optica

Multi-core fiber integrated multi-port beam splitters for quantum information processing

J. Cariñe,[1,2] G. Cañas,[3] P. Skrzypczyk,[4] I. Šupić,[5] N. Guerrero,[1,2] T. Garcia,[1,2] L. Pereira,[1,2] M. A. S. Prosser,[6] G. B. Xavier,[7] A. Delgado,[1,2] S. P. Walborn,[1,2,8] D. Cavalcanti,[5] and G. Lima[1,2,*]

[1]Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile
[2]Millennium Institute for Research in Optics, Universidad de Concepción, 160-C Concepción, Chile
[3]Departamento de Física, Universidad del Bio-Bio, Avenida Collao 1202, Concepción, Chile
[4]H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, UK
[5]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain
[6]Departamento de Ciencias Físicas, Universidad de la Frontera, Temuco, Chile
[7]Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden
[8]Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, Rio de Janeiro, Rio de Janeiro 21941-972, Brazil
*Corresponding author: glima@udec.cl

Received 21 January 2020; revised 26 March 2020; accepted 8 April 2020 (Doc. ID 388912); published 15 May 2020

Multi-port beam splitters are cornerstone devices for high-dimensional quantum information tasks, which can outperform the two-dimensional ones. Nonetheless, the fabrication of such devices has proven to be challenging with progress only recently achieved with the advent of integrated photonics. Here, we report on the production of high-quality $N \times N$ (with $N = 4, 7$) multi-port beam splitters based on a new scheme for manipulating multi-core optical fibers. By exploring their compatibility with optical fiber components, we create four-dimensional quantum systems and implement the measurement-device-independent random number generation task with a programmable four-arm interferometer operating at a 2 MHz repetition rate. Due to the high visibilities observed, we surpass the one-bit limit of binary protocols and attain 1.23 bits of certified private randomness per experimental round. Our result demonstrates that fast switching, low loss, and high optical quality for high-dimensional quantum information can be simultaneously achieved with multi-core fiber technology.

https://doi.org/10.1364/OPTICA.388912

1. INTRODUCTION

Space-division multiplexing (SDM) is currently the main technology considered to overcome the actual capacity limitation of optical telecommunication networks [1]. Basically, it consists of specially designed fibers that can support distinct optical spatial modes in order to increase the multiplexing capabilities. The optical fibers employed in SDM can be divided into two main groups: multi-core fibers (MCFs) [2,3] and few-mode fibers (FMFs) [4–8]. In the former, several single-mode cores are physically contained within the same common cladding, with each core being used independently. A FMF on the other hand consists of a single core that supports several optical modes, each of them capable of transmitting data independently.

Arguably, the development of a major part of experimental quantum information (QI) relies on the fact that it is based heavily on the same hardware employed by classical optical communication [9–13]. Therefore, it is natural to expect that future development will take place using SDM hardware [14]. Indeed, in the past couple of years, the first quantum communication experiments based on MCFs have appeared. The first one used a MCF as a direct multiplexing device: with one core acting as the quantum channel, while other cores contained classical data [15] (see also Refs. [16–19]). Later, the fact that all cores are placed in a common cladding, translating to a long multi-path conduit with intrinsic phase stability, was explored for demonstrating the feasibility of high-dimensional (HD) quantum key distribution over MCFs [20,21]. The relative phase difference between multiple cores of MCF fibers has been shown to be more stable than that of multiple single-mode fibers by at least two orders of magnitude over a 2 km fiber link [22]. The benefit of MCFs for QI has been further reinforced by showing that they can support propagation of entangled photons [23,24]. Similar research has begun for FMFs [25–30]. HD entanglement is advantageous in this regard, as it can be more resistant to noise [31].

Additionally, SDM technology has been exploited for building MCF-based optical fiber sensors, whose remote interrogation capabilities make them attractive for industrial applications

[32–36]. MCF optical sensors have been used for high-temperature sensing up to 1000°C with a typical temperature sensitivity as high as 170 pm/°C [35]. The advantage of using MCFs is that they allow for the fabrication of multi-arm Mach–Zehnder (MZ) interferometers that have higher sensitivity for phase changes since the slopes of the resulting interference peaks are steeper. There has been a large variety of MCF optical sensors but most of them rely on inefficient techniques to launch light into the multi-arm MZ, resulting in prohibitive losses for QI processing. Of particular interest is the work of Gan *et al.* [36], where the authors develop new tapering techniques to build the multi-arm MZ directly into a specially designed MCF.

Inspired by such progress in optical sensing, we report on the production of high-quality $N \times N$ (with $N = 4, 7$) multi-port beam splitters (MBSs) built in commercially available multi-core fibers and their usage for building fast, low-loss, and programmable multi-arm MZ interferometers suitable for QI. In the field of quantum computing, optical interferometers have attracted much attention. Since the seminal work of Knill, Laflamme, and Milburn [37], it has been known that one possible road to universal quantum computing is through an architecture composed of single-photon sources, detectors, and linear-optic multi-arm interferometers. Such interferometers work as quantum circuits that are especially relevant for efficient processing of HD photonic quantum systems (qudits), whose generation has now been harnessed [38–51]. Nonetheless. the development of MBS devices has proven to be challenging [52]. Recent progress has been made with the advent of integrated photonics [21,49,53–55], where multi-arm interferometers are built resorting to a mesh of conventional 2×2 beam splitters [56,57]. In this case, the circuits can present balanced and unbalanced losses, and depending on the circuit size, the fidelity of the operations can be compromised [58,59]. By taking a new approach based on MCFs for building multi-arm interferometers, we present both: (i) a new technology that has technical advantages and is fully compatible with previous efforts in integrated photonics [21], and that at the same time (ii) can be independently used for high-quality processing of QI. It allows one to exploit the stability and compactness of MCF fibers, and their compatibility with trends in telecommunication technology, to build new robust schemes for optical sensing, communication and information processing. Note that N-arm interferometers can also be built with 2×2 in-fiber beam splitters, but the scaling of the quantum circuit favors the use of MBSs. While two $N \times N$ MBSs suffice for a large class of transformations, the number of 2×2 50:50 beam splitters is $N(N-1)$ [56,60,61].

To demonstrate the viability of our approach for HD-QI, we consider the task of random number generation (RNG), which finds several applications in cryptography, gambling, and numerical simulations. In the classical domain, randomness is associated with our ignorance about the parameters describing a process. This perspective is not enough for cryptographic protocols, where we would like to certify that certain data are random for an eavesdropper that could have more knowledge or computational power than the user [62]. This problem was solved by fully device-independent (DI) RNG protocols [63], which makes no assumptions about the source or measurements being used in the protocol [64]. However, this approach is quite demanding and typically results in very low random bit rates (see, e.g., [65]). A solution is to consider semi-DI scenarios [66–71], where partial knowledge of the implementation is assumed. In our scheme, we assume that we control the source of quantum states but do not assume anything about the measurements we perform, a situation called measurement-DI (MDI) RNG [72]. Our implementation resorts to a MCF-based four-arm interferometer operating at 2 MHz repetition rate, which generates and measures path encoded four-dimensional qudit states with fidelities higher than 99.4%. Moreover, we employ theoretical techniques that allow us to handle the issues with finite statistics, and use semi-definite programming to estimate the randomness in this MDI setting. This allows us to attain a generation rate of 1.23 random bits per experimental round, which surpasses the one-bit limit of binary RNG protocols, thus proving the usefulness of exploiting qudit states for RNG.

