Quantum Communication with Ultrafast Time-Bin Qubits

Frédéric Bouchard,[1,*] Duncan England,[1] Philip J. Bustard,[1] Khabat Heshami,[1,2] and Benjamin Sussman[1,2]

[1] *National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada*

[2] *Department of Physics, University of Ottawa, Advanced Research Complex, 25 Templeton Street, Ottawa, Ontario K1N 6N5, Canada*

(Received 17 June 2021; revised 6 January 2022; accepted 3 February 2022; published 28 February 2022)

The photonic temporal degree of freedom is one of the most promising platforms for quantum communication over fiber networks and free-space channels. In particular, time-bin states of photons are robust to environmental disturbances, support high-rate communication, and can be used in high-dimensional schemes. However, the detection of photonic time-bin states remains a challenging task, particularly for the case of photons that are in a superposition of different time bins. Here, we experimentally demonstrate the feasibility of picosecond time-bin states of light, known as ultrafast time bins, for applications in quantum communications. With the ability to measure time-bin superpositions with excellent phase stability, we enable the use of temporal states in efficient quantum key distribution protocols such as the BB84 protocol.

DOI: 10.1103/PRXQuantum.3.010332

I. INTRODUCTION

Quantum communication is the branch of quantum technologies that deals with the distribution of quantum states of light to achieve a specific communication task. The most well known and developed quantum communication protocol is quantum key distribution (QKD), which allows two remote parties to share a secret key, enabling private communication [1–3]. In its simplest form, QKD requires two mutually unbiased two-dimensional bases in which states can be prepared by a sender, Alice, transmitted, and measured by a receiver, Bob. High fidelity is required between the prepared state and the measured state. Loss and decoherence are therefore major challenges in practical QKD implementations, because they reduce, and eventually eliminate, the useful capacity of a communication channel. The decoherence encountered is strongly influenced by the quantum states employed and the mode of transmission. Various optical states have been exploited for QKD, including position bins, spatial modes, time bins, and polarization states [4–9].

The polarization degree of freedom has been the most widely deployed [10–13], not least because polarization states are easy to generate, manipulate, and measure using high-specification off-the-shelf components. However, polarization states are not amenable to long-distance fiber transmission due to issues such as birefringence, polarization mode dispersion, polarization-dependent loss, and the requirement for fast polarization compensation [14]; use of polarization states is, therefore, mainly restricted to free-space transmission. On the other hand, time-bin states can be straightforwardly generated using fast optical modulators, transmitted over long distances in fibers and free space [15,16], and can support high-dimensional encoding [17] leading to a larger information capacity and an improved noise tolerance [18]. However, their detection remains particularly challenging in terms of stability, efficiency, and flexibility. This is mainly due to the necessity of measuring time-bin superpositions, which generally requires imbalanced, or *time-delayed*, interferometers [19,20]. In particular, the path difference between two arms of a time-delayed interferometer is dictated by the time-bin separation time, which is typically on the order of 1 ns, generally matching the timing jitter of standard single-photon detectors. In practice, this amounts to a path difference of approximately 30 cm. Experimentally, achieving subwavelength interferometric phase stability over such a large path difference remains technically challenging due to various experimental disturbances, even with the use of active phase stabilization. Moreover, this active-stabilization feedback loop increases the complexity of the overall system and may open the door to further attacks by an eavesdropper. Thus, the development of

*frederic.bouchard@nrc-cnrc.gc.ca

novel techniques with improved phase stability to measure time-bin superposition states of photons is critical to enhance the performance of time-bin quantum communication systems.

A promising pathway toward achieving improved interferometric stability consists of reducing the path difference of the time-delayed interferometer, consequently reducing the time-bin separation time. However, this requires the use of single-photon detectors with lower timing jitter. With recent developments in superconducting-nanowire single-photon detectors (SNSPDs), timing jitters as low as 50 ps can now be achieved in commercial devices [21] and 3 ps in state-of-the-art devices [22]. Nevertheless, such detectors still require cooling to approximately 1 K, which again increases the complexity of the detection apparatus. SNSPDs have enabled the successful use of time bins with subnanosecond bin width in quantum communication demonstrations [23]. By preparing time bins with a bin width of 400 ps, a delay interferometer can be made into a compact package where interferometric stability is achieved without active stabilization for up to an hour [24]. Nevertheless, such passive interferometric schemes still suffer from limited measurement efficiency in the superposition basis due to the noninterfering measured events.

Recent developments in ultrafast quantum optics [25,26] add to the current experimental toolbox for photonic time-based quantum information processing. The shifting of time-bin qubits to the realm of ultrafast pulses allows the bin widths to be compressed to as low as a few picoseconds. Time-delayed interferometers then only require path differences of a few hundred micrometers, offering the potential for intrinsic passive interferometric stability over long periods of time. Here, we propose and experimentally perform a proof-of-principle quantum communication experiment using ultrafast time bins [27], with a bin width of $\Delta\tau = 4.5$ ps and complete encoding of the qubit in a 7-ps window. These ultrafast time-bin states offer potential advantages by enabling the efficient generation and detection of time-bin states without necessitating active phase stabilization. The time-delayed interferometers required first for qubit creation, and later for measurement in the phase basis, are each based on birefringent crystals. The two arms of each interferometer are collinear and their path difference is due to the difference in group index experienced by pulses with orthogonal polarizations in the crystal. For example, a 10-mm-long α-barium borate (BBO) crystal can induce a time delay of $\Delta\tau = 4.5$ ps between orthogonally polarized pulses at 720.8 nm. Such common-path interferometers have excellent passive phase stability and require no active phase compensation. The ultrafast bin widths are significantly smaller than the timing jitter of conventional single-photon detectors. The time of arrival of the time-bin states is therefore measured by ultrafast polarization switching using cross-phase modulation in a single-mode fiber, applied with an intense ultrafast control pulse [27,28] (see Fig. 1). Moreover, in the superposition (phase) basis, we take advantage of the cross-phase modulation polarization switching to deliver a measurement efficiency for our scheme of 100%, in theory, compared to a measurement efficiency of 50% for standard time-delayed interferometery measurements, where noninterfering events give no information about the relative phase of time-bin superpositions.

