Reconfigurable generation and measurement of mutually unbiased bases for time-bin qudits

Joseph M. Lukens, Nurul T. Islam, Charles Ci Wen Lim, and Daniel J. Gauthier

Citation: Appl. Phys. Lett. **112**, 111102 (2018); doi: 10.1063/1.5024318
View online: https://doi.org/10.1063/1.5024318
View Table of Contents: http://aip.scitation.org/toc/apl/112/11
Published by the American Institute of Physics

Reconfigurable generation and measurement of mutually unbiased bases for time-bin qudits

Joseph M. Lukens,[1,a)] Nurul T. Islam,[2] Charles Ci Wen Lim,[3] and Daniel J. Gauthier[4]
[1]*Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA*
[2]*Department of Physics and Fitzpatrick Institute for Photonics, Duke University, Durham, North Carolina 27708, USA*
[3]*Department of Electrical and Computer Engineering and Centre for Quantum Technologies, National University of Singapore, Singapore 117583, Singapore*
[4]*Department of Physics, The Ohio State University, Columbus, Ohio 43210, USA*

(Received 31 January 2018; accepted 2 March 2018; published online 14 March 2018)

We propose a method for implementing mutually unbiased generation and measurement of time-bin qudits using a cascade of electro-optic phase modulator–coded fiber Bragg grating pairs. Our approach requires only a single spatial mode and can switch rapidly between basis choices. We obtain explicit solutions for dimensions $d = 2$, 3, and 4 that realize all $d + 1$ possible mutually unbiased bases and analyze the performance of our approach in quantum key distribution. Given its practicality and compatibility with current technology, our approach provides a promising springboard for scalable processing of high-dimensional time-bin states. *Published by AIP Publishing.*
https://doi.org/10.1063/1.5024318

Mutually unbiased bases (MUBs) are of fundamental importance in quantum mechanics. A collection of bases is called mutually unbiased if any eigenstate from one basis overlaps equally with all states from the other bases. Since a measurement result in one basis provides no predictive information about the outcome of a subsequent measurement in one of its mutually unbiased partners,[1,2] MUBs represent optimal choices for quantum state tomography in noisy environments[1,3] and guarantee security against eavesdropping in quantum key distribution (QKD).[4,5] Implementing MUBs experimentally can be challenging, especially in high-dimensional Hilbert spaces (dimension $d > 2$). For example, in time-bin encoding, the best known method for measuring states mutually unbiased with respect to single-time-bin wavepackets is to use nested delay interferometers (DIs).[6–8] This approach requires the use of d detectors and is difficult to scale to high d in a practical setting. Furthermore, passive DIs produce satellite pulses that reduce the probability of successful measurements to $1/d$.[9,10]

Therefore, a critical objective is to develop an approach for synthesizing time-bin MUBs, which preserves single-spatial-mode quantum information processing, is rapidly reconfigurable, and enables measurements with high success probability. Here, we propose and analyze a configuration for generating and measuring quantum photonic states prepared in various time-bin MUBs using a cascade of electro-optic phase modulator (EOM)–coded fiber Bragg grating (FBG) pairs (see Fig. 1). We find explicit solutions of $(d + 1)$-element MUB families for $d = 2$, 3, and 4 and simulate performance of a multibasis QKD system. Importantly, our approach can be implemented using current technology and offers the first truly single-mode paradigm for time-bin MUBs.

In our design, we impose the requirement that a physical configuration must transform between all MUBs available in a d-dimensional space. This criterion is motivated by high-dimensional QKD, as both increasing the dimension d and employing $(d + 1)$-basis protocols enhance robustness against noise.[11,12] Moreover, we seek solutions that can efficiently detect each eigenstate in a MUB simultaneously, as opposed to projective measurements that only result in a binary outcome.[13,14] The key technology we explore for generating and measuring discrete time-bin states in multiple MUBs is the coded FBG, which has played an important role in the development of classical optical code division multiple access networks.[15] Such an FBG typically consists of a series of relatively low-reflectivity segments, each with a specified amplitude and phase shift. The (assumed fixed) length of each segment, or "chip," sets the time-bin duration so that the total reflected field for a single quantum wavepacket consists of a series of wavepackets with weight coefficients given by the chip sequence. By extension, if instead a train of wavepackets is input to the FBG, the FBG will cause interference between different time bins. Codes as long as 1023 chips have been implemented experimentally,[16] thus making FBGs an appealing choice for time-bin interference of quantum states in optical fiber.

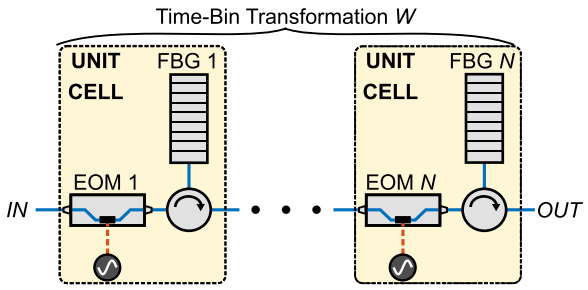

FIG. 1. Proposed system. The input state propagates through a series of N unit cells, each comprising an EOM and coded FBG. Ideally, the input-to-output path produces a one-to-one mapping between states from different bases.

a)Electronic mail: lukensjm@ornl.gov

Unfortunately, coded gratings alone are insufficient for arbitrary mode transformations because they are linear, time-invariant filters, making it impossible to map unique interference patterns to each output bin. For example, a single FBG (or cascade thereof) can, in principle, produce one of the d output transformations realized by $d-1$ nested DIs,[17] but it cannot replace all of them. This problem can be overcome by cascading the coded FBG with an additional time-dependent optical primitive: an electro-optic phase modulator (EOM), which enables user-defined phase shifts to any sequence of time bins.[18] When integrated as a sequence of alternating FBGs and EOMs (Fig. 1), it is possible to realize arbitrary temporal transformations where the number of components scales linearly with the dimensionality d—a conclusion reached by extending, via Fourier duality, recent results on frequency-bin quantum information processing.[19] Nonetheless, it remains to be shown that a particular EOM/FBG sequence can switch between *multiple* MUBs rapidly, a requirement which goes beyond the sufficiency of FBGs and EOMs to produce a *given* transformation, and requires a different design procedure.