Last, we note that the average insertion loss for the fabricated 4×4 (7×7) MBSs is only 4.3% (9.0%), which allows for a qudit transmission of 42% through the programmable circuit and a corresponding overall detection efficiency that can reach at least 35% with commercially available superconducting single-photon detectors (efficiency >85%). This result, together with the interferometer's fast switching and high optical quality, yields potential advantages of this technology for quantum communication [73,74], sensing [75], and computation [76,77].

2. FABRICATION, MODELING, AND VALIDATION OF MULTI-PORT BEAM SPLITTERS

As mentioned before, the cladding of a MCF is composed of several cores, which can be exploited for the propagation of path qudit states defined as the coherent superposition $|\Psi\rangle = \frac{1}{\sqrt{k}} \sum_0^k e^{i\phi_k} |k\rangle$ [20], where $|k\rangle$ denotes the state of the photon transmitted by the kth core mode, and ϕ_k is the relative phase acquired during propagation over the kth core [see Fig. 1(a)]. High-quality 4×4 MBSs are constructed directly in a four-core optical fiber through a tapering technique recently introduced in [36]. In that work, the authors were interested in building multi-arm MZ interferometers for multi-parameter estimation. Their idea was to use

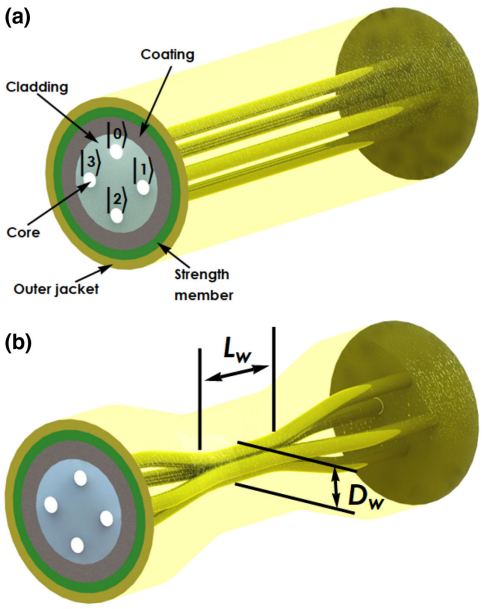

Fig. 1. Schematics of a MCF and of the fabricated MBSs. (a) MCF before tapering and the qudit encoding strategy. (b) The fiber is then heated along a length L and pulled symmetrically from both ends, stretching and thinning the fiber. The final device is the MBS and has a length L_W with diameter D_W.

a heterogeneous multi-core fiber. This fiber is used to minimize inter-core coupling, as it has lower refractive index "trenches" around the cores. In such fibers, there are at least two orthogonal modes propagating over one core of the fiber, which normally never interfere. Nonetheless, by tapering this fiber, they created an overlap between such modes due to strong evanescence effects in the tapered zone. From the interference observed, parameter estimation was possible. The authors then used each core interference for estimating different parameters of a sample. The fiber worked as an instrument composed of several two-path MZ interferometers. In their tapered region, the inter-coupling between different cores was severely reduced by such trenches.

Here, we show that by employing the same technique but with homogeneous MCFs, i.e., fibers where the N cores are not bounded by refractive index trenches, one can build high-quality $N \times N$ MBSs. The tapering is performed by locally heating a small transverse region of the fiber with length L, while applying a controlled longitudinal stretching tension. Since the fiber is mechanically in a partial soft state, it will become thinner with a final diameter D_w at the center of the region where the heat is applied. The cores will consequently be brought together, and due to evanescent coupling, light will leak from one core to the others, similar to what is obtained in a standard fiber-optical bi-directional coupler [see Fig. 1(b)]. The splitting ratio can be balanced by monitoring the transmission of a 1550 nm laser beam sent through the four-core fiber while tapering it. Finally, since the MBS is directly constructed on a MCF, it is compatible for connection with other MCFs by direct contact.

We test the fabricated four-core MBSs by first illuminating one of the cores of a MCF. This fiber is connected to the MBS under test, and at the output, the light is split across the other cores. Figure 2(a) shows the image of the output facet of one MBS on an infrared CCD camera, clearly showing the four-core pattern, as well as the cores fully illuminated. We then measure the output power per core individually with p-i-n photodiodes. Figure 2(b) shows the normalized intensity at each core following the MBS and its evolution over time. The power at each core is very stable and the observed average split ratio is (0.248 ± 0.01). The average insertion loss of the 4×4 MBSs is $(4.3 \pm 0.06)\%$.

In general, symmetric 4×4 MBSs are parameterized in terms of the unitary operation given by [52,56,57]

$$V = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{i\phi} & -1 & -e^{i\phi} \\ 1 & -1 & 1 & -1 \\ 1 & -e^{i\phi} & -1 & e^{i\phi} \end{bmatrix}. \tag{1}$$

Since the cores are equally distant to the center of the four-core MCF, in the tapered zone, they will have the same length L_w. So, it is expected that the MCF MBSs should be described by V when $\phi = 0$. We confirm this by experimentally measuring the unitary implemented by a 4×4 MCF MBS, resorting to the quantum process tomography technique introduced in [78]. Any unitary device is described by $U = \sum_{jk} u_{jk} e^{i\phi_{jk}} |j\rangle\langle k|$. The parameters u_{jk} for our MBS are obtained from the split ratios recorded in the procedure described above. The relative phases are measured by sending states of the form $|\phi_j\rangle = \frac{1}{\sqrt{2}}(|1\rangle + e^{i\varphi}|j\rangle)$ through the MBS. At the MBS output ports, the probabilities of recording the photon are given by $p(k|j) = \frac{1}{2}[u_{k1}^2 + u_{kj}^2 + 2u_{k1}u_{kj}\cos(\varphi + \phi_{kj} - \phi_{k1})]$. Hence, by recording these probabilities with respect to φ, we acquire the relative phases $\phi_{kj} - \phi_{k1}$.