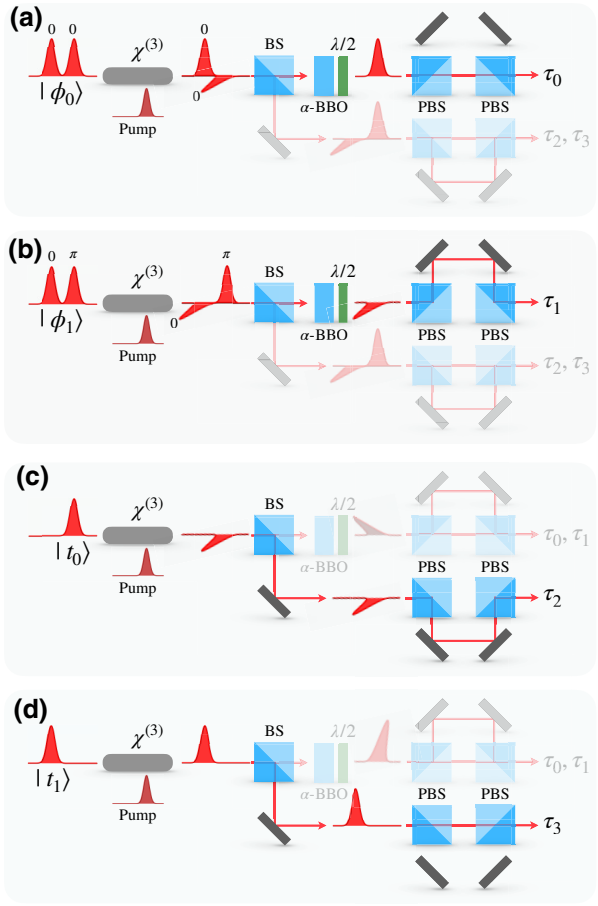

FIG. 1. The measurement of time-bin states. The conceptual experimental setup for (a),(b) the phase-basis measurement and (c),(d) the time-basis measurement. A strong pump is overlapped with the t_0 time bin inside a $\chi^{(3)}$ material, rotating its polarization. A 50:50 beam splitter randomly selects one of two measurement settings, i.e., the phase basis (upper) or time basis (lower). In the scenario where the input state is prepared in one basis but measured in the other basis (the shaded part of the setup), the measurement outcomes are random and will later be sifted. $\chi^{(3)}$, third-order nonlinear material; BS, beam splitter; $\lambda/2$, half-wave plate; PBS, polarizing beam splitter.

II. EXPERIMENT

We demonstrate the experimental feasibility of ultrafast time-bin qubits for quantum communication by

performing a proof-of-principle experiment of a time-bin-based decoy-state BB84 protocol. Our experiment consists of a sender, *Alice*, and a receiver, *Bob*. Alice prepares weak coherent pulses (WCPs) by attenuating ultrafast pulses to the single-photon level. The mean photon number of the WCPs is optimized given the channel conditions, e.g., the channel loss and the quantum bit error rate (QBER). The pulses are obtained from an optical parametric oscillator pumped by a Ti:sapphire laser at a repetition rate of $f_{\text{rep}} = 80$ MHz. Pulses are generated at a central wavelength of $\lambda_{\text{signal}} = 720.8$ nm with a spectral bandwidth of $\Delta\lambda_{\text{signal}} = 1.7$ nm full width at half maximum. In the original BB84 protocol, Alice randomly selects one of four polarization states and transmits the encoded photons to Bob. These four states belong to two mutually unbiased bases (MUBs), i.e., a computational basis and a superposition basis. For time bins, these two bases are usually referred to as the *time basis* and the *phase basis*, where the former contains the states $|t_0\rangle$ and $|t_1\rangle$ and the latter contains the states $|\phi_0\rangle = 1/\sqrt{2}\,(|t_0\rangle + |t_1\rangle)$ and $|\phi_1\rangle = 1/\sqrt{2}\,(|t_0\rangle - |t_1\rangle)$, respectively. Using a half-wave plate (HWP), an α-BBO crystal and a polarizing beam splitter (PBS), Alice generates all four time-bin states by varying the angle of the HWP to 0°, 45°, −22.5°, and 22.5° [see Fig. 2(a)]. We note that for a realistic implementation of this protocol, which is beyond the scope of this work, fast optical modulators would be necessary for the time-bin state preparation, the pulse intensity preparation of the signal and decoy states, and the pulse-to-pulse phase randomization.

