-space link over 300 m,

Table 1. Comparison of some notable high-rate QKD systems. The protocol implemented by Lucamarini *et al.* (*37*) is a $d = 2$ time-bin BB84 protocol, where the two bases are chosen with asymmetric probability. Zhong *et al.* (*21*) and Lee *et al.* (*23*) implement high-dimensional QKD (HD-QKD) using time-bin encoding schemes.

	Protocol	Loss (dB)	Equivalent fiber length (km)	Secret key rate (megabits/s)	Security level
Lucamarini *et al.* (*37*)	T12	7	35	2.20	Collective
		10	50	1.09	
		13	65	0.40	
		16	80	0.12	
Zhong *et al.* (*21*)	HD-QKD	0.02	0.1	7.0	Collective
		4	20	2.7	
Lee *et al.* (*23*)	HD-QKD	0.1	0	23.0	Collective
		7.6	38	5.3	
		12.7	63	1.2	
This work	HD-QKD	4	20	26.2	Coherent/general*
		8	40	11.9	
		10	50	7.71	
		14	70	3.40	
		16.6	83	1.07	

*For the definition of coherent attacks, we refer readers to the study of Sheridan and Scarani (*12*).

wherein, using a four-dimensional state space, a quantum bit error of 11% and a secret key fraction of 0.65 bits/photon were achieved (*33*). Our time–phase state protocol is particularly well suited for field deployment because optical turbulence in free-space channels does not cause scattering of one of our photonic states into another if the wave packet duration is substantially longer than 10 ps for path lengths of tens of kilometers (*34*). Also, in a fiber-based system, the typical dephasing time is substantially longer than our frame duration time τd.

There are several possible directions for increasing the secret key rates in our system. One is developing monolithic (possibly chip-based) interferometer trees to decrease the insertion loss (and hence decrease the phase error rate) and to increase d (*18*, *23*). Another is to use dense wavelength division multiplexing methods, where Alice uses multiple transmitters each with a different carrier frequency sent down the same quantum channel (*35*). The delay interferometers work across the entire telecommunication C band, and hence, it should be possible to operate using multiple spectral channels with a single set of interferometers. Such a system will require many single-photon counting detectors, but substantial progress is under way in realizing arrays with hundreds of detectors (*36*). Finally, there is considerable ongoing research in increasing the saturated detection rate of superconducting nanowire detectors (*9*), which will have a major impact on any QKD system.

MATERIALS AND METHODS

Sketch of security proof

The security of our QKD protocol is defined by two criteria, namely, the secrecy and correctness parameters, which we denote by ε_{sec} and ε_{cor}, respectively. Using these criteria, we say that our protocol is ε-secure if it satisfies $\varepsilon_{sec} + \varepsilon_{cor} \leq \varepsilon$, where ε is a predetermined security parameter. The correctness parameter ε_{cor} is typically fixed and determined by the length of hash codes used in the error verification step. This choice of security definition guarantees that our QKD system is composable with any (possibly larger) cryptographic protocol, for example, the one-time pad encryption protocol.

Using these results, we found that the secret key length (l) is given by

$$l \leq \max_{\beta \geq 0} \left\lfloor 2\tilde{s}_{T,0} + \tilde{s}_{T,1}\left[c - H\left(\lambda^{U}\right)\right] - \mathrm{leak}_{EC} + \Delta_{FK} \right\rfloor \qquad (2)$$

where $\tilde{s}_{T,0}$ and $\tilde{s}_{T,1}$ are the number of vacuum and single-photon detections, respectively, in the time basis of the raw key, and λ^{U} is an upper bound on the single-photon phase error rate in terms of the observed error rate in the phase basis. The quality of the prepared states is quantified by the overlap parameter $c := -\log_2 \max_{i,j} |\langle f_i | t_j \rangle|^2$.