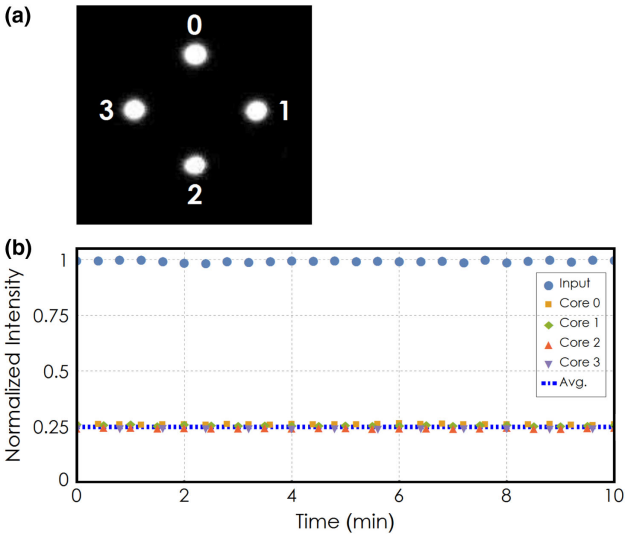

Fig. 2. Multi-port beam splitter performance. (a) Image of the facet of the output of a MCF 4×4 MBS as seen by an infrared CCD camera. (b) Output normalized optical power of each core of the MBS as a function of time.

Using the scheme in Fig. 3 explained below, we obtain the experimental matrix $\tilde{U}$. Nonetheless, due to inherent experimental errors, this matrix is never unitary. In order to obtain the unitary matrix describing the 4×4 MCF MBS, one can optimize a cost function of the experimental data. For this purpose, the fidelity between two matrices, given by $F(A, B) = \frac{1}{N^2}|\mathrm{Tr}(A^\dagger B)|^2$ [79,80], is typically used as a figure of merit. Then, the final MBS matrix is given by the optimization problem: $\hat{U} = \mathrm{argmin}_V\,[1 - F(\tilde{U}, V)]$. Following this procedure, we determine that our MCF MBS matrix representation is

$$\hat{U} = \begin{bmatrix} 0.499 & 0,501 & 0,499 & 0,499 \\ 0,501 & 0,491 + 0,08i & -0,496 - 0,06i & -0,498 - 0,01i \\ 0,499 & -0,495 - 0,06i & 0,498 + 0,03i & -0,499 + 0,03i \\ 0,499 & -0,499 - 0,01i & -0,499 + 0,03i & 0,499 - 0,01i \end{bmatrix}, \tag{2}$$

which has a fidelity with the model of Eq. (1) given by $F(\hat{U}, V_{\phi=0}) = 0.995 \pm 0.003$, confirming the high quality of the 4×4 MCF MBSs. Last, we note that our technique can be extended to MCFs of more cores for creating MBSs with more input/output ports. We present the characterization of a 7×7 MCF MBS in Supplement 1. The average insertion loss of that 7×7 MBS is $(9.0 \pm 0.04)\%$.

3. MULTI-ARM INTERFEROMETERS BASED ON MULTI-CORE FIBERS

A programmable quantum circuit allows one to prepare different quantum states and measure them with different bases in a controllable way. Now, we show (i) how the MCF MBSs can be used to build a multi-arm MZ interferometer, and (ii) how off-the-shelf telecommunication components can be incorporated into it for implementing an efficient quantum circuit.

In our scheme (see Fig. 3), the light source is composed of a semiconductor distributed feedback telecom laser ($\lambda = 1546$ nm)

connected to an external fiber-pigtailed amplitude modulator (FMZ). Driven by a field programmable gate array electronic unit (FPGA1), we use the FMZ to externally modulate the laser to generate optical pulses 5 ns wide. Optical attenuators (ATTs) are then used to create weak coherent states [9].

Following the ATT, we use a commercial spatial demultiplexer/multiplexer unit (DEMUX) [81,82], with insertion losses around 3.2%. This device is composed of four independent single-mode fibers connected to a four-core MCF. Each single-mode fiber is mapped to one of the cores of the MCF fiber. In our system, after the first DEMUX, only one of the MCF cores is illuminated, which is shown schematically in Fig. 3. This MCF fiber is then connected to a 4×4 MBS as the starting point of the programmable four-arm MZ interferometer. A second DEMUX unit (identical to the initial one but connected in reverse) is then used to separate the cores in individual single-mode fiber outputs, allowing access to each core. Each path contains two fiber-pigtailed $LiNbO_3$ phase modulators (PMs) with 10 GHz bandwidth. This allows us to prepare and measure a more general class of path qudit states. Each PM has an internal polarizer used to align the photon polarization state such that in the interferometer there is no path information available [83,84], which would compromise the visibility of the observed interference. Fiber-based polarization controllers (not shown) are used in each path to maximize transmission through the PMs. The first set of PMs is also controlled by the FPGA1 unit and are used for state preparation. The general form of the states that are prepared is

$$|\chi\rangle = \frac{1}{2}(e^{i\phi_0^A}|0\rangle + e^{i\phi_1^A}|1\rangle + e^{i\phi_2^A}|2\rangle + e^{i\phi_3^A}|3\rangle), \tag{3}$$

where ϕ_k^A is the phase applied by the first modulator in mode k.

Finally, the state projection is done by another 4×4 MBS, whose input is first converted from the four individual single-mode arms to a single four-core fiber by a third DEMUX unit. Considering the 4×4 MCF MBS matrix representation, and the action of the second set of PMs, one can show that the form of the measurement basis states at the end of the circuit are given by

$$\begin{aligned}
|\psi_0\rangle &= \frac{1}{2}(e^{i\phi_0^B}|0\rangle + e^{i\phi_1^B}|1\rangle + e^{i\phi_2^B}|2\rangle + e^{i\phi_3^B}|3\rangle),\\
|\psi_1\rangle &= \frac{1}{2}(e^{i\phi_0^B}|0\rangle + e^{i\phi_1^B}|1\rangle - e^{i\phi_2^B}|2\rangle - e^{i\phi_3^B}|3\rangle),\\
|\psi_2\rangle &= \frac{1}{2}(e^{i\phi_0^B}|0\rangle - e^{i\phi_1^B}|1\rangle + e^{i\phi_2^B}|2\rangle - e^{i\phi_3^B}|3\rangle),\\
|\psi_3\rangle &= \frac{1}{2}(e^{i\phi_0^B}|0\rangle - e^{i\phi_1^B}|1\rangle - e^{i\phi_2^B}|2\rangle + e^{i\phi_3^B}|3\rangle),
\end{aligned} \tag{4}$$

where ϕ_k^B is the phase applied by the second modulator in the core mode k. The second set of PMs is independently controlled by a second FPGA2 unit. In order to connect the second 4×4 MBS to single-photon detectors (D_i) and conclude the measurement process, a fourth DEMUX unit is employed to split the four-core fiber into four single-mode fibers. They are each connected to commercial InGaAs single-photon detection modules, working in gated mode and configured with 10% overall detection efficiency, and 5 ns gate width. The detectors' counts are simultaneously recorded by the FPGA2 unit. Through the control of the clock-synchronized FPGA units, one can program the generated path qudit states and measurements to be implemented by the circuit. Last, we note that while only three PMs are needed for each set, we opted to maintain the fourth one for easily matching the paths for future applications.