Upon receiving the transmitted photons, Bob measures the time-bin states and generates a raw key by assigning a value of 0 to the measured state if it is found to be in the state $|t_0\rangle$ or $|\phi_0\rangle$ and a value of 1 when it is found to be in $|t_1\rangle$ or $|\phi_1\rangle$. In order to measure the ultrafast time-bin states, a synchronized pump pulse is combined with the signal pulses using a dichroic mirror (DM). The signal and pump pulses are then coupled to a single-mode fiber (SMF), with a coupling efficiency of 50% and 65%, respectively. The pump pulses are prepared at a center wavelength of $\lambda_{\text{pump}} = 800$ nm and are spectrally filtered with a pair of angle-tuned bandpass filters such that $\Delta\lambda_{\text{pump}} = 2.1$ nm. In the presence of the strong pump pulse, the third-order nonlinearity of the SMF is used

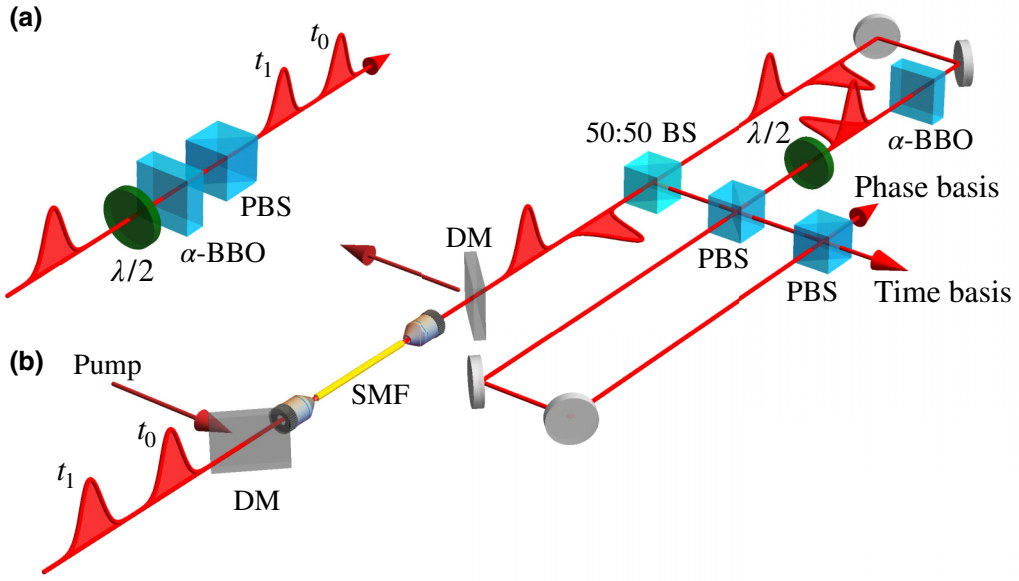

FIG. 2. The experimental setup. A simplified experimental setup showing the state preparation and the state detection of ultrafast time-bin qubit states in a BB84 protocol experiment. (a) In the state-preparation stage, an ultrashort pulse is sent to a 10-mm-long α-BBO birefringent crystal, splitting the input pulse into two output pulses with orthogonal polarization separated by 4.5 ps. A polarizing beam splitter (PBS) is then used to erase the polarization information associated with each time bin, resulting in a uniformly polarized time-bin state. The weight and relative phase of the time-bin state can be determined by a half-wave plate ($\lambda/2$), placed before the α BBO. (b) In the detection stage, the signal pulse is combined with a strong pump pulse at a dichroic mirror (DM) and then coupled to a single-mode fiber where the pump pulse switches the early time bin. The pump pulse is then filtered out using a DM and further spectral filters not shown in the figure. A 50:50 beam splitter (BS) is used to randomly switch the measurement setting from the time basis (the reflected output) to the phase basis (the transmitted output). In the time basis, a delayed interferometer is designed with a path difference of 88 cm such that the time-bin state can be detected by measuring the time of arrival of the pulse with standard single-photon detectors. In the phase basis, a second 10-mm α-BBO crystal is used to recombine the pulses and convert the relative phase information to polarization. The same delayed interferometer can be used in parallel where the phase state is determined from the time of arrival of detected pulses.

to induce a birefringence in the SMF, causing a rotation of the polarization of the signal pulses at time t_0 using cross-phase modulation via the optical Kerr effect. We note that for time-bin superposition states, the relative phase between the states $|t_0\rangle$ and $|t_1\rangle$ is preserved up to an additional constant phase introduced by the pump during the polarization rotation. It has been shown that such an optical switch can rotate the polarization of single-photon pulses with unit efficiency while introducing very little noise [28]. The switching efficiency, η, of the signal pulses is given by

$$\eta = \sin^2(2\theta)\sin^2\left(\frac{\Delta\phi}{2}\right), \tag{1}$$

where θ is the angle between the polarization of the signal and pump pulses, $\Delta\phi = 8\pi n_2 L_{\text{eff}}/3\lambda_{\text{signal}}$ is the induced nonlinear phase shift in the SMF in the presence of the pump pulse, n_2 is the nonlinear refractive index of the SMF, L_{eff} is the effective length of the nonlinear medium, and I_{pump} is the intensity of the pump. A unit switching efficiency is achieved by setting $\theta = \pi/4$, $\Delta\phi = \pi$ and by taking advantage of the group-velocity mismatch between the signal and pump wavelength in the SMF to achieve a full temporal walkoff of the signal and the pump pulses.

