

Scalable implementation of $(d + 1)$ mutually unbiased bases for d -dimensional quantum key distribution

Takuya Ikuta^{1,2,*}, Seiseki Akibue^{3,†}, Yuya Yonezu¹, Toshimori Honjo¹, Hiroki Takesue¹, and Kyo Inoue²

¹NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan

²Graduate School of Engineering, Osaka University, 2-1 Yamadaoka, Suita, Osaka 565-0871, Japan

³NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan



(Received 6 April 2022; accepted 14 September 2022; published 12 October 2022)

A high-dimensional quantum key distribution (QKD) can improve error rate tolerance and the secret key rate. Many d -dimensional QKDs have used two mutually unbiased bases (MUBs), while $(d + 1)$ MUBs enable a more robust QKD, especially against correlated errors. However, a scalable implementation has not been achieved because the setups have required d devices even for two MUBs or a flexible convertor for a specific optical mode. Here, we propose a scalable and general implementation of $(d + 1)$ MUBs using $\log_p d$ interferometers in prime power dimensions $d = p^N$. We implemented the setup for time-bin states and observed an average error rate of 3.8% for phase bases, which is lower than the 23.17% required for a secure QKD against coherent attack in $d = 4$.

DOI: [10.1103/PhysRevResearch.4.L042007](https://doi.org/10.1103/PhysRevResearch.4.L042007)

Quantum key distribution (QKD) is a technique to share a secret key, whose security is guaranteed by quantum mechanics. Ever since the first proposal, called the BB84 protocol [1], many different types of protocols have been proposed and demonstrated [2–13]. One of the key ingredients for QKD is mutually unbiased bases (MUBs) [14–16]. If two d -dimensional states $\forall |\psi\rangle \in \mathcal{B}_0, \forall |\phi\rangle \in \mathcal{B}_1$ for orthonormal bases $\mathcal{B}_0, \mathcal{B}_1$ satisfy $|\langle\psi|\phi\rangle|^2 = 1/d$, the two bases are mutually unbiased. Typical examples of MUBs are sets of eigenstates of the Pauli operators, σ_x, σ_y , and σ_z . Generally, at most $(d + 1)$ bases can be mutually unbiased [14], where any pair of bases satisfies the above condition. The BB84 protocol employs two two-dimensional MUBs (e.g., X and Z bases), while the six-state protocol employs three two-dimensional MUBs (X, Y , and Z bases) [3]. In the case of standard one-way error correction, the error rate threshold to distill a secure key is 11.0% for the BB84 protocol, while the six-state protocol enhances the threshold to 12.6% for a depolarizing channel. In particular, the six-state protocol has a larger error tolerance when bit- and phase-flip errors are correlated [17]; thus, using a larger set of MUBs improves the robustness and secret key rate of QKD.

High-dimensional quantum states open another way to improve the secret key rate [18–21], where the information amount per photon increases with dimensions. A two-basis protocol, which is a d -dimensional extension of the BB84

protocol, uses two MUBs in d dimensions to ensure security. Similar to the two-dimensional QKDs, the secret key rate of a high-dimensional QKD can be further improved by using $(d + 1)$ -MUBs, especially against correlated noises (see the Supplemental Material [22] for an example of correlated noises).

The two-basis protocol has been performed using several optical modes [23–32]. Among these optical modes, a time-bin state is a promising candidate for QKD because of its high robustness against disturbances during fiber transmission [33,34]. Unfortunately, increasing dimensions for time-bin states consumes many time slots, and the improvement of the key rate per unit time is limited if we can use ideal devices. However, dead time due to practical single-photon detectors and slow electrical devices limits the detection count rates in a short distance. In such a situation, the large amount of information per photon in a high-dimensional time-bin state makes it possible to directly improve the secret key rate because we can use many short pulses within the dead time thanks to fast optical devices [27]. On the other hand, a robust $(d + 1)$ -basis protocol has also been implemented using orbital angular momentum (OAM) thanks to the flexibility of spatial light modulators (SLMs) [35].