The interferometer occupies a 30 cm × 30 cm area and is thermally insulated to minimize additional random phase drifts between the single-mode fibers. Nevertheless, long-term phase drifts are present, and we implemented a control system to actively compensate for them. The control is implemented by FPGA2 and based on a perturb and observe power point tracking method [85]. More specifically, each applied phase ϕ_k^B can be decomposed as $\phi_k^B = \phi_k^{\text{bias}} + \phi_k^{\text{mod}}$, where the employed voltage driver is capable of supplying the sum of two independent voltages V_{bias} and V_{mod}. V_{bias} is a low-speed signal used to control ϕ_k^{bias}, and this is intended to compensate for a given phase drift ϕ_k^n. V_{mod} is the high-speed signal for modulating the desired phase ϕ_k^{mod}. Since the total relative phase at the k_{th} arm is $\phi_k^B = \phi_k^{\text{bias}} + \phi_k^{\text{mod}} + \phi_k^n$, the phase drift compensation algorithm running in FPGA2 will perturb the kth PM to make $\phi_k^{\text{bias}} = -\phi_k^n$, such that the phase noise is eliminated. This is done by maximizing the number of photo counts at detector D_0, which corresponds to a situation where there is constructive interference. The algorithm does this sequentially to each PM at the measurement stage. The multi-arm interferometer works with a repetition rate of 2 MHz and has an integration time of 0.1 s. When the system is initialized, the stabilization control typically takes around 15 s to align the interferometer, as shown in the experimental data in Fig. 4(a), where the control system is activated at $t = 50$ s. When this point is achieved, the quantum circuit automatically prepares the desired states and performs the required measurements over experimental blocks of 0.1 s. The control system monitors the phase stabilization of the interferometer in real time, such that it stops the measurement procedure every 0.2 s to check the stabilization. The circuit can realign itself and run for several days continuously. To show the quality of the MCF-based multi-arm interferometer, we gradually generate the quantum

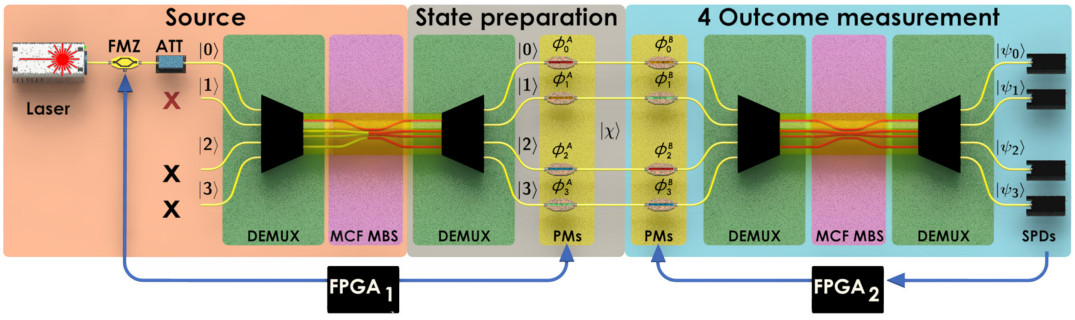

Fig. 3. Schematics of the experimental setup implementing the programmable quantum circuit for HD quantum information processing. Please see the main text for details.

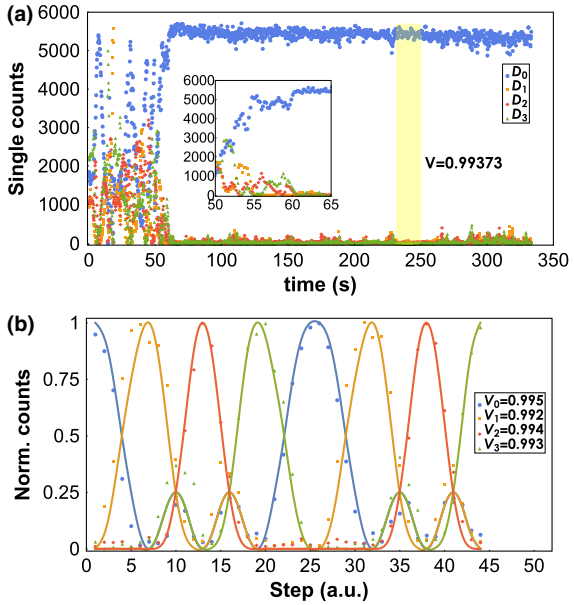

Fig. 4. Phase stabilization and interference fringes of the four-arm programmable circuit. (a) Active stabilization of the multi-arm interferometer (integration time 0.1 s). Inset shows a zoom between 50 and 65 s showing the settling time of the control system after turning it on. (b) Detection rate as a function of modulated phases ϕ_k^A (integration time 1 s).

states associated with each outcome of the interferometer when all ϕ_k^B s are set to zero, obtaining the traditional interference curves in Fig. 4(b). The average visibility recorded is 0.992 ± 0.0015, showing that path qudit states can be prepared and measured with high fidelities in our scheme.

One last point is related with the overall detection efficiency of the circuit, which is a crucial parameter for many fundamental studies and applications in QI science. In our circuit, the transmission of the generated ququarts through the measurement stage is $(43 \pm 0.1)\%$, which is limited mainly by the second set of PMs that add an average 2.05 dB of insertion losses. Note, however, that this value represents a gain of up to two orders of magnitude compared with some aforementioned HD experiments, where filtering techniques drastically reduce the transmission of the employed schemes (see [20], e.g.). Considering that new commercially available superconducting detectors can reach more than 85% of detection efficiency, one can see that our system is capable of reaching at least 35% of overall detection efficiency. Moreover, PMs with smaller insertion losses (<5%) based on poled fibers [86,87] have recently been developed which could be incorporated to the system, and we estimate that an optimized circuit could reach 65% overall efficiency.

4. MEASUREMENT-DEVICE-INDEPENDENT RNG: THEORY

In the scenario of MDI RNG, an end-user in need of random numbers possesses a characterized preparation device and an uncharacterized measurement device $\mathcal{M}$ [72]. This scenario is relevant nowadays, as single-photon detectors are prone to side-channel attacks, which has motivated the development of similar approaches in quantum key distribution [88]. The preparation device is used to prepare quantum states, $\{\omega_x\}$, that are measured by the uncharacterized measuring device $\mathcal{M}$, leading to a classical outcome a. By repeating the process, one estimates the probabilities $p(a|\omega_x)$. Importantly, $\mathcal{M}$ could have been constructed by an eavesdropper (named Eve), who aims to predict the outcome a. Eve in principle can even be quantum-correlated with $\mathcal{M}$, by holding half of an entangled state ρ^{AE}, the other half of which is inside the device. $\mathcal{M}$ performs a measurement on the input state ω_x and a part of ρ^{AE}, while Eve makes a measurement on her part of ρ^{AE} to guess the bit generated.