After mapping the ultrafast time bins onto orthogonal polarization states, we use a polarizing delayed interferometer with a path difference of 88 cm to map the distinct polarization states to separate nanosecond time bins, which can then be straightforwardly detected by avalanche photodiodes (APDs) and processed using a time-to-digital converter (TDC) (Swabian Instruments, Time Tagger Ultra). The path difference of the polarizing delayed interferometer here is determined by the timing jitter of our single-photon detectors and does not represent a limiting factor for the secret-key rate of our scheme. As is required in the BB84 protocol, Bob randomly varies the measurement basis between the time basis and the phase basis: a 50:50 beam splitter (BS) directs the photons randomly to the two alternative measurement pathways [see Fig. 2(b)] through the shared polarizing delayed interferometer. In the time-basis pathway, propagation through the polarizing delayed interferometer maps the two orthogonal polarizations directly to distinct time bins at the time-basis exit port. In the phase-basis pathway, the time difference between the orthogonal polarization states is initially compensated using an α-BBO crystal, with the resulting interference mapping the phase information to polarization. This compact setup delivers a high phase stability for phase-basis measurements. The polarizing delayed interferometer then maps the two orthogonal polarizations directly to distinct time bins at the phase-basis exit port. The sharing of the polarizing delayed intereferometer for the time and phase bases allows measurement of the four distinct states with only two APDs, while maintaining a compact footprint. We note that the polarizing delayed interferometer is only used to measure polarization and does not require phase stability since no interference occurs at the output ports. The final nanosecond signal pulses are analyzed to determine the state sent from Alice (see Fig. 3). In particular, a temporal window of 1.04 ns is defined for each time-bin state. The probability of detection $P_{i,j}^{(\alpha,\beta)} = \left|\langle\psi_j^{(\beta)}|\psi_i^{(\alpha)}\rangle\right|^2$ is experimentally determined, where $|\psi_0^{(0)}\rangle = |\phi_0\rangle$, $|\psi_1^{(0)}\rangle = |\phi_1\rangle$, $|\psi_0^{(1)}\rangle = |t_0\rangle$, and $|\psi_1^{(1)}\rangle = |t_1\rangle$. The measurement bases α and β correspond to Alice's preparation basis and Bob's measurement basis, respectively. The probability

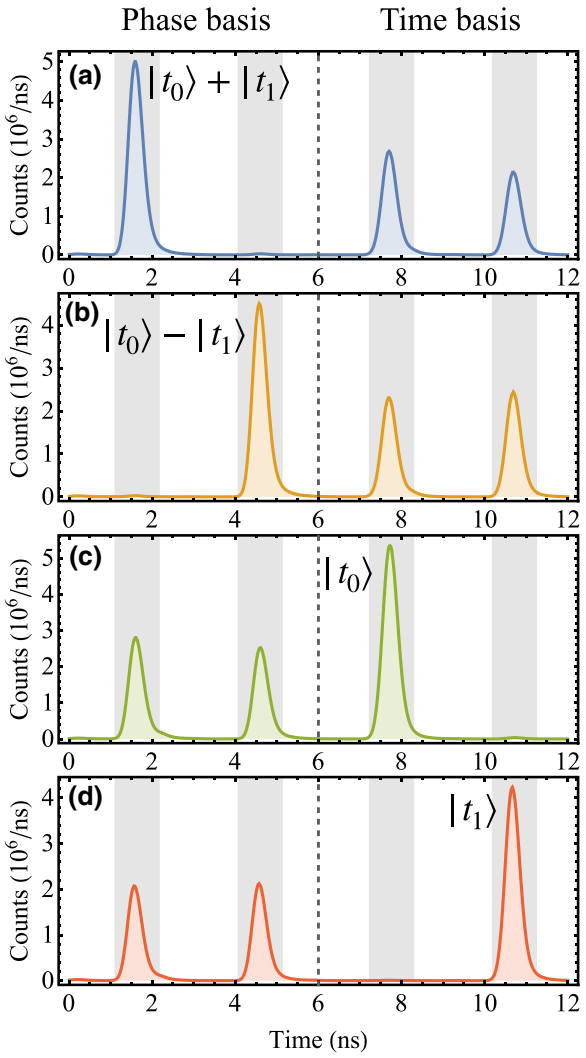

FIG. 3. Time-bin states measurement. (a),(b) Phase-basis measurement: the single-photon data. (c),(d) Time-basis measurement: the shaded area represents the temporal window corresponding to each time-bin state. The number of counts shown is taken for an integration time of 1 s. The gray dotted line shows the separation between the phase basis and the time basis.

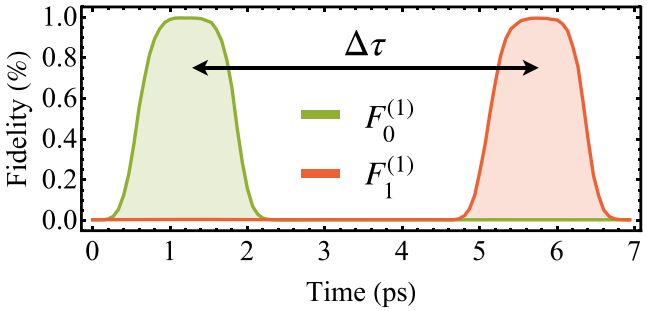

FIG. 4. Pump-delay measurements. Measurement of the state fidelity for the time basis, i.e., $F_0^{(1)}$ (solid green curve) and $F_1^{(1)}$ (solid red curve). The arrow shows the time-bin separation, or bin width, $\Delta\tau$. The shape of the fidelity curve as a function of the pump delay is dictated by the pulse duration of the pump and signal and by the difference in group velocity of the pump and signal inside the SMF.

of detection is obtained from measured detection events, i.e., $P_{i,j}^{(\alpha,\beta)} = N_{i,j}^{(\alpha,\beta)} / \sum_{k=0}^{1} N_{i,k}^{(\alpha,\beta)}$. The state fidelity is then obtained from the probability of detection, i.e., $F_i^{(\alpha)} = P_{i,i}^{(\alpha,\alpha)}$.

We further characterize our experimental setup by varying the delay between the pump and signal pulses while measuring each output state. By repeating these measurements for all input states, we can extract information about the pump-pulse temporal profile and the temporal walkoff of the signal and pump pulses. The state fidelity in the time basis as a function of the pump delay is shown in Fig. 4. Moreover, we measure the temporal separation between the time states $|t_0\rangle$ and $|t_1\rangle$ to be $\Delta\tau = 4.5$ ps, in agreement with the expected value from the thickness of the α-BBO crystal.