Although the advantages of high-dimensional QKD have been demonstrated, important problems still remain in scaling up the dimensions. One problem is the number of devices required for the measurement. For example, the Fourier basis $\mathcal{F}$ used in [27] is given by

$$\mathcal{F} = \left\{ |f_n\rangle = \frac{1}{\sqrt{d}} \sum_m e^{\frac{2\pi i m n}{d}} |m\rangle \mid n \in \{0, \dots, d-1\} \right\}, \quad (1)$$

where $\{|m\rangle \mid m \in \{0, \dots, d-1\}\}$ is the Z basis selected as the time-bin basis representing a photon in a specific time slot. To

*takuya.ikuta.xu@hco.ntt.co.jp

†seiseki.akibue.rb@hco.ntt.co.jp

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

measure a time-bin state in $\mathcal{F}$, $(d-1)$ delay Mach-Zehnder interferometers (MZIs) and d single-photon detectors are required; thus, the number of devices increases linearly with dimensions [26,27]. Another problem is a requirement for precise control and calibration of devices because the phase in Eq. (1) is $\propto 1/d$. Some approaches mitigated these problems by using other bases for specific dimensions [30] or using fewer states instead of all the states in a basis [36,37]. However, a generally scalable method has not been established to the best of our knowledge. Furthermore, a generalization to $(d+1)$ MUBs is more challenging, especially for time-bin states because they cannot be modulated flexibly as in the case of OAM using an SLM in the current technology, although, in principle, a universal unitary gate can be implemented by optical switches and many 2×2 beam splitters [of the order of $O(d^2)$] [38]. In addition, previous analyses of the $(d+1)$ -basis protocol were limited to prime dimensions [19–21], which largely restricts the dimensions available for the $(d+1)$ -basis protocol.

Here, we propose an implementation of $(d+1)$ MUBs for prime power dimensions $d = p^N$, where the number of interferometers scales logarithmically with d and the phase resolution is constant regardless of N . The proposed method can also be applied to general optical modes. In addition, the required number of detectors is constant regardless of N in the case of time-bin states. We also show that the MUBs we use can ensure security against coherent attack in prime power dimensions.

To implement a compact setup, we use MUBs constructed by the Galois field [14–16]. Because the equation representing MUBs depends on whether p is 2 or odd prime number, we first explain the case of $d = 2^N$, and the case of odd prime numbers is explained later. Let $GF[2^N]$ be the Galois field of order 2^N , where the addition is elementwise exclusive OR in a bit representation of $e \in GF[2^N]$. We also define a binary symmetric matrix $\mathbf{A}^{(k)}$ whose element satisfies $2^i \odot 2^j = \bigoplus_{k=0}^{N-1} A_{ij}^{(k)} 2^k$, where $\oplus$ and $\odot$ denote the addition and multiplication in $GF[2^N]$, respectively. We select the Z basis as one basis in $(d+1)$ MUBs. Then, all states in other d MUBs (phase bases) are represented by $|\psi_n^{(r)}\rangle = \sum_m B_{mn}^{(r)} |m\rangle$, where $r, n \in GF[2^N]$ are the labels of the phase basis and state, respectively. If we define the probability amplitude by the following equation, the Z and phase bases form $(d+1)$ MUBs [14].

$$B_{mn}^{(r)} = \frac{1}{\sqrt{2^N}} \exp \left[\frac{\pi}{2} i \left(\sum_{j=0}^{N-1} r_j \mathbf{m}^T \mathbf{A}^{(j)} \mathbf{n} + 2 \mathbf{m} \cdot \mathbf{n} \right) \right]. \quad (2)$$

Here, $\mathbf{m}$ and $\mathbf{n}$ are binary vectors representing m and n , respectively, and r_j is the j th element of r in bit representation. In contrast to the phase resolution of $1/2^N$ in Eq. (1), it is clear that the phase in Eq. (2) takes only four values $\{0, \pi/2, \pi, 3\pi/2\}$ because $r_j, \mathbf{m}, \mathbf{n}$, and $\mathbf{A}^{(j)}$ are a binary value, vector, and matrix. Therefore, these states can be easily generated for any large N . For example, if we use the time-bin basis as the Z basis, the phase basis state can be generated by quadrature phase shift keying (QPSK) modulation of d sequential pulses.