In Ref. [72], it was shown that the maximal probability $P_g(x^*)$ that Eve guesses correctly the outcomes a for a given input x^*, compatible with $p(a|\omega_x)$, can be estimated by the solution of a semi-definite program [89]. Finally, the amount of randomness that is certified per round under the assumption that Eve carries out individual attacks is given by the min-entropy of P_g:

$$H_{\min}(x^*) = -\log_2 P_g(x^*). \tag{5}$$

A drawback of the approach proposed in [72] is that it relies on having exact knowledge of the probabilities $p(a|\omega_x)$. In any real experiment, we have access to only a finite number of experimental rounds, which allows us to estimate the frequencies $\xi(a|\omega_x)$ at which different measurement results are observed. To account for finite-statistics effects we adapt the semi-definite program described in Ref. [72] to make use of the Chernoff–Hoeffding tail inequality [90]. This inequality asserts that with high probability, $p(a|\omega_x)$ is bounded by the observed frequencies $\xi(a|\omega_x)$ via

$$\xi(a|\omega_x) - t_x(\epsilon) \le p(a|\omega_x) \le \xi(a|\omega_x) + t_x(\epsilon), \tag{6}$$

where $t_x(\epsilon) = \sqrt{\frac{\log(1/\epsilon)}{2n_x}}$ depends on a confidence parameter ϵ and the total number of measurement rounds n_x in which the input is ω_x. The confidence parameter corresponds to the probability that Eq. (6) is not satisfied. In our analysis, we choose $\epsilon = 10^{-9}$ (see Supplement 1 for details).

An implementation of the MDI RNG protocol with four-dimensional quantum states involves the state preparation device that can randomly prepare five different states. Four of them, $\{|\omega_x\rangle\}_{x=0}^3$, are orthogonal to each other, and the fifth, $|\omega_4\rangle$, is mutually unbiased with respect to the first four, so that $|\langle\omega_x|\omega_4\rangle|^2 = 1/4 \ \forall\, x = 0, \ldots, 3$. The measuring device is set to measure in the basis spanned by $\{|\omega_x\rangle\}_{x=0}^3$, so that the measurement outputs are uniformly random whenever the state $|\omega_4\rangle$ is measured. The min-entropy Eq. (5) for this ideal implementation gives $H_{\min}(x=4) = 2$, showing that two bits of randomness per round can be generated.

5. MEASUREMENT-DEVICE-INDEPENDENT RNG: IMPLEMENTATION

As previously explained, our source consists of an attenuated pulsed laser that produces weak coherent states. The probability of emitting j photons per pulse is characterized by the mean photon number, μ, such that $p(j) = e^{-\mu}\mu^j/j!$. We consider states with average mean photon numbers of $\mu = 0.2$ and $\mu = 0.4$, while recording the single, double, and triple coincidence counts between the four detectors D_i. Typically, for the experiment working with $\mu = 0.4$, we observe $\sim 50000 \pm 225$ single counts per second, $\sim 90 \pm 9$ double coincidences, and only 1 ± 1 triple coincidence count. For $\mu = 0.2$, we have not observed any triple coincidences. Thus, in our randomness analysis, we consider

a multi-photon Hilbert space truncated up to two photons. Moreover, we adopt the fair sampling assumption and post-select on having at least one photon detected. Then, the set of input states has the following form:

$$\rho_x = p(1)|\omega_x\rangle\langle\omega_x| + p(2)|\phi_x^{(2)}\rangle\langle\phi_x^{(2)}|, \tag{7}$$

where $p(1) + p(2) = 1$, $|\omega_{x=0}\rangle = |0\rangle, \ldots, |\omega_{x=3}\rangle = |3\rangle$ are the states corresponding to one photon traveling in each mode (labeled by x), $|\omega_4\rangle = (|0\rangle - |1\rangle + |2\rangle + |3\rangle)/2$ is the mutually unbiased state, and $|\phi_x^{(2)}\rangle$ refers to states where two photons are generated in a single pulse. These states are given in Supplement 1. Notice that in our experiment, we observe 10 measurement outcomes: four single clicks corresponding to photon detection at one of the four detectors D_i $(i = 0, \ldots, 3)$, and six coincidence detections between detectors D_i and D_j with $i \neq j$. The statistics of all these events are taken into consideration in the randomness estimation.

The experiment operates at the repetition rate of 2 MHz. Over the course of one integration sample of 0.1 s, 90% of the rounds are randomly chosen by FPGA1 to send ρ_4. The other 10% of samples are uniformly chosen between $\rho_{x=0}, \ldots, \rho_{x=3}$. In this way, we prioritize the generation of random bits, while still having enough statistics to certify the amount of private randomness created. We continuously verify that the protocol is working properly through the average success probability of identifying the states ω_x (i.e., $\bar{p} = \frac{1}{4}\sum_{x=0}^{3} p(x|\rho_x)$. If $\bar{p} > 0.992$, then the random bit sequence is recorded. Otherwise, the control system starts a realignment procedure automatically. This threshold value has been chosen to maintain the system producing more than one bit of randomness per experimental round, the maximum that a RNG protocol based on dichotomic outcomes (and post-processing of it) would achieve.

Figure 5 shows a fragment of the recorded data while the random number generator is operating with $\mu = 0.4$. The points in Fig. 5(a) represent the single-photon detection rate in kHz. There are discontinuities that arise from the fact that only the results when $\bar{p} > 0.992$ are displayed. E_i with $i = \{1, 2, \ldots, 13\}$ represent small zones, between which the realignment procedure occurs. The system is continuously realigning itself, but sometimes it does not quickly achieve a visibility higher than the given threshold. The experiment ran over a total of 103.7 h. The corresponding average success probabilities per zone E_i are shown in Fig. 5(b). The total average success probability is $\bar{p}_t = 0.9946 \pm 0.0001$. From all the recorded data, the minimum entropy is estimated. The experimental $H_{\min}^{\exp}$ is bounded by $1.133 < H_{\min}^{\exp} < 1.232$, with its maximum value obtained at zone E_4 [see Fig. 5(c)]. The average value is $\bar{H}_{\min}^{\exp} = 1.153 \pm 0.007$, which implies that the generator works with an average private random bit key rate of $\sim 57650 \pm 350$ bits/s. With additional improvements in temporal width of the pulses, and faster clock rates of the detectors, it should be possible to increase this by at least two orders of magnitude. For the case with $\mu = 0.2$, we obtain similar results. In this case, $H_{\min}^{\exp}$ is bounded by $1.134 < H_{\min}^{\exp} < 1.178$, with the average value given by $\bar{H}_{\min}^{\exp} = 1.156 \pm 0.003$. Thus, we have demonstrated the robustness of the MDI RNG method while being implemented with weak coherent states. Importantly, these results show that the random number generator has been able to exploit the advantages provided by HD quantum systems, since it always produces a min-entropy greater than one bit per experimental round. We notice that a theoretical upper bound to the private random bit key rate is given by the min-entropy of the most likely measurement outcome, which corresponds to an attack where an eavesdropper always bets on this outcome. In our case, this corresponds to $H_{\min}^{\text{the}} \approx 2.03$ for $\mu = 0.4$ and $H_{\min}^{\text{the}} \approx 2.02$ for $\mu = 0.2$ (see Supplement 1).