III. RESULTS

We now test the experimental viability of ultrafast time-bin qubits in the context of quantum communication. In particular, we use our experimental generation and detection setting to perform a proof-of-principle QKD demonstration using the formalism of the decoy-state BB84 protocol [29–31], where the secret-key rate is the key metric of performance. As a first test, we measure the state fidelity for each input time-bin state over the course of 28 h [see Fig. 5(a)]. By doing so, we demonstrate the feasibility of using time-bin states in quantum communication, where time-delayed interferometry is inherently phase stable due to the small path difference and common-path nature of our interferometer. We show an average state fidelity in excess of 99%, corresponding to a QBER below 1% (see Fig. 5). Variations in the state fidelity over time can be attributed to slight fluctuations in the intensity or polarization of the pump pulses. We note that the time-bin state $|t_1\rangle$ has a much less variable state fidelity, since it is unaffected by the pump pulse. From the measurements in Fig. 5(a), we can calculate a probability-of-detection matrix, which is taken over the integration time of 28 h [see Fig. 6(a)]. Measurements done in different MUBs yield uncorrelated results that are subsequently discarded in the sifting phase of the BB84 protocol.

The performance of our experimental setup is then evaluated using the formalism of finite-key security

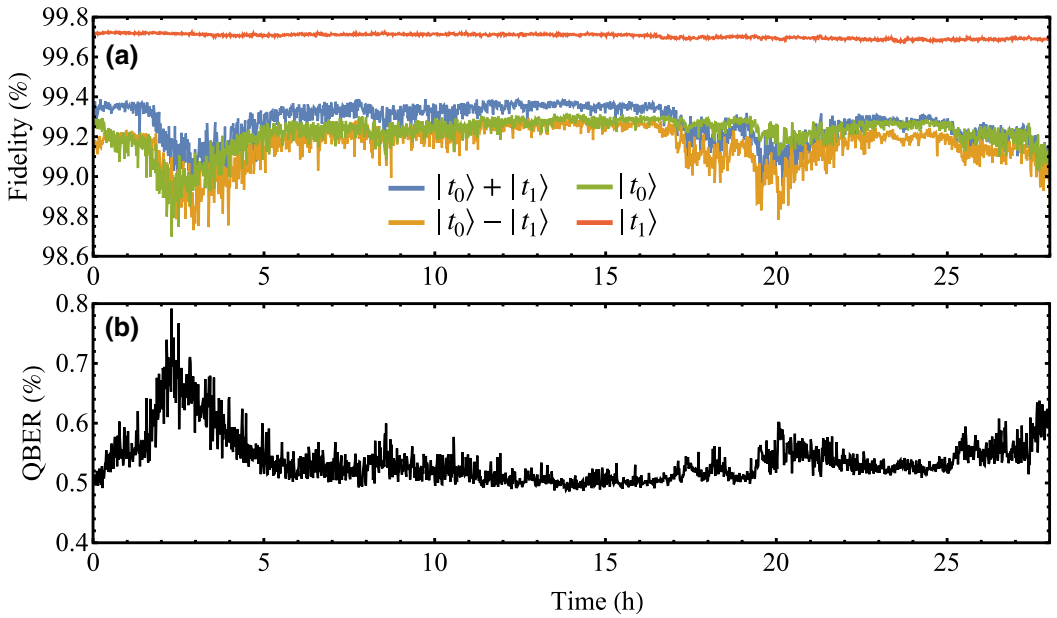

FIG. 5. Time-bin measurement over 28 h. (a). The state fidelity for all four measured states, i.e., $|\phi_0\rangle$ (blue curve), $|\phi_1\rangle$ (yellow curve), $|t_0\rangle$ (green curve), and $|t_1\rangle$ (red curve). (b) The QBER is calculated from the state fidelity averaged over all states.

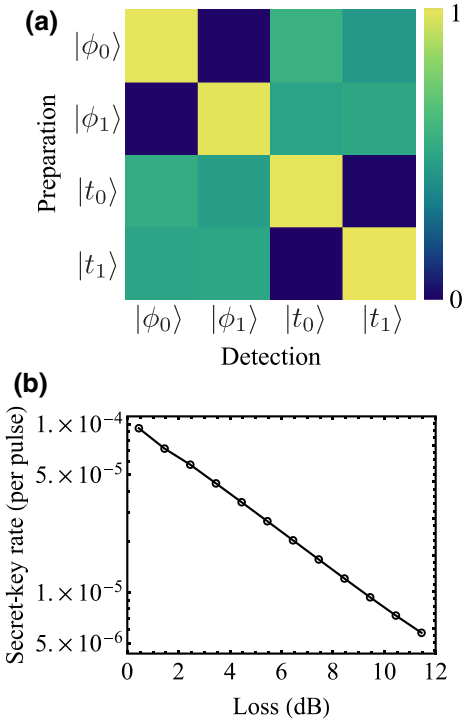

FIG. 6. QKD results. (a) The probability-of-detection matrix. The rows correspond to different prepared input time-bin states and the columns correspond to different measured output states. (b) The secret-key rate as a function of the channel loss.

bounds for the decoy-state BB84 protocol in the universally composable framework [32–34]. Following the standard procedure, our protocol is said to be $(\varepsilon_{\text{cor}}+\varepsilon_{\text{sec}})$-secure if it is ε_{cor}-correct and ε_{sec}-secret for small errors, $\varepsilon_{\text{cor}}, \varepsilon_{\text{sec}} > 0$.