To formulate this problem, we assume a Hilbert space spanned by the single-photon states $|k\rangle = \hat{a}_k^\dagger|\text{vac}\rangle$ (k integer), which are pulse-like in the continuous-time basis, i.e., $\langle t|k\rangle = g(t-kT)$, where $g(t)$ vanishes for $t \notin (0,T)$, and $\int dt\, g^*(t)g(t) = 1$. On the input side, we take the wavepackets from $k=0$ to $d-1$ as the subspace of interest for quantum communication. The modes are manipulated by EOMs each capable of applying an arbitrary phase shift to each time bin $[\hat{a}_k^{(\text{out})} = e^{i\phi_k}\hat{a}_k^{(\text{in})}]$ and FBGs that implement the tapped delay line $[\hat{a}_n^{(\text{out})} = \sum_n c_{n-k}\hat{a}_k^{(\text{in})}]$, with the values of c_n chosen to ensure unitarity. After such a sequence, the output wavepacket modes described by $\hat{a}_l^{(\text{out})}$ are given by

$$\hat{a}_l^{(\text{out})} = \sum_{k=0}^{d-1} W_{lk}\hat{a}_k^{(\text{in})}. \tag{1}$$

The EOM/FBG network is completely described by the matrix W, and, in general, the output includes many possible time-bin modes. For convenience, we also define the projection onto the desired d-dimensional output subspace: $V_{lk} = W_{lk}$ ($k, l = 0, 1, \ldots, d-1$). Finally, we consider $d+1$ different parameter sets so that we label the matrices as $W^{(m)}$ and $V^{(m)}$ ($m = 0, 1, \ldots, d$).

Ideally, these $d+1$ matrices $V^{(m)}$ will be both unitary and mutually unbiased, in the sense that

$$|V^{(m)\dagger}V^{(p)}|^2 = \begin{cases} \mathbb{1}_{d\times d}, & m = p \\ \dfrac{1}{d}\text{ones}(d,d), & m \neq p, \end{cases} \tag{2}$$

where the modulus-squared is taken element-by-element, $\mathbb{1}_{d\times d}$ is the $d\times d$ identity matrix, and ones(d, d) is the $d\times d$ matrix with all elements equal to unity. Equation (2) is fully equivalent to the standard definition of MUBs in terms of basis-state overlap, by taking each matrix's rows (or columns) as the coefficients of a particular orthonormal basis. If the proposed system can realize a set of such $d+1$ unitary transformations, then it provides a one-to-one mapping for each state from a given MUB to a time-bin eigenstate, permitting direct measurements with a single time-resolving detector.

To demonstrate the ability of our approach to satisfy Eq. (2) with realistic components, we consider a fixed arrangement consisting of two pairs of EOM/FBG combinations ($N=2$ in Fig. 1) and examine $d=2$, 3, and 4. The choice of $N=2$ strikes a balance between the number of free parameters and computational efficiency in our numerical optimization. From an implementation perspective, we must treat the reconfigurability of EOMs and FBGs differently. The phase sequence imparted by an EOM can be updated rapidly, on the timescale of the chip rate itself, by simply applying a different radio-frequency voltage pattern. On the other hand, the response of each FBG is essentially fixed, with only slow thermal tuning possible (on the order of seconds).[20–22] Thus, we impose the constraint that FBG chips remain fixed across all MUBs, whereas the EOM waveforms are free to vary between them.

For a given dimension d, we search numerically over all possible phase patterns to minimize the average mean-squared error (MSE) between the actual and desired states, defined as

$$\epsilon_{\text{MSE}} = \frac{2}{d(d+1)}\sum_{m=0}^{d-1}\sum_{p=m+1}^{d} \times \left\{\frac{1}{d^2}\sum_{l=0}^{d-1}\sum_{k=0}^{d-1}\left[\left(V^{(m)\dagger}V^{(p)}\right)_{lk} - \frac{1}{d}\right]^2\right\}. \tag{3}$$

This provides a measure of closeness to the MUB condition for the $d+1$ configurations (similar to previous "mubness" parameters[23]). Following MATLAB optimization, we attain solutions for $d=2$, 3, and 4 with $\epsilon_{\text{MSE}} = 1.05\times10^{-7}$, 1.50×10^{-4}, and 1.60×10^{-4}, respectively.

We analyze each of these solutions in the context of $(d+1)$-basis prepare-and-measure QKD. We assume that the sender, Alice, has at her disposal a source emitting single photons in a superposition of d time bins. Using a combination of intensity and phase modulators, she imprints onto each wavepacket the appropriate amplitude and phase to match a basis state chosen at random. She then transmits this state to the receiver, Bob, who utilizes the proposed EOM/FBG system to measure the quantum wavepacket in one of the $d+1$ bases, recording the time bin in which the photon is found at the output. Ideally, he will receive a deterministic result whenever his basis matches that from which Alice prepared her state and a random result for mismatched selections.

Specifically, Alice chooses from the $d(d+1)$ input states

$$|\nu_m[n]\rangle = \frac{\sum_{k=0}^{d-1}\left[V_{nk}^{(m)}\right]^*|k\rangle}{\left(\sum_{l=0}^{d-1}|V_{nl}^{(m)}|^2\right)^{1/2}}; \quad \begin{matrix} m = 0,1,\ldots,d \\ n = 0,1,\ldots,d-1, \end{matrix} \tag{4}$$

using the numerically obtained $d+1$ mode transformations $V^{(m)}$ ($m = 0,1,\ldots,d$). For ideal unitary matrices, the normalization factor in the denominator is unity, but this is not