For a compact measurement of phase bases, we use a decomposition of the matrix $\mathbf{B}^{(r)}$ whose element is $B_{mn}^{(r)}$. $\mathbf{B}^{(r)}$ can

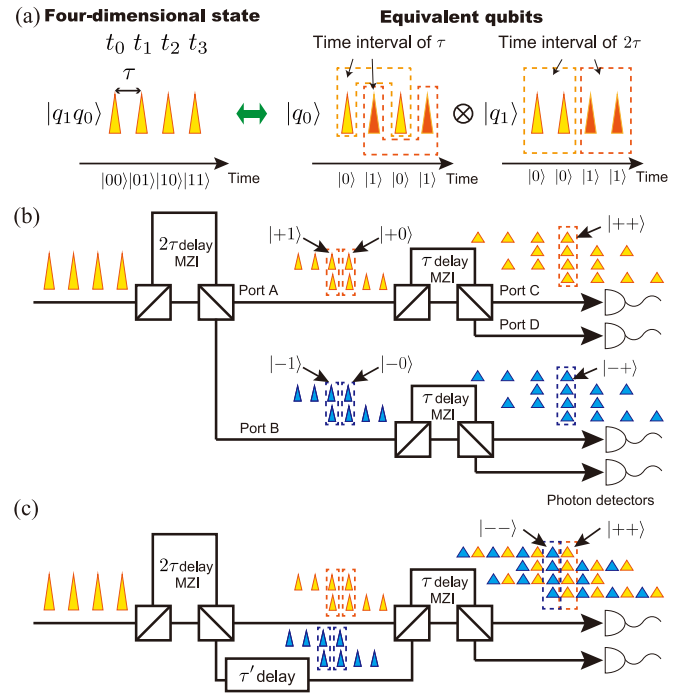


FIG. 1. (a) Two blockwise qubits equivalent to a four-dimensional time-bin state. Measurement setup for the Hadamard basis using cascaded MZIs with (b) a tree structure and (c) time division multiplexing.

be decomposed as $\mathbf{D}^{(r)} \mathbf{B}^{(0)}$, where $\mathbf{D}^{(r)}$ is a diagonal unitary and the m th element of $\mathbf{D}^{(r)}$ is given by

$$D_{mm}^{(r)} = \exp \left[\frac{\pi}{2} i \left(\sum_{j=0}^{N-1} r_j \mathbf{m}^T \mathbf{A}^{(j)} \mathbf{m} \right) \right]. \quad (3)$$

This decomposition implies that the measurement of the r th phase basis can be implemented by two sequential procedures: the first procedure is a basis selection corresponding to $\mathbf{D}^{(r)}$, and the second procedure is a projective measurement onto $\{|\psi_n^{(0)}\rangle\}$ corresponding to $\mathbf{B}^{(0)}$. Since $\mathbf{D}^{(r)}$ is a diagonal unitary, the basis change is a phase modulation on Z basis states. If Z basis states are time-bin states, $\mathbf{D}^{(r)}$ can be implemented by an optical phase modulator. Regarding the projective measurement, we can confirm that $\{|\psi_n^{(0)}\rangle\}$ are the Hadamard basis states because $B_{mn}^{(0)} = \frac{1}{\sqrt{2^N}} \exp(\pi i \mathbf{m} \cdot \mathbf{n})$ is the Hadamard transform matrix. Therefore, $\{|\psi_n^{(0)}\rangle\}$ can be readily represented in N -qubit space equivalent to the d -dimensional Hilbert space.

For a more concrete explanation, let us consider two qubits equivalent to a four-dimensional time-bin state [Fig. 1(a)]. We assign two-qubit states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ to a photon existing in time slots t_m in ascending order. Here, these two qubits span the four-dimensional Hilbert space. When we look at each qubit, each qubit is a conventional time-bin qubit, except that $|0\rangle$ and $|1\rangle$ correspond to blocks of several time slots. For example, $|0\rangle$ and $|1\rangle$ for the first qubit q_0 correspond to $\{t_0, t_2\}$ and $\{t_1, t_3\}$, respectively, and the time interval between the blocks is τ . Similarly, the second qubit q_1 is a time-bin qubit with a different time interval, 2τ . The Hadamard transform

converts $|0\rangle$ and $|1\rangle$ to $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ for each qubit. Therefore, $|\psi_n^{(0)}\rangle$ are the tensor products of $|\pm\rangle$ for these qubits. Because a projection onto $|\pm\rangle$ can be performed by a delay MZI having the same delay time as the interval of a time-bin qubit [39], the projective measurement onto $\{|\psi_n^{(0)}\rangle\}$ can be implemented by cascading several MZIs.