During the calibration of our experiment, we measured a lower bound on this quantity of $c = 1.89$, as shown in Fig. 2D, where we plotted the probability of detection matrices for all input states. Specifically, we measured all eight states in both bases and calculated the overlap of the prepared and measured states. When a state is measured in the same basis in which it is prepared, the probability should be ~ 1, as indicated by the data along the diagonal. The quantity c corresponds to the logarithm of the maximum of the anti-diagonal elements, where the measurement and preparation bases are different. For ideal state preparation and measurement, the overlap is 1/4, corresponding to $c = 2$; however, in the experiment, these matrix elements varied about 1/4, and we picked the element that gives the worst-case estimate of c, as required by the overlap parameter defined above.

Finally, $H := -x \log_2(x/3) - (1 - x)\log_2(1 - x)$ is the Shannon entropy for $d = 4$, $\mathrm{leak}_{EC} = 1.16\, H(x)$ is the number of bits published during error correction, and $\Delta_{FK} := -\log(32\beta^{-8}\varepsilon_{cor}^{-1})$. The secret key length is maximized numerically over β satisfying $4\varepsilon_{cor} + 18\beta \leq \varepsilon$ (section S1).

Phase-state detection

We described here our method for measuring the phase states because this system has not yet been widely discussed in the literature. The interferometric setup required to perform the phase basis measurement consists of a cascade of three interferometers, as shown in Fig. 2C, where the second stage of the tree has interferometers whose

time delay (τ) is a factor of 2 shorter than the interferometer in the first stage (2τ) (*28*).

When a phase state $|f_n\rangle$ (n = 0, 1, 2, 3) enters the interferometric setup, the first 50/50 BS of DI 1 splits the wave packet into two equal parts, with one part propagating through a longer arm relative to the other. The longer arm of the interferometer is set to delay the propagation of the wave packet by 2τ (two time bins) relative to the part propagating through the shorter arm. The two parts of the wave packet then recombine at a second 50/50 BS in DI 1, resulting in an interference pattern at the two outputs denoted by + and −.

In the second-stage interferometers, the wave packets propagating through the longer arms are delayed by just one time bin before interfering with the part propagating through the shorter arms. The expected interference patterns, representing the probability distribution function (PDF) of the single-photon wave packets, when state $|f_0\rangle$ propagates through the interferometric setup are shown in Fig. 2D.

It is seen that the wave packets emerging from the interferometers occupy seven time bins, where there is a 75% chance that a photon is detected outside the central time bin in each channel. The central time bin is due to the interference of all four wave packet peaks of the incident state, and there is a one-to-one correspondence between the incident phase state $|f_n\rangle$ and detection events in this time bin for detector *Dn*. We only used these events in our security analysis. Except for the outermost peaks, the other peaks are due to interference of a subset of the incident wave packet peaks. Although some information about the incident state could be extracted from the measurement of photons in these peaks, we did not consider this here.

A detailed analysis reveals that the sifting process ensures that there is no increase in error rate due to the spillover of these wave packets into the neighboring frames. However, the lower probability for a detection event in the central time bin reduces the overall number of events used in our security analysis and hence lowers our secret key rate. On the other hand, the higher-dimension protocol used here has higher noise tolerance and allows for a higher secure rate (*12*).

Transmitter design

The entire system is driven with serial pattern generators realized on an FPGA, which are used to generate the photonic wave packets in different bases and different intensities. The FPGA memory is preloaded with a fixed pattern sequence, representing Alice's bases and signal choices, and repeated until $N = 6.25 \times 10^{10}$ is achieved. Specifically, the pattern consists of time and phase basis states, chosen with probabilities p_T = 0.90 and p_F = 0.10, respectively. The three-intensity decoy levels are also preset on the FPGA serial pattern generators to create time and phase basis states of different mean photon numbers.

Generating a provable secure key from a QKD system requires real-time generation of quantum random numbers for state and basis selection. For our system, this requires a random number generator operating at 625 MHz, which is our state generation rate. We intended to use real-time quantum random number generators in the future once they can operate at the required rate and are commercially available.