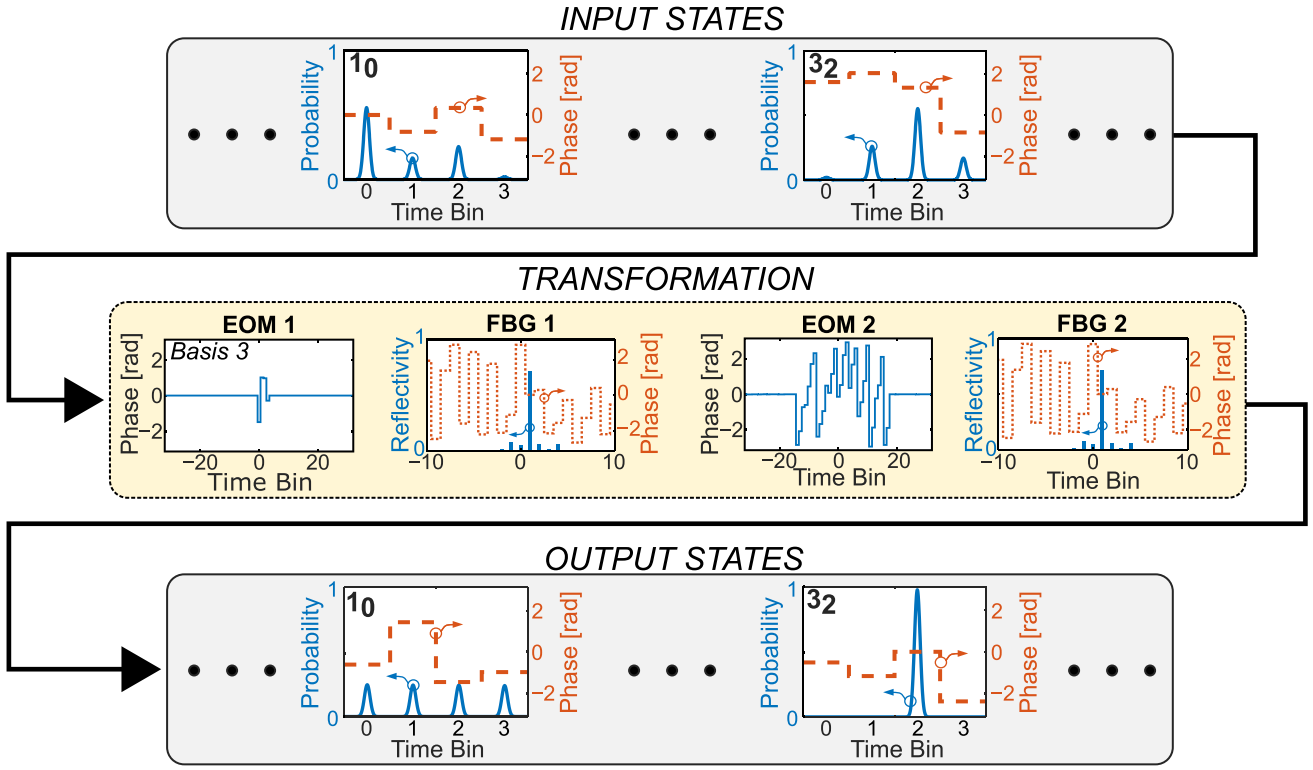

FIG. 2. Examples for $d=4$. Labels 1_0 and 3_2 mark the input/output states corresponding to Alice's choices $|\nu_1[0]\rangle$ and $|\nu_3[2]\rangle$, respectively. The transformation consists of amplitude and phase modulation patterns for basis 3. In practice, the step-function phases need only be constant over the duration of the temporal pulses, with finite transition times acceptable between bins.

necessarily the case here, so it is retained. After Alice sends $|\nu_m[n]\rangle$, Bob applies the transformation $V^{(p)}$ and measures the output time bin q.

Because Bob post-selects on the photon being found in the d-dimensional subspace, we define the detection probability $\mathcal{D}_{pm}[n]$ as the probability that Bob registers a click within bins 0, 1,…, $d-1$ when Alice prepares $|\nu_m[n]\rangle$ and Bob measures in basis p. Similarly, we take $\mathcal{P}_{pm}[q|n]$ as the probability that, conditioned on such a projection into the d-dimensional subspace, the input state is measured in bin q. Both probabilities are important in evaluating the MUBs: $\mathcal{D}_{pm}[n]$ quantifies the intrinsic efficiency of the measurement process while $\mathcal{P}_{pm}[q|n]$ the selectivity in distinguishing states.

As an example of how this protocol could be implemented, we illustrate part of the solution for $d=4$ in Fig. 2. Shown are two of Alice's possible state choices, $|\nu_1[0]\rangle$ and $|\nu_3[2]\rangle$; the amplitude varies pulse-to-pulse, unlike MUBs based on phase states.[7,8] This is a general feature of our solution method, which places no restrictions on the form of the resultant states, in order to maximize flexibility in the optimization algorithm. In this example, Bob applies the transformation corresponding to basis 3, $V^{(3)}$, which outputs a uniform time-bin superposition for the mismatched choice $|\nu_1[0]\rangle$ and a single wavepacket (in bin 2) for the matched choice $|\nu_3[2]\rangle$.

In Fig. 3(a), we provide a histogram of all $d(d+1)^2$ detection probabilities from each solution (the quantities $\mathcal{D}_{pm}[n]$ defined above). Unsurprisingly, given the associated MSE values, $d=2$ has the highest detection probabilities (>0.999). Nonetheless, $d=3$ and 4 still reach values in the range of 0.96–0.99: very close to one and substantially higher than the $1/d$ possible with passive DIs.[7] The post-selected probabilities $\mathcal{P}_{pm}[q|n]$ are also near-ideal, as illustrated in Fig. 3(b), which shows all prepare-and-measure combinations for $d=4$. (Plots of all basis states, measurement settings, and probability distributions for $d=2$, 3, and 4 can be found in the supplementary material.)

To estimate the impact of physical imperfections on the EOM/FBG measurement, we conduct further simulations that add random errors to the phase of each EOM modulation value and FBG chip (keeping the amplitude unchanged). Each perturbation is drawn independently from a Gaussian distribution of variance σ^2. To concentrate only on aspects relevant to our proposal, we introduce no other sources of errors (e.g., transmission loss, detector inefficiency, or dark counts). For each phase error σ, we generate 1000 mode transformations via Monte Carlo simulation, which we take

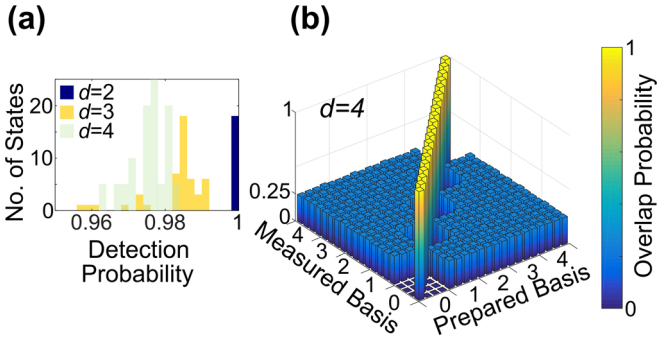

FIG. 3. Time-bin MUBs. (a) Histogram of detection probabilities for all state/measurement combinations. (b) Post-selected probability distributions for $d=4$.

to represent imperfections in Bob's measurement setup, while Alice continues to send the ideal states. Employing the complete probability distributions from the Monte Carlo simulation [perturbed versions of Fig. 3(b)], we extract the quantum bit error rate (QBER) and calculate the corresponding secret key fraction (SKF) using the lower bound for an asymmetric $(d+1)$-basis protocol.[12]

In Fig. 4(a), we show the SKF as a function of QBER, where the error bars indicate statistical uncertainty associated with each dataset generated from the Monte Carlo simulation. The behavior matches that expected for high-dimensional QKD: an SKF of $\log_2 d$ at QBER $= 0$, along with greater tolerance to QBER for larger d. We note that, while generated by introducing phase errors, the scaling shown in Fig. 4(a) depends only on the QBER, regardless of origin; the SKF is insensitive to how phase error, loss, or an eavesdropper contributes to an observed QBER.

Yet to elucidate scaling with phase error only, we plot the SKF against σ in Fig. 4(b) as well. Overall, the trend is similar, with the exception that the $d = 2$ solution shows greater robustness to phase error at high σ, with its SKF even exceeding those of $d = 3$ and 4 at $\sigma = 0.28$ and 0.47, respectively. This feature follows from the quality of the solution itself. As noted above, the metric ϵ_{MSE} is over three orders of magnitude closer to zero for the $d = 2$ solution than for $d = 3$ and 4. The results of Fig. 4(b) then indicate that lower ϵ_{MSE} directly translates to greater robustness against phase error (i.e., lower QBER for a given σ), validating the utility of the metric ϵ_{MSE} in designing QKD systems based on our proposal. Accordingly, one may be faced with a tradeoff in experiment: while more robust against eavesdropping and loss-induced errors, a higher-d solution may actually be less robust against measurement phase error—at least for a fixed number of components. The optimal choice then will depend in part on fabrication and control precision.