Figure 1(b) shows the measurement setup for $\{|\psi_n^{(0)}\rangle\}$ by cascaded MZIs using a tree structure. First, a four-dimensional time-bin state is launched into an MZI with a delay time of 2τ . By setting the relative phase between the two arms at 0, the interferences at port A correspond to projections onto $|+0\rangle$ and $|+1\rangle$, while those at port B correspond to projections onto $|-0\rangle$ and $|-1\rangle$. Then, these states are launched into another MZI with a delay time of τ . As a result, the projections onto $|++\rangle$ and $|+-\rangle$ are performed at ports C and D, respectively. Similarly, the projections onto $|-+\rangle$ and $|--\rangle$ are performed at the other MZI with a delay time of τ . By expanding the tree structure, we can implement projective measurements onto the tensor product states of $|\pm\rangle$ for any 2^N dimensions. However, this implementation is not scalable because it requires $(d - 1)$ MZIs, the same as the implementation of the Fourier basis measurement does [26,27]. An important difference between these implementations is that the Hadamard basis measurement is implemented simply with the relative phase of 0, while the Fourier basis measurement requires several different phases. Because the same MZIs are used several times for the Hadamard basis measurement, we can reduce the number of MZIs significantly [Fig. 1(c)]. In this setup, each output of the first MZI is connected to each input of the second MZI after the input timings are adjusted by an optical delay line. Here, the delay time τ' is chosen so that the two inputs for the second MZI do not make interferences. By concatenating this time-division multiplexing, all projections onto $\{|\psi_n^{(0)}\rangle\}$ for general 2^N -dimensional states can be implemented using $\log_2 d$ MZIs and two single-photon detectors. Combined with the basis selection of $\mathbf{D}^{(r)}$, d phase basis measurements can be implemented by a significantly compact setup using a phase modulator and cascaded MZIs. The remaining measurement on the time-bin basis can be performed by simply launching the photon into a single-photon detector, and the Z and phase basis measurements can be simultaneously implemented by a beam splitter.

Note that the method using cascaded interferometers is also available for other optical modes. The general structure is as follows. $\mathbf{D}^{(r)}$ is implemented by a mode-dependent phase modulator. The projective measurement onto $\{|\psi_n^{(0)}\rangle\}$ is implemented by cascading $\log_2 d$ MZIs having different mode shifts connected via delay lines or optical lines with mode shifts (see the Supplemental Material [22]).

In the proposed method, the discarded time slots at the outputs of the MZIs reduce the detection efficiency, whose equivalent optical loss is $N \times 3$ dB. It is known that, ideally, this inefficiency of the Hadamard transform can be removed by replacing the input beam splitters in MZIs with active optical switches [38,40]. For example, if we replace the first beam splitter of the 2τ -delay MZI in Fig. 1(c), the optical switch can transfer the pulses corresponding to $|0\rangle$ and $|1\rangle$ for the equivalent qubit q_1 to the long and short arms, respectively.

As a result, the outputs from the 2τ -delay MZI contain the optical pulses only for the time slots surrounded by dotted lines in Fig. 1(c). The same operation can be implemented for the τ -delay MZI and the equivalent qubit q_0 . By iterating the same operation for all equivalent qubits, we can avoid the inefficiency of the Hadamard transform for the passive implementation. Although active devices usually introduce additional insertion losses, such a modification is beneficial if the insertion loss per switch is less than 3 dB.