SUPPLEMENTARY MATERIALS

Supplementary material for this article is available at http://advances.sciencemag.org/cgi/content/full/3/11/e1701491/DC1

section S1. Finite-key estimates for the experiment
section S2. Secret key rate simulation
section S3. Detector efficiency calibration
section S4. Numerically optimized secret key rate
section S5. Experimental parameters
section S6. Generation of the phase states
fig. S1. Efficiency of single-photon detectors.
fig. S2. Numerical simulation.
fig. S3. Graphical illustration of all phase states in d = 4.
fig. S4. Generation of phase states.
table S1. Length of sifted data.
References (*38*–*40*)

REFERENCES AND NOTES

1. S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, C. Monroe, Demonstration of a small programmable quantum computer with atomic qubits. *Nature* **536**, 63–66 (2016).
2. N. M Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, C. Monroe, Experimental comparison of two quantum computing architectures. *Proc. Natl. Acad. Sci. U.S.A.* **114**, 3305–3310 (2017).
3. T. S. Metodi, D. D. Thaker, A. W. Cross, F. T. Chong, I. L. Chuang, A quantum logic array microarchitecture: Scalable quantum data movement and computation, *Proceedings of the 38th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO 38 2005)*, Barcelona, Spain, 12 to 16 November 2005 (IEEE Computer Society, 2005).
4. M. Ahsan, R. V. Meter, J. Kim, Designing a million-qubit quantum computer using a resource performance simulator. *ACM J. Emerg. Technol. Comput. Syst.* **12**, 39 (2015).
5. S. M. Barnett, Quantum information, in *Oxford Master Series in Physics* (Oxford Univ. Press, 2009).
6. H.-K. Lo, M. Curty, K. Tamaki, Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2014).
7. E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 16025 (2016).
8. 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, S. W. Nam, Detecting single infrared photons with 93% system efficiency. *Nat. Photonics* **7**, 210–214 (2013).
9. Q. Zhao, T. Jia, M. Gu, C. Wan, L. Zhang, W. Xu, L. Kang, J. Chen, P. Wu, Counting rate enhancements in superconducting nanowire single-photon detectors with improved readout circuits. *Opt. Lett.* **39**, 1869–1872 (2014).
10. H. Bechmann-Pasquinucci W. Tittel, Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).
11. N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Security of quantum key distribution using *d*-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
12. L. Sheridan V. Scarani, Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82**, 030301 (2010).
13. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, A. Zeilinger, Experimental quantum cryptography with qutrits. *New J. Phys.* **8**, 75 (2006).
14. J. Leach, E. Bolduc, D. J. Gauthier, R. W. Boyd, Secure information capacity of photons entangled in many dimensions. *Phys. Rev. A* **85**, 060304 (2012).
15. M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, R. W. Boyd, High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
16. G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, G. Lima, High-dimensional decoy-state quantum key distribution over 0.3 km of multicore telecommunication optical fibers. *Phys. Rev. A* **96**, 022317 (2016).
17. Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, L. K. Oxenløwe, High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Inf.* **3**, 25 (2017).
18. T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, D. J. Gauthier, Security of high-dimensional quantum key distribution protocols using Franson interferometers. *J. Phys. B At. Mol. Opt. Phys.* **46**, 104010 (2013).
19. J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, D. Englund, High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A* **87**, 062322 (2013).
20. D. J. Gauthier, C. F. Wildfeuer, H. Guilbert, M. Stipčević, B. G. Christensen, D. Kumor, P. Kwiat, K. T. McCusker, T. Brougham, S. Barnett, Quantum key distribution using hyperentangled time-bin states, *The Rochester Conferences on Coherence and Quantum Optics and the Quantum Information and Measurement Meeting (CQO and QIM 2013)*, Rochester, NY, 17 to 20 June 2013 (Optical Society of America, 2013).
21. 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, F. N. C. Wong, Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding. *New J. Phys.* **17**, 022002 (2015).