An important prerequisite toward implementation is matching the characteristic timescales for EOM, FBG, and detector capabilities. With current single-photon detection jitters <20 ps,[24,25] time-bin spacings must be at least this large; voltage patterns with $\sim$10 ps chips are accessible with modern electronic arbitrary waveform generators,[26] so electro-optic modulation at this speed is achievable. Detailed analysis of our MUB solutions (supplementary material) implies that $\sim$20 chips would be desirable, giving total code durations $\gtrsim 400$ ps, comfortably within the design space of previously fabricated FBGs.[15,16,27] With thermal tuning,[20–22] fine adjustments to each chip's phase could compensate for fabrication errors as well. Coupled with picosecond-level synchronization between Alice and Bob via clock recovery of a wavelength-multiplexed reference pulse train,[28,29] the necessary timing precision should be attainable even at long distances.

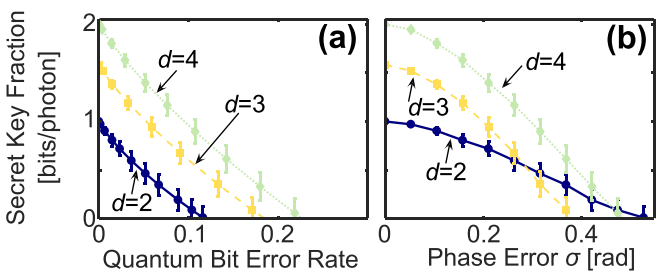

FIG. 4. Predicted QKD performance with errors. (a) Key fraction against quantum bit error rate. (b) Key fraction against random EOM/FBG phase error σ.

From a practical side, insertion loss will also prove important in assessing our scheme for any particular system; 2–3 dB loss is typical for high-performance commercial EOMs, and the low reflectivity of many coded FBGs can reduce output amplitude by several dB as well. However, such loss is of a technical nature—not inherent to the phase operations themselves—and there are important examples of much better performance, including integrated EOMs with $\sim$1 dB loss[30] and apodized coded FBGs with $\sim$90% peak reflectivity.[31]

In summary, we have introduced a scheme for implementing mutually unbiased generation and measurement of time-bin photonic qudits, addressing three persistent challenges in time-bin-based quantum information: (1) preserving single-spatial-mode operation; (2) actualizing multiple MUBs in the same physical setup; and (3) measuring states without $\mathcal{O}(1/d)$ post-selection. While this combination is currently unfulfilled in any other approach, we do note that points (2) and (3) could in principle be addressed by more complex DI networks containing fast phase shifters in each arm and optical switches in lieu of beasmplistters[32]—though extremely fast (multi-GHz) switching speed is required. Far more unique is our ability to complete all processing tasks within the innate stability of a single fiber-optic mode [point (1)]: no other single-mode alternative for time-bin MUBs exists at present. So, in addition to the obvious goal of implementing our scheme experimentally, we hope that our work will motivate the quantum information community to further study the possibilities of coded fiber Bragg gratings for high-dimensional quantum information processing.

See supplementary material for details on each numerical solution and its properties.

We thank B. Qi and P. Lougovski for discussions. This work was performed in part at Oak Ridge National Laboratory, operated by UT-Battelle for the U.S. Department of Energy under Contract No. DE-AC05-00OR22725. J.M.L. acknowledges support from a Wigner Fellowship at ORNL. N.T.I. and D.J.G. acknowledge support from the ONR MURI program, Wavelength-Agile QKD in a Marine Environment (Grant No. N00014-13-1-0627), and the DARPA DSO InPho program. C.C.W.L. acknowledges support from NUS startup Grant No. R-263-000-C78-133/731 and CQT fellow grant.

[1]W. K. Wootters and B. D. Fields, Ann. Phys. **191**, 363 (1989).
[2]T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, Int. J. Quantum Inf. **8**, 535 (2010).
[3]R. B. A. Adamson and A. M. Steinberg, Phys. Rev. Lett. **105**, 030406 (2010).
[4]N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[5]V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[6]T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, J. Phys. B: At., Mol. Opt. Phys. **46**, 104010 (2013).

[7]N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, and D. J. Gauthier, Phys. Rev. Appl. **7**, 044010 (2017).
[8]N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, e1701491 (2017).
[9]D. Hillerkuss, M. Winter, M. Teschke, A. Marculescu, J. Li, G. Sigurdsson, K. Worms, S. B. Ezra, N. Narkiss, W. Freude, and J. Leuthold, Opt. Express **18**, 9324 (2010).
[10]D. Hillerkuss, R. Schmogrow, T. Schellinger, M. Jordan, M. Winter, G. Huber, T. Vallaitis, R. Bonk, P. Kleinow, F. Frey, M. Roeger, S. Koenig, A. Ludwig, A. Marculescu, J. Li, M. Hoh, M. Dreschmann, J. Meyer, M. Huebner, J. Becker, C. Koos, W. Freude, and J. Leuthold, Nat. Photonics **5**, 364 (2011).
[11]N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[12]L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
[13]G. Lima, L. Neves, R. Guzmán, E. S. Gómez, W. A. T. Nogueira, A. Delgado, A. Vargas, and C. Saavedra, Opt. Express **19**, 3542 (2011).
[14]D. Giovannini, J. Romero, J. Leach, A. Dudley, A. Forbes, and M. J. Padgett, Phys. Rev. Lett. **110**, 143601 (2013).
[15]H. Yin and D. J. Richardson, *Optical Code Division Multiple Access Communication Networks* (Springer, 2007).
[16]Y. Dai, X. Chen, Y. Zhang, J. Sun, and S. Xie, in *Optical Fiber Communication Conference* (Optical Society of America, 2007), p. JWA28.
[17]H. Chen, M. Chen, and S. Xie, J. Lightwave Technol. **27**, 4848 (2009).
[18]E. L. Wooten, K. M. Kissa, A. Yi-Yan, E. J. Murphy, D. A. Lafaw, P. F. Hallemeier, D. Maack, D. V. Attanasio, D. J. Fritz, G. J. McBrien, and D. E. Bossi, IEEE J. Sel. Top. Quantum Electron. **6**, 69 (2000).
[19]J. M. Lukens and P. Lougovski, Optica **4**, 8 (2017).
[20]M. R. Mokhtar, M. Ibsen, P. C. Teh, and D. J. Richardson, IEEE Photonics Technol. Lett. **15**, 431 (2003).
[21]Z. Zhang, C. Tian, M. R. Mokhtar, P. Petropoulos, D. J. Richardson, and M. Ibsen, IEEE Photonics Technol. Lett. **18**, 1216 (2006).
[22]C. Tian, Z. Zhang, M. Ibsen, P. Petropoulos, and D. J. Richardson, IEEE J. Sel. Top. Quantum Electron. **13**, 1480 (2007).
[23]I. Bengtsson, AIP Conf. Proc. **889**, 40 (2007).
[24]J. Wu, L. You, S. Chen, H. Li, Y. He, C. Lv, Z. Wang, and X. Xie, Appl. Opt. **56**, 2195 (2017).
[25]I. E. Zadeh, J. W. N. Los, R. B. M. Gourgues, G. Bulgarini, S. M. Dobrovolskiy, V. Zwiller, and S. N. Dorenbos, preprint arXiv:1801.06574 (2018).
[26]Keysight Technologies, www.keysight.com for "AXIe arbitrary waveform generators," (2017).
[27]Z. Si, F. Yin, M. Xin, H. Chen, M. Chen, and S. Xie, Opt. Lett. **35**, 229 (2010).
[28]J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley, and J. Wen, Opt. Express **12**, 2011 (2004).
[29]K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Phys. Rev. X **2**, 041010 (2012).
[30]L. Fan, C.-L. Zou, M. Poot, R. Cheng, X. Guo, X. Han, and H. X. Tang, Nat. Photonics **10**, 766 (2016).
[31]X. Wang, K. Matsushima, K.-I. Kitayama, A. Nishiki, N. Wada, and F. Kubota, Opt. Lett. **30**, 355 (2005).
[32]S. Wang, Z.-Q. Yin, H. F. Chau, W. Chen, C. Wang, G.-C. Guo, and Z.-F. Han, Quantum Sci. Technol. **3**, 025006 (2018).