In the preparation stage, Alice randomly selects between the time and phase basis with probabilities p_{Z} and p_{X} [35], where we label the time and phase basis with Z and X, respectively. With the decoy-state protocol, Alice randomly selects the intensity of her WCPs to be μ, ν, and ω, with probabilities, p_μ, p_ν, and p_ω, respectively, where the μ, ν, and ω intensities correspond to the signal state, the decoy state, and the vacuum-decoy state. In the measurement stage, Bob randomly selects a measurement basis with probabilities p_{Z} and p_{X} and assigns a bit value of 0 or 1 depending on which detector clicks in his measurement. For the case of double-detection events, a random bit value is assigned. After the basis reconciliation, Alice and Bob perform error correction, error verification, and privacy amplification to yield a final secret key of length ℓ. The final ε_{sec}-secret-key length is given by

$$\ell \geq s^L_{\mathsf{Z},0} + s^L_{\mathsf{Z},1}\left[1 - h\left(e^U_{\mathsf{X},1}\right)\right] - \text{leak}_{\text{EC}} - 6\log_2\frac{21}{\varepsilon_{\text{sec}}} - \log_2\frac{2}{\varepsilon_{\text{cor}}}, \tag{2}$$

where $s^L_{\mathsf{Z},0}$ is the lower bound of vacuum events in Z, $s^L_{\mathsf{Z},1}$ is the lower bound of single-photon events in Z, $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, $e^U_{\mathsf{X},1}$ is the upper bound of the phase error rate, $\text{leak}_{\text{EC}} = n_{\mathsf{Z},\mu}\, f_{\text{EC}}\, h(e_{\mathsf{Z},\mu})$ is the amount of information revealed by Alice and Bob during the error-correction step, $n_{\mathsf{Z},\mu}$ is the number of detected signal pulses in Z, f_{EC} is the error-correction efficiency, $e_{\mathsf{Z},\mu} = m_{\mathsf{Z},\mu}/n_{\mathsf{Z},\mu}$ is the QBER, and $m_{\mathsf{Z},\mu}$ is the number of bit errors from signal pulses in Z. The standard error-correction efficiency factor of $f_{\text{EC}} = 1.16$ is used in our analysis. The formulas for the estimation of the above parameters are given in Appendix A. Finally, the secret-key rate R is given by

$$R = \ell/N, \tag{3}$$

where N is the number of laser pulses sent by Alice.

In our analysis, we consider a security level of $\varepsilon_{\text{cor}} = 10^{-15}$ and $\varepsilon_{\text{sec}} = 10^{-10}$. The block size N is chosen for an integration time of 5 min, i.e., $N = 2.4\times10^{10}$. From the averaged probability-of-detection matrix, we obtain an averaged QBER of $e_{\mathsf{Z},\mu} = (0.8 \pm 0.3)$ % over the integration time of 28 h. The mean photon number of the signal pulse is set to $\mu = 0.8$ and the brightness of the decoy states ν is optimized depending on the channel conditions. This is achieved using a combination of neutral-density filters, a HWP mounted in a motorized stage, and a PBS. The probabilities p_μ and p_ν are also optimized for different channel losses. The modulation of the signal and decoy states guarantees the security of our demonstration against photon-number-splitting attacks. An additional pair of HWPs and PBSs is used to introduce losses in the channel. The secret-key rate is then measured for channel-loss conditions varying from 0.45 to 12 dB channel loss. Hence, the total loss of our system is varied from 14.6 to 26.1 dB, with an additional 3 dB SMF coupling loss, a 2.2 dB detector efficiency loss, and another 8.9 dB loss at Bob's detection stage (wave plates, PBS, α BBO, and spectral filters). The secret-key rate per pulse, R, is shown in Fig. 6(b) as a function of the channel loss.

IV. DISCUSSION AND OUTLOOK

From our QKD demonstration, we experimentally demonstrate that ultrafast time-bin qubits offer a versatile platform for QKD where standard protocols such as the BB84 protocol can now be considered due to the ability to directly measure the time-bin states in MUBs with high detection efficiencies. Previously, the temporal degree of freedom of photons has been an important candidate in quantum communication, particularly due to its ease of use in fiber networks. However, due to the lack of efficient, stable, and passive measurement techniques for time-bin superposition states, more complicated

QKD protocols are yet to be employed. For example, the differential phase shift [8], the coherent one-way [36], and the round-robin differential phase shift [17] protocols have been specifically designed to overcome the technical difficulties associated with measuring time-bin qubits. On the other hand, the BB84 protocol, initially designed for polarization states, offers a higher overall efficiency, a simpler postprocessing, and has well-studied security considerations in practical implementations [3].

Another QKD protocol with a high efficiency is the six-states protocol [37], where an additional MUB is considered. Though reducing the sifting efficiency, the tomographic nature of the protocol results in a slightly larger error threshold, which can translate to a larger amount of loss tolerability. We note that our experimental setup is also suited to perform the six-states protocol, where a quarter-wave plate is added to both the preparation and detection stages. This will result in the generation and measurement of a third MUB consisting of the states $(|t_0\rangle \pm i|t_1\rangle)/\sqrt{2}$. The addition of the third MUB would allow the tomographic reconstruction of ultrafast time-bin qubits.

In using ultrafast pulses, we are taking advantage of the favorable properties of near-Fourier-transform-limited pulses to encode information onto photons in the most condensed manner possible. Our experiment uses signal pulses that are in a near-single spectrotemporal mode. In the ultrafast regime, we have direct access to both the temporal and spectral domains. This feature, which is notable with ultrafast pulses, can be exploited to achieve passive noise filtering on both the temporal and spectral degrees of freedom. By doing so, a noise tolerance approaching the ultimate limit in QKD can be achieved [38,39], where this approach is compatible with the use of ultrafast time-bin qubits. In practical scenarios, this consideration is particularly important since beyond the loss simulated in our experiment, environmental noise and channel disturbances will lead to additional errors in the raw key, which are effects not captured by our experimental demonstration. Moreover, mature technologies exist to compensate for channel disturbances such as chromatic dispersion occurring in long-distance fiber networks. Finally, we note that our experimental platform can be extended to more general time-bin states such as two-photon entangled states and high-dimensional time-bin states, also known as *qudits*. Our technique using cross-phase modulation inside an SMF via the optical Kerr effect is compatible with the measurement of entangled and qudit states, leading to the development of a larger toolkit to perform quantum communication in the time domain.