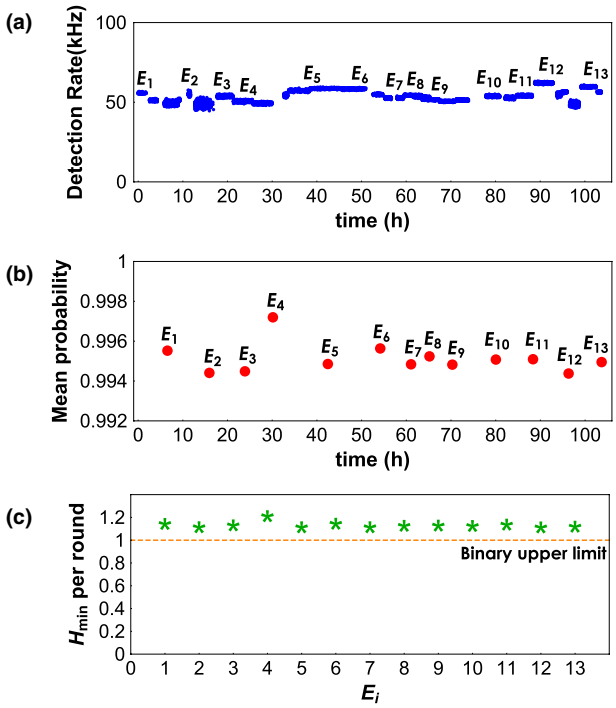

Fig. 5. Fragment of the data recorded over time. (a) Single count detection rate considering only the selected samples (please see text for details). E_i with $i = \{1, 2, \ldots, 13\}$ represent small zones, mostly between or with long realignment procedures. (b) Observed average success probability for each zone E_i. Error bars lie within the experimental point representation. (c) Average obtained randomness per experimental round for each zone E_i. Error bars lie within the star symbols. The dashed line represents the theoretical upper bound allowed for binary RNG protocols.

6. CONCLUSION

We have reported on the production and characterization of high-quality $N \times N$ MBS devices built directly within a MCF. This is an important step towards the construction of universal photonic QI processing circuits based entirely on the new MCF platform, which will take advantage of the high phase stability provided by these fibers. We use a 4×4 device to experimentally show that a programmable quantum circuit for efficient four-dimensional QI processing can be built using MCF-based technology. Since it is constructed with commercially available components, it can be easily integrated with telecom fiber networks. To demonstrate the versatility and advantages of this circuit, we have demonstrated a MDI quantum random number generator using four-dimensional photonic states, which yield a maximum of 1.23 private certified random bits generated per experimental round, surpassing the one-bit limit of binary protocols. To achieve these results, we employ a theoretical approach that allows for the evaluation of available private randomness using semi-definite programming and taking into account finite statistics of events. Furthermore, our programmable circuit operates at 2 MHz repetition rate (scalable to several GHz), generating about 6×10^4 random bits/s. With scalability

taken into account, our results compare favorably in terms of generation rate to other state-of-the-art quantum certified randomness generators, while providing better scalability to even higher dimensions. These results are critical in demonstrating a new robust and versatile HD-QI processing platform for implementing universal programmable optical circuits. In this regard, note that MCF BS technology has very recently been used to implement a quantum computational circuit based on a quantum N-switch [91].

Funding. Fondo Nacional de Desarrollo Científico y Tecnológico (1200859, 1200266, 1190933, 3170596, 3170400); Millennium Institute for Research in Optics; Ramón y Cajal fellowship; Spanish MINECO (QIBEQI FIS2016-80773-P, Severo Ochoa SEV-2015-0522); AXA Chair in Quantum Information Science, Generalitat de Catalunya (SGR875, CERCA Programme); Fundació Privada Cellex; ERC CoG QITBOX; Royal Society; COST project (CA16218, NANOCOHYBRI); Brazilian grants CNPq (304196/2018-5, FAPERJ E-26/010.002997/2014, E-26/202.7890/2017); INCT-Informação Quântica; Ceniit Linköping University; Vetenskapsrådet (VR 2017-04470).

Disclosures. The authors declare no conflicts of interest.

See Supplement 1 for supporting content.