Reconfigurable, single-mode mutually unbiased bases for time-bin qudits: Supplementary material

Joseph M. Lukens,[1, a)] Nurul T. Islam,[2] Charles Ci Wen Lim,[3] and Daniel J. Gauthier[4]

[1)] *Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA*

[2)] *Department of Physics and Fitzpatrick Institute for Photonics, Duke University, Durham, North Carolina 27708, USA*

[3)] *Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, Singapore*

[4)] *Department of Physics, The Ohio State University, Columbus, Ohio 43210, USA*

(Dated: 27 February 2018)

Here we provide details on the numerical solutions for time-bin MUBs, including the specific EOM/FBG transformations, associated basis states, measurement probabilities, and finite chip number effects.

[a)] Electronic mail: lukensjm@ornl.gov

I. OPTIMAL SOLUTIONS

As noted in the main text, the goal of our simulations is to determine, for a given dimension d, time-bin transformations $W^{(m)}$ $(m = 0, 1, ..., d)$ that are mutually unbiased within the d-mode subspace of interest. After truncating the in general infinite-dimensional space to S modes ($S \gg d$), and considering N unit cells (cf. Fig. 1 of the main text), we can express each transformation $W^{(m)}$ as the matrix product

$$W^{(m)} = C_N D_N^{(m)} \cdots C_1 D_1^{(m)}. \tag{S1}$$

Here, each matrix C_n signifies a FBG with a particular complex reflection pattern, while $D_n^{(m)}$ is a diagonal unitary matrix denoting an EOM that imparts an arbitrary phase shift to each temporal mode.

In contrast to the FBG matrices, the EOM matrices are delineated by basis m. This follows from the rapid reconfigurability of the modulation patterns applied to each EOM, which can be updated quickly to switch the measurement basis. On the other hand, the FBGs are constrained to fixed responses across bases. Each matrix $D_n^{(m)}$ is thus parameterized by a real phase function $\varphi_n^{(m)}[l]$ such that

$$\left(D_n^{(m)}\right)_{lk} = e^{i\varphi_n^{(m)}[l]}\delta_{lk}, \tag{S2}$$

with δ_{lk} the Kronecker delta function, nonzero only when $l = k$.

Although the FBG matrices C_n can be decomposed into complex reflections directly—*i.e.*, as $(C_n)_{lk} = (c_n)_{l-k}$—it is simpler to parameterize C_n in the frequency domain through the transformation

$$C_n = F^\dagger \tilde{D}_n F, \tag{S3}$$

where F is the S-point discrete Fourier transform, and

$$\left(\tilde{D}_n\right)_{lk} = e^{i\phi_n[l]}\delta_{lk}. \tag{S4}$$

is a diagonal matrix of spectral phases. The corresponding complex reflection amplitudes (chips) are then related to the spectral phases via

$$c_n[l] = \frac{1}{S}\sum_{s=0}^{S-1} e^{i\phi_n[s]} e^{2\pi i s l/S}, \tag{S5}$$

so that $\sum_s c_n^*[l-s]c_n[k-s] = \delta_{lk}$ (unitarity) follows automatically.

In this formulation, each FBG and EOM configuration is characterized by S real numbers, for a total of $SN(d+2)$ free parameters, after accounting for the $d+1$ basis choices. The optimality of a given set of matrices $W^{(m)}$ is determined by computing the "mubness" mean-squared-error ϵ_{MSE} [cf. Eqs. (2)-(4) of the main text].

Before delving into the specific solution forms, we note that embedded within this general formulation are several important physical assumptions. First, the electro-optic phase modulation must be fast enough to apply completely arbitrary phases to successive bins. Similarly, the pulse duty cycle must be small enough to avoid any distortion effects from the finite electro-optic phase transition slope. Combined, these conditions ensure that fully arbitrary interpulse phases are realizable, while preserving intrapulse uniformity.

Second, the FBG reflection bandwidth must be wide enough to encompass that of each pulse (otherwise additional loss will result). With this assumption fulfilled, the impulse response delays and phase shifts each pulse without temporal distortion.

Finally, the truncation of the full time-bin Hilbert space to S modes must be large enough to approximate infinity, thereby avoiding numerically-induced artifacts resulting from undersampling. In practical terms, any legitimate solution must not contain coupling from the d computational input modes to the exterior modes of the clipped space, which we can confirm *a posteriori* via numerical filtering (see Sec. IV below).

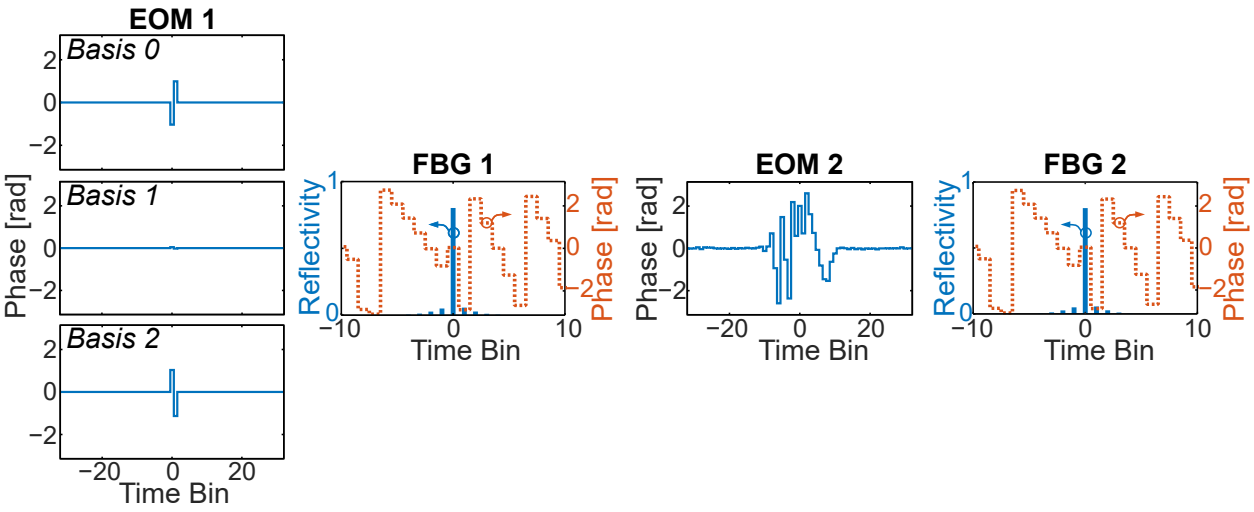

FIG. S1. Phase modulation patterns and impulse responses for each EOM and FBG, respectively, for measuring three MUBs for $d = 2$ time bins. The modulation applied to EOM 1 changes from basis to basis, whereas all other transformations are fixed.