We implemented the proposed setup for four-dimensional time-bin states (see the Supplemental Material [22] for more details, including calibration). A continuous-wave light, whose wavelength was 1559.0 nm, was modulated into a single pulse or four sequential pulses by an optical in-phase and quadrature phase (IQ) modulator (Fig. 2). A single pulse corresponded to the time-bin basis state, while a set of four-sequential pulses corresponded to the phase basis state represented by Eq. (2). The pulse width, time interval, and repetition frequency of the state preparation were 33 ps, 500 ps, and 250 MHz, respectively. The optical power was attenuated by variable optical attenuators and optical couplers so that the average photon number became 1 M photons per second.

The prepared states were measured by two measurement setups. The first setup was used to measure the photons in the phase bases. The weak optical pulses were launched into a LiNbO₃ phase modulator (PM), by which we implemented the phase basis selection $\mathbf{D}^{(r)}$. The modulated pulses were then launched into a stable MZI fabricated by using a planar light-wave circuit (PLC) technology [41,42]. The delay time was 1 ns and the relative phase between the two arms was adjusted to be 0. The outputs from this MZI were launched into another MZI after a relative delay of ≈ 250 ps was introduced by two optical delay lines (DLs). The delay time of the second MZI was 500 ps, and the relative phase was also adjusted to be 0. The outputs from these cascaded MZIs were detected by using two superconducting nanowire single-photon detectors (SNSPDs). The detection efficiencies were set at 56%, and the dark counts were < 100 cps. The single count rates for SNSPD1 and 2 were 52 and 47 kcps, respectively; thus, the dark counts were negligible. These counts were recorded by a time-interval analyzer. The second setup was used to perform the time-bin basis measurement, where the photons were directly detected by SNSPD1 after removing the PM and MZIs. The single count rate was 546 kcps. Due to the timing jitter of the detectors and electrical system, we observed the full-width at half-maximum temporal width of 78 ps for the histogram of the arrival time records. As we described above, this measurement can be simultaneously performed by using a beam splitter when we implement an actual QKD protocol.

Figure 3(a) shows a conditional probability distribution of photon detection $\Pr(n_b|r_a, n_a, r_b)$, where a photon was detected as the n_b th state when it had been prepared as the n_a th state in the r_a th basis and measured by the r_b th basis. Here, $r_a(r_b) = 0$ corresponds to the time-bin basis and $r_a(r_b) = r + 1$ corresponds to the r th phase basis. When the measurement basis was the same as the prepared basis, the distribution was close to the identity matrix because each basis is an orthonormal basis. On the other hand, the distribution was close to the uniform distribution when the state preparation

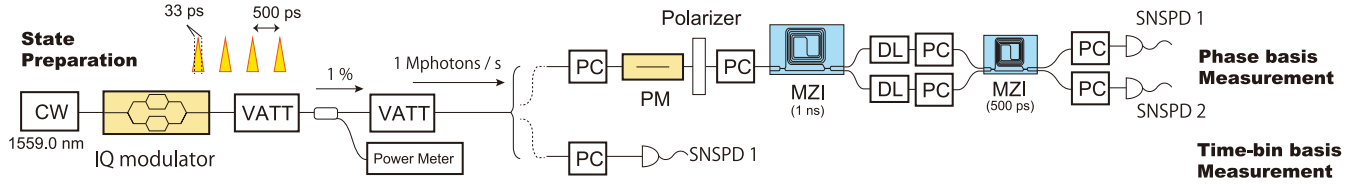


FIG. 2. Experimental setup for the four-dimensional MUBs using a time-bin state. The dotted lines in the middle were manually selected. CW: continuous-wave light; IQ modulator: LiNbO₃ in-phase and quadrature phase modulator; VATT: optical variable attenuator; PC: polarization controller; PM: LiNbO₃ phase modulator; MZI: Mach-Zehnder interferometer fabricated by planar light-wave circuit technology; DL: optical delay line; SNSPD: superconducting nanowire single-photon detector.

and measurement were performed by different bases, which formed MUBs. Therefore, we clearly observed the probability distribution expected from the five four-dimensional MUBs using the compact experimental setup.