REFERENCES

1. D. J. Richardson, J. M. Fini, and L. E. Nelson, "Space-division multiplexing in optical fibres," Nat. Photonics **7**, 354–362 (2013).
2. S. Iano, T. Sato, S. Sentsui, T. Kuroha, and Y. Nishimura, "Multicore optical fiber," in *Optical Fiber Communication Conference (OFC)*, OSA Technical Digest (Optical Society of America, 1979), paper WB1.
3. K. Saitoh and S. Matsuo, "Multicore fiber technology," J. Lightwave Technol. **34**, 55 (2016).
4. P. Sillard, M. Bigot-Astruc, and D. Molin, "Few-mode fibers for mode-division-multiplexed systems," J. Lightwave Technol. **32**, 2824 (2014).
5. N. Bozinovic, Y. Yue, Y. Ren, M. Tur, P. Kristensen, H. Huang, A. E. Willner, and S. Ramachandran, "Terabit-scale orbital angular momentum mode division multiplexing in fibers," Science **340**, 1545–1548 (2013).
6. C. Brunet, B. Ung, L. Wang, Y. Messaddeq, S. LaRochelle, and L. A. Rusch, "Design of a family of ring-core fibers for OAM transmission studies," Opt. Express **23**, 10553 (2015).
7. P. Gregg, P. Kristensen, and S. Ramachandran, "Conservation of orbital angular momentum in air-core optical fibers," Optica **2**, 267–270 (2015).
8. L. Zhu, G. Zhu, A. Wang, L. Wang, J. Ai, S. Chen, C. Du, J. Liu, S. Yu, and J. Wang, "18 km low-crosstalk OAM +WDM transmission with 224 individual channels enabled by a ring-core fiber with large high-order mode group separation," Opt. Lett. **43**, 1890–1893 (2018).
9. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
10. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**, 595–604 (2014).
11. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**, 16025 (2016).
12. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Quantum cryptography with realistic devices," arXiv:1903.09051 (2019).
13. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," arXiv:1906.01645v1 [quant-ph] (2019).
14. G. B. Xavier and G. Lima, "Quantum information processing with space-division multiplexing optical fibres," Commun. Phys. **3**, 9 (2020).
15. J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution over multicore fiber," Opt. Express **24**, 8081–8087 (2016).
16. R. Lin, A. Udalcovs, O. Ozolins, X. Pang, L. Gan, L. Shen, M. Tang, S. Fu, S. Popov, C. Yang, W. Tong, D. Liu, T. Ferreira da Silva, G. B. Xavier, and J. Chen, "Telecom compatibility validation of quantum key distribution co-existing with 112 Gbps/λ/core data transmission in non-trench and trench-assistant multicore fibers," in *European Conference on Optical Communications (ECOC)* (2018) paper We1A.3.
17. E. Hugues-Salas, R. Wang, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Co-existence of 9.6 Tb/s classical channels and a quantum key distribution (QKD) channel over a 7-core multicore optical fibre," in *IEEE British and Irish Conference on Optics and Photonics (BICOP)* (IEEE, 2019).
18. C. Cai, Y. Sun, Y. Zhang, P. Zhang, J. Niu, and Y. Ji, "Experimental wavelength-space division multiplexing of quantum key distribution with classical optical communication over multicore fiber," Opt. Express **27**, 5125–5135 (2019).
19. T. A. Eriksson, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Takeoka, Y. Awaji, M. Sasaki, and N. Wada, "Inter-core crosstalk impact of classical channels on CV-QKD in multicore fiber transmission," in *Optical Fiber Communication Conference (OFC)*, OSA Technical Digest (Optical Society of America, 2019), paper Th1J.1.
20. G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, and G. Lima, "High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers," Phys. Rev. A **96**, 022317 (2017).
21. 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).
22. B. Da Lio, D. Bacco, D. Cozzolino, N. Biagi, T. N. Arge, E. Larsen, K. Rottwitt, Y. Ding, A. Zavatta, and L. K. Oxenløwe, "Stable transmission of high-dimensional quantum states over a 2-km multicore fiber," IEEE J. Sel. Top. Quantum Electron. **26**, 6400108 (2020).
23. H. J. Lee, S.-K. Choi, and H. S. Park, "Experimental demonstration of four-dimensional photonic spatial entanglement between multi-core optical fibres," Sci. Rep. **7**, 4302 (2017).
24. H. J. Lee and H. S. Park, "Generation and measurement of arbitrary four-dimensional spatial entanglement between photons in multicore fibers," Photon. Res. **7**, 19–27 (2019).
25. L. Cui, J. Su, X. Li, and Z. Y. Ou, "Distribution of entangled photon pairs over few-mode fibers," Sci. Rep. **7**, 14954 (2017).
26. A. Sit, R. Fickler, F. Alsaiari, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, and E. Karim, "Quantum cryptography with structured photons through a vortex fiber," Opt. Lett. **43**, 4108–4111 (2018).
27. H. Cao, S.-C. Gao, C. Zhang, J. Wang, D.-Y. He, B.-H. Liu, Z.-W. Zhou, G.-X. Zhu, Y.-J. Chen, Z.-H. Li, S.-Y. Yu, Y.-F. Huang, C.-F. Li, and G.-C. Guo, "Distribution of high- dimensional orbital angular momentum entanglement at telecom wavelength over 1km OAM fiber," Optica **7**, 232 (2020).
28. D. Cozzolino, E. Polino, M. Valeri, G. Carvacho, D. Bacco, N. Spagnolo, L. K. Oxenløwe, and F. Sciarrino, "Air-core fiber distribution of hybrid vector vortex-polarization entangled states," Adv. Photon. **1**, 1 (2019).
29. J. Liu, I. Nape, Q. Wang, A. Vallés, J. Wang, and A. Forbes, "Multi-dimensional entanglement transport through single-mode fibre," Sci. Adv. **6**, eaay0837 (2020).
30. N. H. Valencia, S. Goel, W. McCutcheon, H. Defienne, and M. Malik, "Unscrambling entanglement through a complex medium," arXiv:1910.04490 (2019).
31. 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).
32. Z. Zhao, M. Tang, S. Fu, S. Liu, H. Wei, Y. Cheng, W. Tong, P. P. Shum, and D. Liu, "All-solid multi-core fiber-based multipath Mach-Zehnder interferometer for temperature sensing," Appl. Phys. B **112**, 491–497 (2013).
33. J. E. Antonio-Lopez, Z. S. Eznaveh, P. LiKamWa, A. Schülzgen, and R. Amezcua-Correa, "Multicore fiber sensor for high-temperature applications up to 1000 C," Opt. Lett. **39**, 4309–4312 (2014).