For our solutions, we take $S = 128$, set the number of EOM/FBG unit cells to $N = 2$, and numerically search over all possible phases to minimize ϵ_{MSE}. The solution obtained for $d = 2$ is shown in Fig. S1, which reaches $\epsilon_{\mathrm{MSE}} = 1.05 \times 10^{-7}$. The temporal phase shifts for each EOM and basis ($\varphi_n^{(m)}[l]$) are shown directly. For the FBGs, we highlight the discrete-time impulse responses $c_n[l]$, both reflectivity $|c_n[l]|^2$ and phase $\arg c_n[l]$. Interestingly, although we permit three distinct phase patterns for EOM 2 (one for each basis), the solver converges to a configuration with identical modulation across basis choices. Thus, only EOM 1 must be updated to shift between MUBs, making the solution even simpler than demanded physically. Additionally, we note that the FBG impulse responses are not causal, with appreciable reflectivities at negative delays; this simply means that an overall delay must be present in practice, the amount equal to roughly half of the total number of chips kept in the implementation (quantified in Sec. IV).

The solution for $d = 3$ follows in Fig. S2 ($\epsilon_{\mathrm{MSE}} = 1.50 \times 10^{-4}$). One more MUB is available, and unlike the $d = 2$ case, EOM 2's phases must be modified from basis-to-basis as well as those of EOM 1 (no simplification similar to that of $d = 2$ was found). Rounding

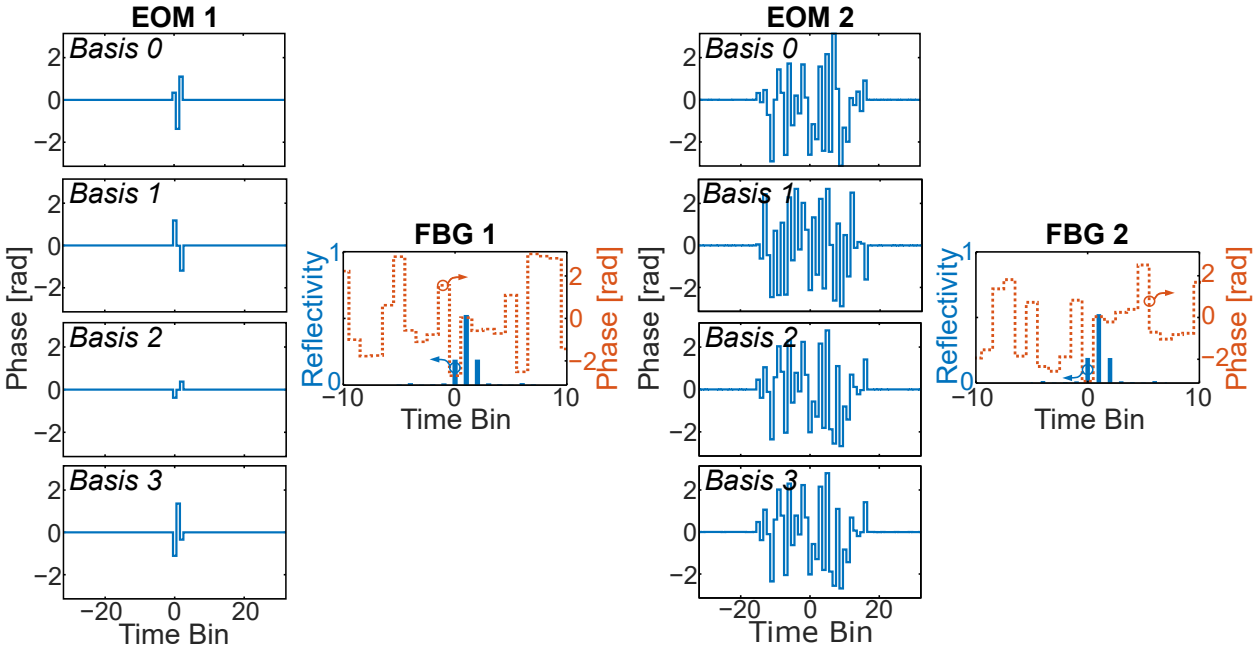

FIG. S2. Modulation functions and impulse responses to realize four MUBs on time-bin qutrits ($d = 3$). The phase modulation patterns applied to both EOM 1 and EOM 2 are selected to produce a particular basis measurement.