Important parameters for QKD are error rates [Fig. 3(b)], which were estimated from the diagonal blocks of the conditional probability distribution. In the time-bin basis ($r_b = 0$), the average error was the lowest thanks to the SNSPD, which had a low timing jitter and dark count. In the Hadamard basis ($r_b = 1$), the error rate increased slightly, but it was clearly smaller than the error rates in the other phase bases. The amplitude imbalance of the generated states and limited extinction ratio of the MZIs can be considered as error sources for the Hadamard basis measurement. Therefore, the error could be mitigated by controlling the IQ modulation signal more precisely and compensating for the relative transmittance between the short and long arms in the MZIs (see the Supplemental Material [22] and Refs. [43,44]). The difference in the error rates between the Hadamard basis and the other phase bases can be considered as the difference in operational conditions for the IQ modulator and PM. As the Hadamard basis state is composed of $|\pm\rangle$ for the equivalent qubits, the state has only real amplitudes and thus the IQ modulator operated as a simple amplitude modulator. In addition, the Hadamard basis state can be measured without driving the PM. On the other hand, the other phase bases have both real and imaginary amplitudes and require the basis selection by the PM. Thus, inaccurate bias voltages for the IQ modulator and distorted modulation signal for the PM would impose additional errors for these phase bases. Therefore, we can expect that the error rates for these phase bases can be mitigated so that they are

close to the error rate for the Hadamard basis with more precise controls of these parameters.

Unfortunately, previous security analyses were limited to prime dimensions [19–21]. However, we can follow a similar analysis by using Weyl operators generalized by the Galois field (see the Supplemental Material [22]). Although the observed error rates depended on the basis, all error rates were clearly smaller than the threshold value of 23.17%, below which we can generate secure keys in an asymptotic limit. In addition, the error rates were also comparable to or lower than the $\approx 4\%$ error rates using the Fourier basis [27]. Important future work includes more thorough investigations, e.g., a decoy-state method, finite key analysis, and various noise models, to evaluate the secure key rate in a practical situation. Note that the efficiency due to the basis mismatch is not as small as $1/(d+1)$ in an asymmetric basis selection, where the time-bin basis is selected to generate a raw key with a high probability, while other d phase bases are used to upper bound the amount of eavesdropped information. The inefficiency due to the basis mismatch is negligible in an asymptotic limit, although a finite key analysis should be included for an actual implementation. In addition, the $(d+1)$ -basis protocol shows a strong robustness against correlated noise (see the Supplemental Material [22]), and what kind of physical noise shows such a correlation is an interesting open question. Although a practical implementation requires these investigations, the present results indicate the feasibility of fast and robust secret key generation enabled by the $(d+1)$ -basis protocol using the proposed setup.

Finally, we explain the extension of the method to the case of the power of odd prime numbers. When $d = p^N$ for odd prime number p , $(d+1)$ MUBs can be constructed by the following equation instead of Eq. (2) [14]:

$$B_{mn}^{(r)} = \frac{1}{\sqrt{p^N}} \exp \left[\frac{2\pi i}{p} \left(\sum_{j=0}^{N-1} r_j \mathbf{m}^T \mathbf{A}^{(j)} \mathbf{n} + \mathbf{m} \cdot \mathbf{n} \right) \right]. \quad (4)$$

Here, each element of $\mathbf{r}$, $\mathbf{m}$, $\mathbf{n}$, and $\mathbf{A}^{(j)}$ takes a value in $[0, \dots, p-1]$, and $\mathbf{A}^{(j)}$ is similarly constructed by using $GF[p^N]$. In this case, the phase takes only p values, which is a large reduction from p^N values in the Fourier basis in Eq. (1). Interestingly, the minimum number of phases is obtained for $d = 3^N$ because Eq. (2) requires four phases. This matrix can also be decomposed as $\mathbf{D}^{(r)} \mathbf{B}^{(0)}$, and the diagonal unitary $\mathbf{D}^{(r)}$ can be similarly implemented by a phase modulator. On the other hand, $\mathbf{B}^{(0)}$ is not the Hadamard transform matrix but a tensor product of the p -dimensional Fourier transform matrices. Namely, we need to project the state onto the ten-