There are now several factors limiting the performance of current state-of-the-art QKD systems. In particular, limitations in secret-key rates may be caused by source flaws, noise in the communication channel, detector performance, or repetition rates of the overall system. In the latter case, QKD systems with repetition rates up to 2.5 GHz have been demonstrated for high secret-key rates [40] and over longer distances [15]. Although increasing the repetition rates of QKD systems might result in technical and security challenges [12], it also offers a path to larger secret-key rates. With a total encoding time window of 7 ps for our ultrafast time-bin states, a repetition rate of up to a 100 GHz would be compatible with our scheme.

In conclusion, we experimentally demonstrate the use of ultrafast time-bin qubits in quantum communication by experimentally investigating the performance of a proof-of-principle decoy-state BB84 QKD protocol. By significantly reducing the size of the time bins from nanoseconds to picoseconds, we enable the use of time-delayed interferometers with excellent inherent phase stability. Here, this is achieved using a 10-mm-thick birefringent crystal as a common-path time-delayed interferometer. Thus, an average state fidelity in excess of 99% is achieved over a period of time of 28 h. These results provide a pathway to achieve larger secret-key rates by taking advantage of the extremely small encoding time window. Moreover, this new platform is compatible with quantum communication systems through fiber networks or free space.

ACKNOWLEDGMENTS

This work is supported by the High Throughput Secure Networks Challenge Program at the National Research Council of Canada, the Natural Sciences and Engineering Research Council of Canada, and the University of Ottawa–NRC Joint Centre for Extreme Photonics. We thank Ebrahim Karimi, Rune Lausten, Denis Guay, Doug Moffatt, Kent Bonsma-Fisher, and Kate Fenwick for support and insightful discussions.

APPENDIX: PARAMETER ESTIMATIONS

From experimentally measured quantities such as the number of signal, decoy, and decoy-vacuum pulses in Z and X—respectively, $n_{\mathsf{Z},\mu}$, $n_{\mathsf{Z},\nu}$, $n_{\mathsf{Z},\omega}$, $n_{\mathsf{X},\mu}$, $n_{\mathsf{X},\nu}$, and $n_{\mathsf{X},\omega}$—and the number of bit errors from signal, decoy, and decoy-vacuum pulses in Z and X—respectively, $m_{\mathsf{Z},\mu}$, $m_{\mathsf{Z},\nu}$, $m_{\mathsf{Z},\omega}$, $m_{\mathsf{X},\mu}$, $m_{\mathsf{X},\nu}$, and $m_{\mathsf{X},\omega}$—it is possible to estimate the parameters that are required for the calculation of the secret-key length, namely, $s^L_{\mathsf{Z},0}$, $s^L_{\mathsf{Z},1}$, and $e^U_{\mathsf{X},1}$. Following the analysis in Ref. [34], we obtain the following formulas:

$$s^L_{\mathsf{Z},0} = \frac{\tau_0}{\nu-\omega}\left(\frac{\nu e^{\omega} n^L_{\mathsf{Z},\omega}}{p_\omega} - \frac{\omega e^{\nu} n^U_{\mathsf{Z},\nu}}{p_\nu}\right), \tag{A1}$$

$$s^L_{\mathsf{Z},1} = \frac{\mu\tau_1}{\mu(\nu-\omega)-(\nu^2-\omega^2)}\left[\frac{e^{\nu} n^L_{\mathsf{Z},\nu}}{p_\nu} - \frac{e^{\omega} n^U_{\mathsf{Z},\omega}}{p_\omega} - \frac{\nu^2-\omega^2}{\mu^2}\left(\frac{e^{\mu} n^U_{\mathsf{Z},\mu}}{p_\mu} - \frac{s^L_{\mathsf{Z},0}}{\tau_0}\right)\right], \tag{A2}$$

$$e^U_{\mathsf{X},1} = \frac{v^U_{\mathsf{X},1}}{s^L_{\mathsf{X},1}} + \gamma\left(\varepsilon_{\text{sec}}, \frac{v^U_{\mathsf{X},1}}{s^L_{\mathsf{X},1}}, s^L_{\mathsf{X},1}, s^L_{\mathsf{Z},1}\right), \tag{A3}$$

where

$$\gamma(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{c\,d\log_2(2)}\log_2\left(\frac{c+d}{c\,d(1-b)b}\frac{21^2}{a^2}\right)}$$

and $\tau_n = \Sigma_{k\in\{\mu,\nu,\omega\}} p_k e^{-k} k^n/n!$ is the probability that Alice prepares an n-photon state. The upper bound on the number of bit errors from single-photon events in X, $v^U_{\mathsf{X},1}$, is given by

$$v^U_{\mathsf{X},1} = \frac{\tau_1}{\nu-\omega}\left(\frac{e^\nu m^U_{\mathsf{X},\nu}}{p_\nu} - \frac{e^\omega m^L_{\mathsf{X},\omega}}{p_\omega}\right). \tag{A4}$$