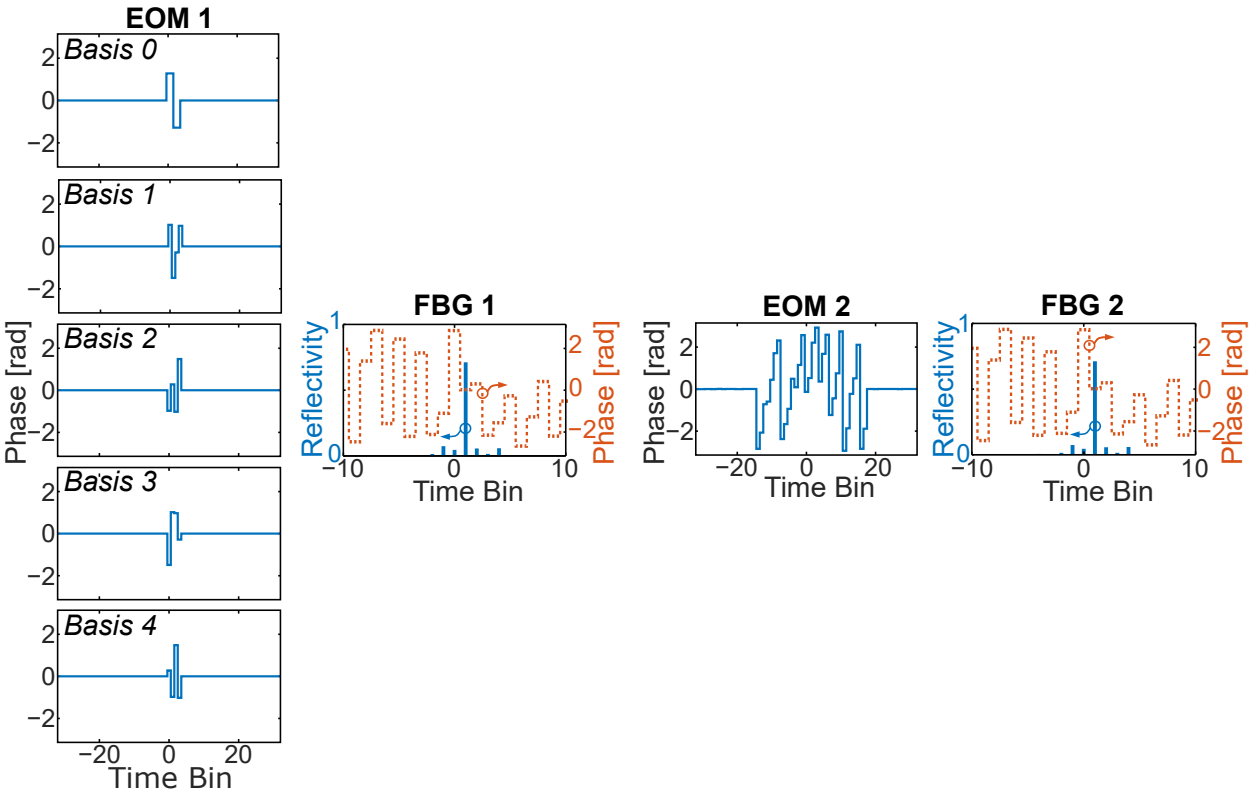

FIG. S3. EOM and FBG transformations producing MUBs for $d = 4$. By selecting the particular phase modulation pattern for EOM 1, any of five mutually unbiased measurements can be effected.

out the optimizations, Fig. S3 furnishes the modulation functions for the five MUBs in $d = 4$, which together enable $\epsilon_{\mathrm{MSE}} = 1.60 \times 10^{-4}$. As with the $d = 2$ case, the second EOM is fixed across bases, demanding only that EOM 1 be modified from measurement to measurement.

II. BASIS STATES

We next examine the basis states corresponding to the mode transformations described above. As specified by Eq. (5) of the main text, we define the normalized state vectors $|\nu_m[n]\rangle$ $(m = 0, 1, ..., d;\ n = 0, 1, ..., d-1)$ such that applications of transformation $W^{(m)}$ ideally projects $|\nu_m[n]\rangle$ onto the pure time bin $|n\rangle$, whereas $W^{(m')}$ $(m' \neq m)$ produces an equi-amplitude d-mode time-bin superposition. In this way, all detections occur within the time-bin eigenbasis, even though the input states themselves may possess a nontrivial phase/amplitude structure.

For example, Fig. S4 shows the six basis states for $d = 2$. The probability and phase are

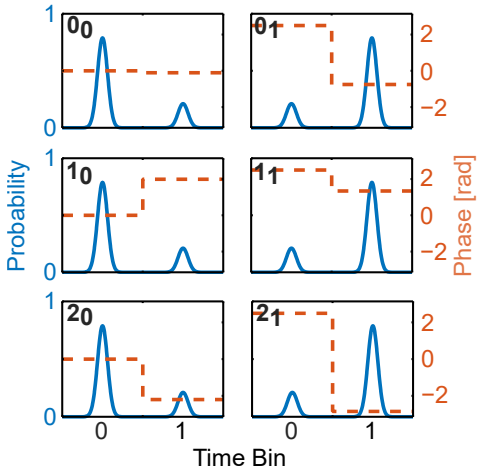

FIG. S4. Basis states for $d = 2$. Each row denotes one of the three MUBs; subscripts label the particular states.

shown as functions of time bin, with a finite pulse width provided for aesthetics. The label pair m_n marks state n of basis m ($|\nu_m[n]\rangle$). Because we enforce no *a priori* requirement that one MUB be the time-bin basis (the optimizer is free to choose), all states show finite probability in both basis states; this poses no serious technical limitation in state preparation, since amplitude and phase can be readily set by modulators. The greater challenge is the basis measurement—precisely what this EOM/FBG setup accomplishes.

Figures S5 and S6 show the basis states for the $d = 3$ and $d = 4$ solutions, respectively. The same considerations and formalism for $d = 2$ apply here as well.

III. DETECTION PROBABILITIES

As noted in the main text, single-photon states prepared according to each solution (from Figs. S4-S6) and sent through the relevant EOM/FBG network (Figs. S1-S3) are projected onto time-bin states that signify the d possible outcomes in the chosen measurement basis. For a given state selection $|\nu_m[n]\rangle$ and measurement $V^{(p)}$, we quantify performance via two metrics: (i) the detection probability $\mathcal{D}_{pm}[n]$, which gives the probability the photon indeed remains in the d-dimensional output subspace; and (ii) the post-selected probability $\mathcal{P}_{pm}[q|n]$ that, given the photon does remain in the desired subspace, it is found in time-bin q.

Figure S7 shows these values for all three solutions ($d = 2, 3, 4$). Panels (a) and (b) are reproduced from Fig. 3 of the main text, but are included here to aid in comparison of the

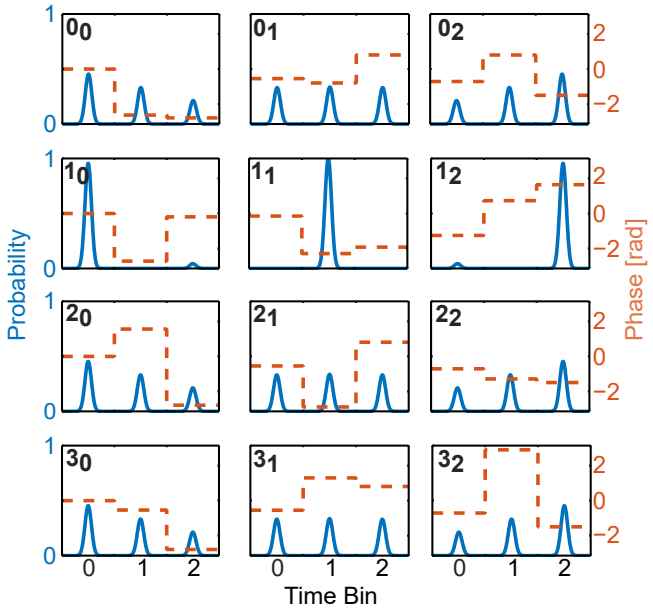

FIG. S5. Basis sates for $d = 3$.

results for all dimensions. The histogram of Fig. S7(a) bins the $d(d+1)^2$ detection probabilities [$d(d+1)$ total basis states $\times$ $(d+1)$ measurement choices]. The case $d = 2$ is closest to the ideal, with $d = 3, 4$ still attaining values of $\mathcal{D}_{pm}[n]$ above $\sim$0.96. The post-selected probabilities for $d = 2, 3, 4$ follow in Figs. S7(b)-(d). For all three cases, matched basis choices produce localized probability peaks, as expected for near-perfect correlation. Mismatched choices leave uniform outcomes for each input state, all with probabilities around $1/d$. These probability sets form the foundation of our estimates of QKD performance.