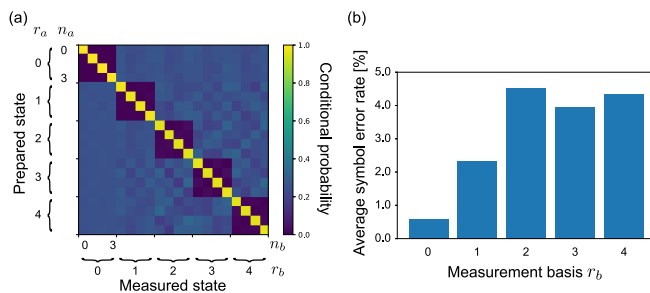


FIG. 3. Experimental results. (a) Conditional probability of photon detection, $\Pr(n_b | r_a, n_a, r_b)$. (b) Average symbol error rate for each basis estimated by $1 - \frac{1}{4} \sum_{n_a=n_b} \Pr(n_b | r_a, n_a, r_b)$, where $r_a = r_b$.

sor product of the p -dimensional Fourier basis states for the equivalent p -dimensional qudits. Note that the tensor product states of the p -dimensional Fourier basis states are different from p^N -dimensional Fourier basis states for $N \geq 2$. For a three-dimensional time-energy entanglement, the Fourier basis measurement has been demonstrated by using a three-arm interferometer [45], which is a natural extension of $|\pm\rangle$ measurements by an MZI. Generally, the p -dimensional Fourier basis measurement can be implemented by a p -arm interferometer. Therefore, the desired measurement corresponding to $\mathbf{B}^{(0)}$ can be implemented by cascading p -arm interferometers with different delays N times via additional delay lines.

In conclusion, we proposed a compact implementation of $(d + 1)$ MUBs for prime power dimensions using $\log_p d$ interferometers. The proposed method was demonstrated using

a four-dimensional time-bin state, where we observed the low average error rate of 3.8% for the phase bases. All error rates were below the threshold to distill a secure key against coherent attack, and comparable to or lower than those in a previous implementation using the Fourier basis, although the number of bases increased. Our method can also be applied for other optical modes and constitutes an important step toward a practical implementation of fast, secure, and robust communications realized with a high-dimensional quantum state.

We thank K. Igarashi, K. Tamaki, and G. Kato for fruitful discussions and H. Tamura for administrative support in this research.

T.I. and S.A. contributed equally to this work.

-
- [1] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* (IEEE, Bangalore, India, 1984), pp. 175–179.
 - [2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, *Phys. Rev. Lett.* **81**, 3018 (1998).
 - [4] D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson, and P. G. Kwiat, Entangled-photon six-state quantum cryptography, *New J. Phys.* **4**, 45 (2002).
 - [5] K. Inoue, E. Waks, and Y. Yamamoto, Differential Phase Shift Quantum Key Distribution, *Phys. Rev. Lett.* **89**, 037902 (2002).
 - [6] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, *Nat. Photon.* **1**, 343 (2007).
 - [7] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, *Phys. Rev. Lett.* **98**, 010504 (2007).
 - [8] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
 - [9] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, *Nature (London)* **509**, 475 (2014).
 - [10] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, *Nat. Photon.* **9**, 827 (2015).
 - [11] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, *Phys. Rev. Lett.* **117**, 190501 (2016).
 - [12] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou *et al.*, Satellite-to-ground quantum key distribution, *Nature (London)* **549**, 43 (2017).
 - [13] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, 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).
 - [14] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Phys.* **191**, 363 (1989).
 - [15] T. Durt, About mutually unbiased bases in even and odd prime power dimensions, *J. Phys. A: Math. Gen.* **38**, 5267 (2005).
 - [16] T. Durt, B.-G. Englert, I. Bengtsson, and K.  yczkowski, On mutually unbiased bases, *Intl. J. Quantum Inf.* **08**, 535 (2010).
 - [17] M. Koashi, Simple security proof of quantum key distribution based on complementarity, *New J. Phys.* **11**, 045018 (2009).
 - [18] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d -Level Systems, *Phys. Rev. Lett.* **88**, 127902 (2002).
 - [19] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, *Phys. Rev. A* **82**, 030301(R) (2010).
 - [20] A. Ferenczi and N. L utkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, *Phys. Rev. A* **85**, 052310 (2012).
 - [21] R. Wang, Z.-Q. Yin, H. Liu, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Tight finite-key analysis for generalized high-dimensional quantum key distribution, *Phys. Rev. Res.* **3**, 023019 (2021).
 - [22] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevResearch.4.L042007> for (1) measurement setup for general optical modes; (2) details of the experimental setup including calibration; (3) security analysis against coherent attack and an example of strongly correlated noise model.
 - [23] S. Etcheverry, G. Ca as, E. S. G omez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Quantum key distribution session with 16-dimensional photonic states, *Sci. Rep.* **3**, 2316 (2013).
 - [24] M. Mirhosseini, O. S. Maga a-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, High-dimensional quantum cryptography with twisted light, *New J. Phys.* **17**, 033033 (2015).