34. C. Guan, X. Zhong, G. Mao, T. Yuan, J. Yang, and L. Yuan, "In-line Mach-Zehnder interferometric sensor based on linear five-core fiber," IEEE Photon. Technol. Lett. **27**, 635–638 (2015).
35. S. Zhou, B. Huang, and X. Shu, "A multi-core fiber based interferometer for high temperature sensing," Meas. Sci. Technol. **28**, 045107 (2017).
36. L. Gan, R. Wang, D. Liu, L. Duan, S. Liu, S. Fu, B. Li, Z. Feng, H. Wei, W. Tong, P. Shum, and M. Tang, "Spatial-division multiplexed Mach-Zehnder interferometers in heterogeneous multicore fiber for multiparameter measurement," IEEE Photon. J. **8**, 1 (2016).
37. E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," Nature **409**, 46–52 (2001).
38. L. Neves, G. Lima, J. G. Aguirre Gómez, C. H. Monken, C. Saavedra, and S. Pádua, "Generation of entangled states of qudits using twin photons," Phys. Rev. Lett. **94**, 100501 (2005).
39. M. N. O'Sullivan-Hale, I. Ali Khan, R. W. Boyd, and J. C. Howell, "Pixel entanglement: experimental realization of optically entangled d = 3 and d = 6 qudits," Phys. Rev. Lett. **94**, 220501 (2005).
40. J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, "Generation of hyperentangled photon pairs," Phys. Rev. Lett. **95**, 260501 (2005).
41. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," New J. Phys. **8**, 75 (2006).
42. S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro, Quantum key distribution with higher-order alphabets using spatially encoded qudits, Phys. Rev. Lett. **96**, 090501 (2006).
43. A. Rossi, G. Vallone, A. Chiuri, F. De Martini, and P. Mataloni, "Multipath entanglement of two photons," Phys. Rev. Lett. **102**, 153902 (2009).
44. W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Guhne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Experimental demonstration of a hyper-entangled ten-qubit Schrödinger cat state, Nat. Phys. **6**, 331–335 (2010).
45. A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson, "Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities," Nat. Phys. **7**, 677–680 (2011).
46. S. Etcheverry, G. Cañas, E. S. Gómez, 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).
47. P.-L. De Assis, M. A. D. Carvalho, L. P. Berruezo, J. Ferraz, and S. Pádua, "Generation of two pairs of qudits using four photons and a single degree of freedom," Opt. Express **24**, 30149–30163 (2016).
48. M. Malik, M. Erhard, M. Huber, M. Krenn, R. Fickler, and A. Zeilinger, "Multi-photon entanglement in high dimensions," Nat. Photonics **10**, 248–252 (2016).
49. J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, "Multidimensional quantum entanglement with large-scale integrated optics," Science **360**, 285–291 (2018).
50. E. A. Aguilar, M. Farkas, D. Martínez, M. Alvarado, J. Cariñe, G. B. Xavier, J. F. Barra, G. Cañas, M. Pawłowski, and G. Lima, "Certifying an irreducible 1024-dimensional photonic state using refined dimension witnesses," Phys. Rev. Lett. **120**, 230503 (2018).
51. D. Martínez, A. Tavakoli, M. Casanova, G. Cañas, B. Marques, and G. Lima, "High-dimensional quantum communication complexity beyond strategies based on Bell's theorem," Phys. Rev. Lett. **121**, 150504 (2018).
52. G. Weihs, M. Reck, H. Weinfurter, and A. Zeilinger, "All-fiber three-path Mach-Zehnder interferometer," Opt. Lett. **21**, 302–304 (1996).
53. A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, "Silica-on-silicon waveguide quantum circuits," Science **320**, 646–649 (2008).
54. J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing, "Universal linear optics," Science **349**, 711–716 (2015).
55. N. Spagnolo, C. Vitelli, L. Aparo, P. Mataloni, F. Sciarrino, A. Crespi, R. Ramponi, and R. Osellame, "Three-photon bosonic coalescence in an integrated tritter," Nat. Commun. **4**, 1606 (2013).
56. M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," Phys. Rev. Lett. **73**, 58–61 (1994).
57. M. Zukowski, A. Zeilinger, and M. Horne, "Realizable higher-dimensional two-particle entanglements via multiport beam splitters," Phys. Rev. A **55**, 2564–2579 (1997).
58. W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, "Optimal design for universal multiport interferometers," Optica **3**, 1460–1465 (2016).
59. F. Flamini, N. Spagnolo, N. Viggianiello, A. Crespi, R. Osellame, and F. Sciarrino, "Benchmarking integrated linear-optical architectures for quantum information processing," Sci. Rep. **7**, 15133 (2017).
60. M. Y. Saygin, I. V. Kondratyev, I. V. Dyakonov, S. A. Mironov, S. S. Straupe, and S. P. Kulik, "Robust architecture for programmable universal unitaries," Phys. Rev. Lett. **124**, 010501 (2020).
61. L. Pereira, A. Rojas, G. Cañas, G. Lima, A. Delgado, and A. Cabello, "Universal multi-port interferometers with minimal optical depth," arXiv:2002.01371 (2020).
62. A. Acín and L. Masanes, "Certified randomness in quantum physics," Nature **540**, 213–219 (2016).
63. S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).
64. N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," Rev. Mod. Phys. **86**, 419 (2014).
65. Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, "High-speed device-independent quantum random number generation without a detection loophole," Phys. Rev. Lett. **120**, 010503 (2018).
66. M. Pawłowski and N. Brunner, "Semi-device-independent security of one-way quantum key distribution," Phys. Rev. A **84**, 010302 (2011).
67. G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, "Experimental quantum randomness generation invulnerable to the detection loophole," arXiv:1410.3443v2 (2014).
68. T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, "Self-testing quantum random number generator," Phys. Rev. Lett. **114**, 150501 (2015).
69. J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, "Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination," Phys. Rev. Appl. **7**, 054018 (2017).
70. T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, "Semi-device-independent framework based on natural physical assumptions," Quantum **1**, 33 (2017).
71. D. Rusca, T. van Himbeeck, A. Martin, J. Bohr Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, "Practical self-testing quantum random number generator based on an energy bound," arXiv:1904.04819 [quant-ph].
72. I. Supic, P. Skrzypczyk, and D. Cavalcanti, "Measurement-device independent entanglement and randomness estimation in quantum networks," Phys. Rev. A **95**, 042340 (2017).
73. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using -level systems," Phys. Rev. Lett. **88**, 127902 (2002).
74. D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, and A. Zeilinger, "Violations of local realism by two entangled N-dimensional systems are stronger than for two qubits," Phys. Rev. Lett. **85**, 4418–4421 (2000).
75. S. Pirandola, B. R. Bardhan, C. Weedbrook, and S. Lloyd, "Advances in photonic quantum sensing," Nat. Photonics **12**, 724–733 (2018).
76. T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," Nature **464**, 45–53 (2010).
77. M. Araújo, F. Costa, and C. Brukner, "Computational advantage from quantum-controlled ordering of gates," Phys. Rev. Lett. **113**, 250402 (2014).
78. S. Rahimi-Keshari, M. A. Broome, R. Fickler, A. Fedrizzi, T. C. Ralph, and A. G. White, "Direct characterization of linear-optical networks," Opt. Express **21**, 13450–13458 (2013).
79. C. H. Baldwin, A. Kalev, and I. H. Deutsch, "Quantum process tomography of unitary and near-unitary maps," Phys. Rev. A **90**, 012110 (2014).
80. A. Acín, "Statistical distinguishability between unitary operations," Phys. Rev. Lett. **87**, 177901 (2001).
81. K. Watanabe, T. Saito, K. Imamura, and M. Shiino, "Development of fiber bundle type fan-out for multicore fiber," in *17th Opto Electronics and Communications Conference* (2012).

82. Y. Tottori, T. Kobayashi, and M. Watanabe, "Low loss optical connection module for seven-core multicore fiber and seven single-mode fibers," IEEE Photon. Technol. Lett. **24**, 1926–1928 (2012).
83. P. Walborn, M. O. Terra Cunha, S. Pádua, and C. H. Monken, "Double-slit quantum eraser," Phys. Rev. A **65**, 033818 (2002).
84. F. A. T. Ruiz, G. Lima, A. Delgado, S. Pádua, and C. Saavedra, "Decoherence in a double-slit quantum eraser," Phys. Rev. A **81**, 042104 (2010).
85. P. Bhatnagar and R. K. Nema, "Maximum power point tracking control techniques: state-of-the-art in photovoltaic applications," Renew. Sustain. Energy Rev. **23**, 224–241 (2013).
86. M. Malmström, O. Tarasenko, W. Margulis, and F. Laurell, "All-fiber nanosecond gating for time-resolved spectral analysis," IEEE Photon. Technol. Lett. **28**, 829–832 (2016).
87. W. Margulis, (personal communication, 2019).
88. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
89. S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University, 2004).
90. W. Hoeffding, "Probability inequalities for sums of bounded random variables," J. Am. Stat. Assoc. **58**, 13–30 (1963).
91. M. M. Taddei, J. Cariñe, D. Martínez, T. García, N. Guerrero, A. A. Abbott, M. Araújo, C. Branciard, E. S. Gómez, S. P. Walborn, L. Aolita, and G. Lima, "Experimental computational advantage from superposition of multiple temporal orders of quantum gates," arXiv:2002.07817 (2020).