IV. CHIP NUMBER ANALYSIS

In evaluating the aforementioned solutions in the context of practical implementation, an important consideration is the effective number of chips needed on each FBG to realize full functionality. For while parameterizing the FBG transformation in the frequency domain [Eq. (S3)] proves extremely convenient for enforcing unitarity, the resulting impulse response can potentially extend over the entire numerical domain. To monitor against such a situation, here we intentionally remove chips from the FBG responses and quantify the impact on basis measurement performance. Such tests serve a twofold purpose: (i) they validate the solution's trustworthiness against potential aliasing effects resulting from numerical

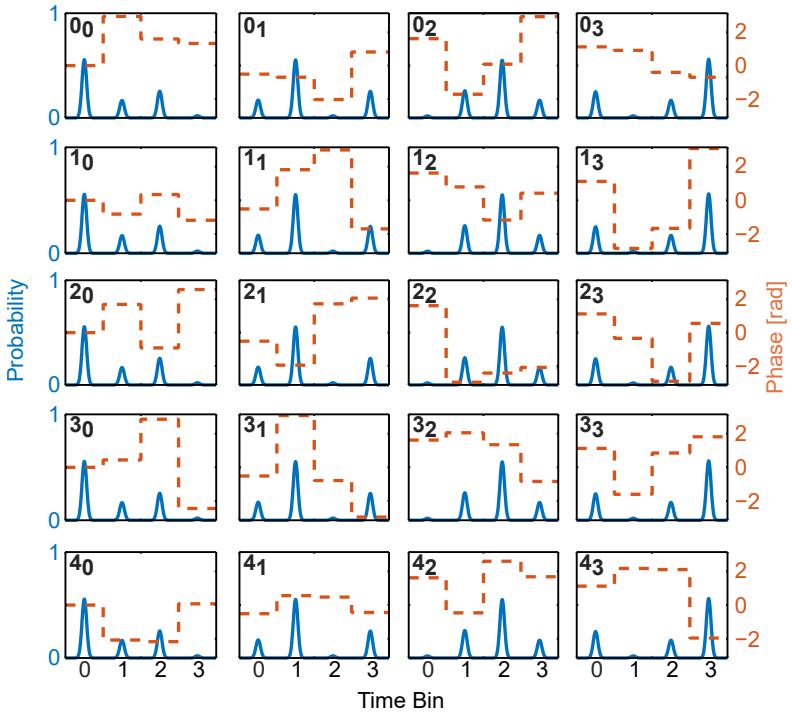

FIG. S6. Basis states for $d = 4$.

truncation; (ii) they reveal precisely just how many chips are required from fabricated FBGs.

For our particular solutions, we force all but some subset of FBG chips to zero and recompute the average MSE (ϵ_{MSE}). Starting with only one nonzero chip (time-bin 0 in the FBG plots above), we successively increase the number of chips in increments of two—adding one preceding time bin and one succeeding. The results of these tests for all dimensions $d = 2, 3, 4$ are given in Fig. S8. As expected, the error begins high and drops off rapidly, until leveling off at the respective optima. The error floors are reached well before incorporating the full numerical size (128 chips), confirming the validity of the solutions in light of modal truncation. Finally, for the purposes of design, we observe that including any chips beyond $\sim$20 is superfluous in all cases, thus providing a quantitative bound on required complexity. We make use of this number in the main text to estimate FBG length in view of the expected time-bin spacing.

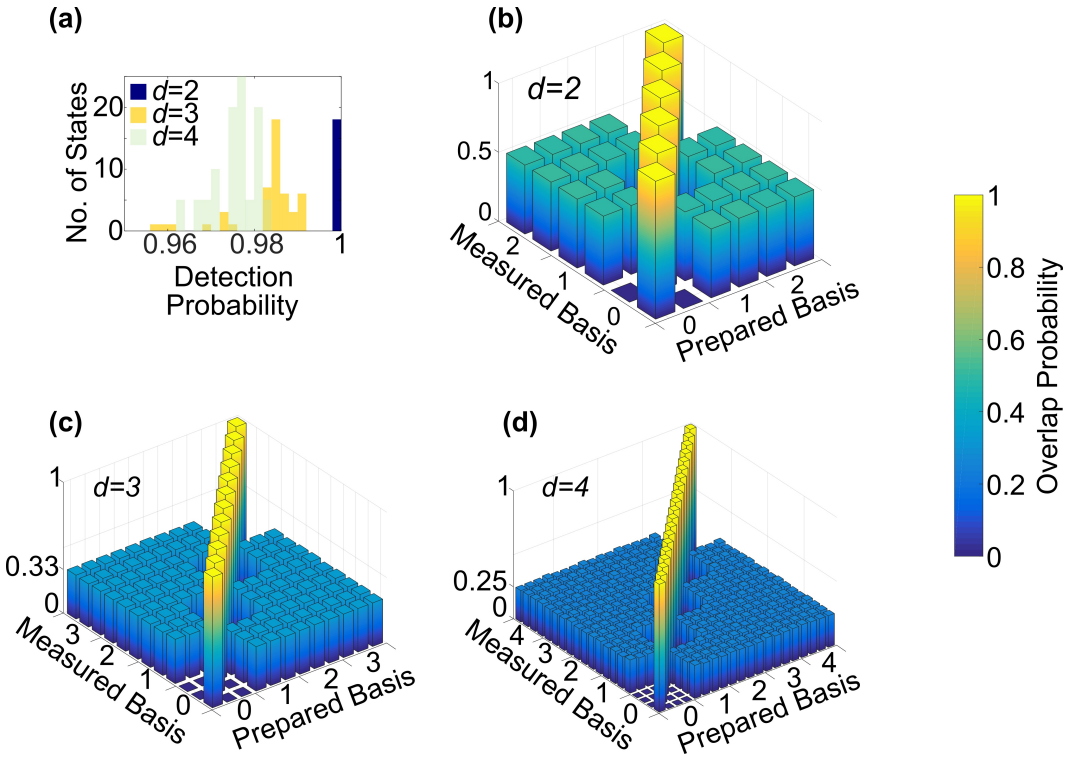

FIG. S7. (a) Histogram of detection probabilities $\mathcal{D}_{pm}[n]$ for all state/measurement basis combinations. Post-selected probability distributions $\mathcal{P}_{pm}[q|n]$ for (b) $d = 2$, (c) $d = 3$, and (d) $d = 4$. The tick marks at $1/d$ show the expected level for mismatched prepare/measure basis choices.

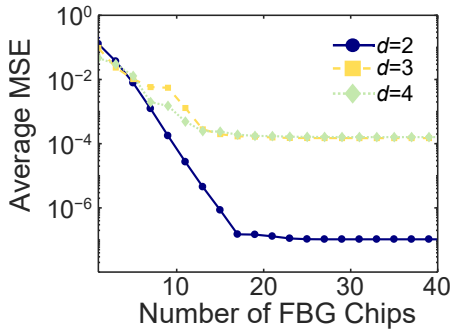

FIG. S8. Average mean-squared error (ϵ_{MSE}) as a function of the number of chips applied by each coded FBG.