The upper and lower bounds for the number of detected pulses and the number of bit errors, taking finite-key effects into account, are given by

$$n^U_{\mathsf{Z},\mathsf{k}} = n_{\mathsf{Z},\mathsf{k}} + \sqrt{\frac{n_\mathsf{Z}}{2}\ln\frac{21}{\varepsilon_{\text{sec}}}}, \tag{A5}$$

$$n^L_{\mathsf{Z},\mathsf{k}} = n_{\mathsf{Z},\mathsf{k}} - \sqrt{\frac{n_\mathsf{Z}}{2}\ln\frac{21}{\varepsilon_{\text{sec}}}}, \tag{A6}$$

$$m^U_{\mathsf{X},\mathsf{k}} = m_{\mathsf{X},\mathsf{k}} + \sqrt{\frac{m_\mathsf{X}}{2}\ln\frac{21}{\varepsilon_{\text{sec}}}}, \tag{A7}$$

$$m^L_{\mathsf{X},\mathsf{k}} = m_{\mathsf{X},\mathsf{k}} - \sqrt{\frac{m_\mathsf{X}}{2}\ln\frac{21}{\varepsilon_{\text{sec}}}}, \tag{A8}$$

where $n_\mathsf{Z} = \Sigma_{k\in\{\mu,\nu,\omega\}} n_{\mathsf{Z},k}$ and $m_\mathsf{X} = \Sigma_{k\in\{\mu,\nu,\omega\}} m_{\mathsf{X},k}$.

[1] C. Bennett and G. Brassard, Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984), 175 1984.

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

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[4] 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 Inf. **3**, 25 (2017).

[5] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, High-dimensional quantum cryptography with twisted light, New J. Phys. **17**, 033033 (2015).

[6] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons, Quantum **2**, 111 (2018).

[7] 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).

[8] K. Inoue, E. Waks, and Y. Yamamoto, Differential Phase Shift Quantum Key Distribution, Phys. Rev. Lett. **89**, 037902 (2002).

[9] V. Ansari, G. Harder, M. Allgaier, B. Brecht, and C. Silberhorn, Temporal-mode measurement tomography of a quantum pulse gate, Phys. Rev. A **96**, 063817 (2017).

[10] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, and Z.-P. Li, *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[11] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, and H. Li, *et al.*, Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels, Phys. Rev. Lett. **122**, 160501 (2019).

[12] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H Zbinden, Performance and security of 5 GHz repetition rate polarization-based quantum key distribution, Appl. Phys. Lett. **117**, 144003 (2020).

[13] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, and X. Jiang, High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics, Phys. Rev. X **10**, 031030 (2020).

[14] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Decoy-state quantum key distribution with polarized photons over 200 km, Opt. Exp. **18**, 8587 (2010).

[15] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[16] J. Jin, J.-P. Bourgoin, R. Tannous, S. Agne, C. J. Pugh, K. B. Kuntz, B. L. Higgins, and T. Jennewein, Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel, Opt. Exp. **27**, 37214 (2019).

[17] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature **509**, 475 (2014).

[18] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Overcoming Noise in Entanglement Distribution, Phys. Rev. X **9**, 041042 (2019).

[19] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin, Time-bin entangled qubits for quantum communication created by femtosecond pulses, Phys. Rev. A **66**, 062308 (2002).

[20] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, Security of high-dimensional quantum

key distribution protocols using Franson interferometers, J. Phys. B **46**, 104010 (2013).

[21] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, R. J. Warburton, H. Zbinden, and F. Bussières, High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors, Appl. Phys. Lett. **112**, 061103 (2018).

[22] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, A. D. Beyer, R. M. Briggs, B. Bumble, and M. Colangelo, *et al.*, Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector, Nat. Photonics **14**, 250 (2020).

[23] 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, Sci. Adv. **3**, e1701491 (2017).

[24] N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, and D. J. Gauthier, Robust and Stable Delay Interferometers with Application to *d*-Dimensional Time-Frequency Quantum Key Distribution, Phys. Rev. Appl. **7**, 044010 (2017).

[25] J.-P. W. MacLean, J. M. Donohue, and K. J. Resch, Direct Characterization of Ultrafast Energy-Time Entangled Photon Pairs, Phys. Rev. Lett. **120**, 053601 (2018).

[26] D. G. England, K. A. Fisher, J.-P. W. MacLean, P. J. Bustard, R. Lausten, K. J. Resch, and B. J. Sussman, Storage and Retrieval of THz-Bandwidth Single Photons Using a Room-Temperature Diamond Quantum Memory, Phys. Rev. Lett. **114**, 053602 (2015).

[27] C. Kupchak, P. J. Bustard, K. Heshami, J. Erskine, M. Spanner, D. G. England, and B. J. Sussman, Time-bin-to-polarization conversion of ultrafast photonic qubits, Phys. Rev. A **96**, 053812 (2017).

[28] C. Kupchak, J. Erskine, D. England, and B. Sussman, Terahertz-bandwidth switching of heralded single photons, Opt. Lett. **44**, 1427 (2019).

[29] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[30] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[31] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[32] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[33] M. Tomamichel, C. C.-W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

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

[35] H.-K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptol. **18**, 133 (2005).

[36] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Fast and simple one-way quantum key distribution, Appl. Phys. Lett. **87**, 194108 (2005).

[37] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett. **81**, 3018 (1998).

[38] F. Bouchard, D. England, P. J. Bustard, K. L. Fenwick, E. Karimi, K. Heshami, and B. Sussman, Achieving Ultimate Noise Tolerance in Quantum Communication, Phys. Rev. Appl. **15**, 024027 (2021).

[39] M. G. Raymer and K. Banaszek, Time-frequency optical filtering: Efficiency vs. temporal-mode discrimination in incoherent and coherent implementations, Opt. Exp. **28**, 32819 (2020).

[40] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, and A. Murakami, *et al.*, 10-Mb/s quantum key distribution, J. Lightwave Technol. **36**, 3427 (2018).