22. T. Brougham, C. F. Wildfeuer, S. M. Barnett, D. J. Gauthier, The information of high-dimensional time-bin encoded photons. *Eur. Phys. J. D* **70**, 214 (2016).
23. C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, D. Englund, High-rate field demonstration of large-alphabet quantum key distribution. https://arxiv.org/abs/1611.01139 (2016).
24. W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
25. H.-K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
26. X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
27. C. C. W. Lim, M. Curty, N. Walenta, F. Xu, H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
28. N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, D. J. Gauthier, Robust and stable delay interferometers with application to *d*-dimensional time-frequency quantum key distribution. *Phys. Rev. Applied* **7**, 044010 (2017).
29. M. Tomamichel R. Renner, Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106**, 110506 (2011).
30. M. Tomamichel, C. C. W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
31. K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent, R. Boyd, Finite-key security analysis for multilevel quantum key distribution. *New J. Phys.* **18**, 073030 (2016).
32. B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, H. Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photonics* **9**, 163–168 (2015).
33. 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, E. Karimi, High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).
34. L. Kral, I. Prochazka, K. Hamal, Optical signal path delay fluctuations caused by atmospheric turbulence. *Opt. Lett.* **30**, 1767–1769 (2005).
35. W. Sun, L.-J. Wang, X.-X. Sun, H.-L. Yin, B.-X. Wang, T.-Y. Chen, J.-W. Pan, Integration of quantum key distribution and gigabit-capable passive optical network based on wavelength-division multiplexing. https://arxiv.org/abs/1604.07578 (2016).
36. M. D. Shaw, F. Marsili, A. D. Beyer, J. A. Stern, G. V. Resta, P. Ravindran, S. Chang, J. Bardin, D. A. Russell, J. W. Gin, F. D. Patawaran, V. B. Verma, R. P. Mirin, S. W. Nam, W. H. Farr, Arrays of WSi superconducting nanowire single photon detectors for deep space optical communications, *CLEO: 2015*, San Jose, CA, 10 to 15 May 2015 (Optical Society of America, 2015).
37. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, A. J. Shields, Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **21**, 24550–24565 (2013).
38. J. Müller-Quade R. Renner, Composability in quantum cryptography. *New J. Phys.* **11**, 085006 (2009).
39. M. Tomamichel M. Hayashi, A hierarchy of information quantities for finite block length analysis of quantum tasks. *IEEE Trans. Inf. Theory* **59**, 7693–7710 (2013).
40. R. Konig, R. Renner, C. Schaffner, The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55**, 4337–4347 (2009).

Acknowledgments: We acknowledge discussion of this work with P. Kwiat and A. Aragoneses and thank D. Kumor for providing us custom time tagger data collection software.
Funding: We acknowledge the financial support of the Office of Naval Research Multidisciplinary University Research Initiative program on Wavelength-Agile QKD in a Marine Environment (grant N00014-13-1-0627) and the Defense Advanced Research Projects Agency Defense Sciences Office Information in a Photon program. C.C.W.L. acknowledges support from the Oak Ridge National Laboratory, operated by UT-Battelle for the U.S. Department of Energy under contract no. DE-AC05-00OR22725, and support from National University of Singapore startup grant R-263-000-C78-133/731. **Author contributions:** D.J.G. conceived the concept and helped design the experiment. N.T.I. designed, developed, and performed the experiment. C.C., D.J.G., and J.K. designed the readout circuit for the single-photon detectors. C.C.W.L. and N.T.I. performed the security analysis. N.T.I. performed the data analysis and numerical simulation. All authors contributed to writing the manuscript.
Competing interests: The authors declare that they have no competing interests.
Data and materials availability: All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper may be requested from the authors.

Submitted 7 May 2017
Accepted 2 November 2017
Published 24 November 2017
10.1126/sciadv.1701491

Citation: N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits. *Sci. Adv.* **3**, e1701491 (2017).

Science Advances

Provably secure and high-rate quantum key distribution with time-bin qudits

Nurul T. Islam, Charles Ci Wen Lim, Clinton Cahall, Jungsang Kim and Daniel J. Gauthier

Sci Adv **3** (11), e1701491.
DOI: 10.1126/sciadv.1701491