- [25] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, High-dimensional intracity quantum cryptography with structured photons, *Optica* **4**, 1006 (2017).
- [26] N. T. Islam, C. Cahall, A. Aragonese, 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).
- [27] 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).
- [28] 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).
- [29] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysieszna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers, *Phys. Rev. A* **96**, 022317 (2017).
- [30] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution, *Phys. Rev. Appl.* **14**, 014051 (2020).
- [31] X.-M. Hu, C. Zhang, Y. Guo, F.-X. Wang, W.-B. Xing, C.-X. Huang, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, X. Gao, M. Pivoluska, and M. Huber, Pathways for Entanglement-Based Quantum Communication in the Face of High Noise, *Phys. Rev. Lett.* **127**, 110505 (2021).
- [32] Q.-K. Wang, F.-X. Wang, J. Liu, W. Chen, Z.-F. Han, A. Forbes, and J. Wang, High-Dimensional Quantum Cryptography with Hybrid Orbital-Angular-Momentum States through 25 km of Ring-Core Fiber: A Proof-of-Concept Demonstration, *Phys. Rev. Appl.* **15**, 064034 (2021).
- [33] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, Entanglement distribution over 300 km of fiber, *Opt. Express* **21**, 23241 (2013).
- [34] T. Ikuta and H. Takesue, Four-dimensional entanglement distribution over 100 km, *Sci. Rep.* **8**, 817 (2018).
- [35] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, *Phys. Rev. A* **88**, 032305 (2013).
- [36] N. T. Islam, Charles Ci Wen Lim, C. Cahall, J. Kim, and D. J. Gauthier, Securing quantum key distribution systems using fewer states, *Phys. Rev. A* **97**, 042347 (2018).
- [37] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, Scalable high-rate, high-dimensional time-bin encoding quantum key distribution, *Quantum Sci. Technol.* **4**, 035008 (2019).
- [38] F. Bussières, Y. Soudagar, G. Berlin, S. Lacroix, and N. Godbout, Deterministic unitary operations on time-bin qudits for quantum communication, [arXiv:quant-ph/0608183](https://arxiv.org/abs/quant-ph/0608183).
- [39] H. Takesue and Y. Noguchi, Implementation of quantum state tomography for time-bin entangled photon pairs, *Opt. Express* **17**, 10976 (2009).
- [40] T. M. Rambo, Low-loss, all-optical, quantum switching for interferometric processing of weak signals, Ph.D. thesis, Northwestern University, 2016.
- [41] T. Honjo, K. Inoue, and H. Takahashi, Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer, *Opt. Lett.* **29**, 2797 (2004).
- [42] H. Takesue and K. Inoue, Generation of 1.5- μ m band time-bin entanglement using spontaneous fiber four-wave mixing and planar light-wave circuit interferometers, *Phys. Rev. A* **72**, 041804(R) (2005).
- [43] H.-P. Lo, T. Ikuta, N. Matsuda, T. Honjo, and H. Takesue, Entanglement generation using a controlled-phase gate for time-bin qubits, *Appl. Phys. Express* **11**, 092801 (2018).
- [44] H.-P. Lo, T. Ikuta, N. Matsuda, T. Honjo, W. J. Munro, and H. Takesue, Quantum Process Tomography of a Controlled-Phase Gate for Time-Bin Qubits, *Phys. Rev. Appl.* **13**, 034013 (2020).
- [45] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin, Bell-Type Test of Energy-Time Entangled Qutrits, *Phys. Rev. Lett.* **93**, 010503 (2004).