UNIVERSIDAD DE CONCEPCIÓN

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

High-dimensional measurement device-independent quantum random number generation protocol

Generación aleatoria dispositivo independiente en alta dimensión

Nayda Sofía Guerrero Pulgar

Tesis presentada a la Facultad de Ciencias Físicas y Matemáticas
de la Universidad de Concepción para optar al grado académico de
Magíster en Ciencias con mención en Física

Profesor guía: Dr. Gustavo Moreira Lima.

Marzo 2025

Concepción, Chile

Agradecimientos

Es dificil expresar en palabras mi gratitud cuando ha pasado tanto tiempo desde el inicio de este trabajo. Muchas personas han contribuido, en pequeña o gran medida, a que esta etapa llegue a su fin.

Es probable que jamás lean esto, pero debo agradecer a mis padres, quienes, a pesar de no entender qué hago — o tal vez preferir que hubiera escogido otro rumbo —, nunca han dejado de apoyarme en el camino académico.

A mis compañeros de laboratorio: Tania, Ítalo, Santiago y Daniel, por sus contínuas enseñanzas. A mis profesores, en particular a Gustavo Lima, por su infinita paciencia y por nunca dejar de confiar en este trabajo.

Quiero agradecer a los exiliados del sexto piso, quienes me alentaron (u obligaron, ya es irrelevante ahora) a iniciar un postgrado en Información Cuántica. Luciano, Jean, Gerald, Nicole, Sebastián, y todos aquellos que pasaron en algún momento por las oficinas 604 y 606: cada vez que escucharon mis anécdotas de laboratorio, me explicaron algo que no entendía o compartieron conmigo nuestras tardes de Catán, ayudaron a que este momento llegara. Sin sus retos y sin papitas esto no habría ocurrido. No importa la distancia geográfica, el compañerismo permanece. Los quiero.

A Ernesto y Patrick, mis amigos de Ingeniería Matemática. Desde el 2011 no nos hemos separado, y nunca han perdido la fe en mi, incluso cuando yo la perdí.

Antes que todos los anteriores llegó mi mejor amigo. Creo que cuando íbamos a congresos de Astronomía o viajamos a Tololo, nunca imaginamos que terminaríamos haciendo cosas

tan distintas. Gustavo, has sido testigo de todas mis buenas decisiones y cómplice en las malas, y espero que siga siendo así.

El último en llegar fuiste tú, Felipe, y no habría completado esto sin tu permanente apoyo y cariño. Me incentivas a hacer las cosas de una manera distinta y a buscar una paz y un bienestar personal al que no estoy acostumbrada. Tratas constantemente de hacerme una mejor persona. Esto jamás se habría escrito sin ti, gracias por insistir.

Table of contents

List of Figures

Resumen

Los protocolos de información cuántica se ven favorecidos por el uso de tecnología usada en telecomunicaciones. En particular, las fibras ópticas y el desarrollo de fibras ópticas multinúcleos permite aumentar los canales de transmisión, lo que conlleva un mayor envío de información, con posibles aplicaciones en criptografía cuántica y comunicación cuántica, entre otros.

Con estas fibras se pueden fabricar divisores de haz multinúcleos de alta calidad basados en un esquema de manipulación de los núcleos.

Mediante el uso de MBS de 4×4, generamos sistemas cuánticos de cuatro dimensiones y llevamos a cabo una tarea de generación de números aleatorios independiente del dispositivo de medición, utilizando un interferómetro programable de cuatro brazos que opera a una frecuencia de repetición de 2 MHz.

Gracias a las altas visibilidades obtenidas, superamos el límite de un bit de los protocolos binarios.

En conjunto, este estudio allana el camino hacia sistemas cuánticos de alta dimensión eficientes y escalables aprovechando la tecnología de fibra óptica multinúcleo, lo que supone un avance significativo en el campo del procesamiento cuántico de la información.

Abstract

Quantum information protocols benefit from the use of technology commonly employed in telecommunications. In particular, optical fibers and the advancement of multi-core optical fiber technology enable an increase in transmission channels, thereby allowing for a higher data transfer rate with potential applications in quantum cryptography, quantum networks, and quantum-enhanced sensing.

High-quality multi-core beam splitters based on a core manipulation scheme can be fabricated with these fibers.

Using 4×4 multi-core beam splitters we generate four-dimensional quantum systems and implement a measurement-device-independent random number generation task using 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.

Overall, this study paves the way for efficient and scalable high-dimensional quantum systems by leveraging multi-core optical fiber technology, significantly advancing the field of quantum information processing.

Chapter 1

Introduction

The utilization of quantum information technologies provides unconditionally secure communication models [1, 2]. These models benefit from the incorporation of devices that are commonly employed in classical telecommunications. Thus, high-dimensional quantum systems offer significant advantages over two-dimensional systems. To illustrate, the implementation of quantum communication protocols in high-dimensional systems can be accomplished in a manner that is more secure, efficient, and resistant to noise [3–5]. This enhancement in protocols enables greater violations of Bell's inequalities [6] and facilitates improvements in complex computational and quantum communication tasks [7, 8]. These systems enable the precise and regulated preparation and measurement of different quantum states in a variety of bases.

In this thesis, we propose the construction of a programmable quantum circuit suitable for a variety of experimental applications. Using high-dimensional beam splitters, we construct a 4-path Mach-Zehnder interferometer, which is optimal for the efficient processing of single or entangled high-dimensional quantum systems (qudits). Through this interferometer, we generate qudits with dimension 4 and implement random generation independent of the measurement device.

With this circuit, we achieved average visibilities greater than 99.4% and certified the generation of 1.23 random bits per round. These results demonstrate that the use of qudits is crucial for random number generation, as increasing the dimensionality is one of the few strategies that enables the generation of a larger amount of randomness per measurement. Furthermore, our scheme delivers a random bit rate of $60,000$ bits/s, reaching the state-of-the-art in experiments manipulating high-dimensional states.

In chapter 2, a concise overview of quantum mechanics and quantum information is presented. Chapter 3 details the experimental framework within which the quantum information processing scheme is developed. In chapter 4, the design and implementation of the circuit are presented. In chapter 5, the results of the experiment are reported. Two appendices are included, featuring experiments that utilize the proposed scheme, thereby demonstrating its versatility.

The results presented in chapters 4 and 5 have been published in the paper *Multi-core fiber integrated multi-port beam splitters for quantum information processing* [9].

Chapter 2

Foundational concepts of quantum information

In this chapter, we will review some fundamental mathematical concepts necessary for understanding the proposal presented in this thesis [10].

2.1 Fundaments of Quantum Mechanics

2.1.1 Hilbert space

A Hilbert space, denoted by the symbol $\mathcal{H}$, is defined as a linear vector space over the complex numbers, denoted by $\mathbb{C}$. It is closed under both addition $(+)$ and the scalar product $(\cdot)$.

$$+ : \mathcal{H} \times \mathcal{H} \longrightarrow \mathcal{H}, \tag{2.1}$$

$$\cdot : \mathbb{C} \times \mathcal{H} \longrightarrow \mathcal{H}. \tag{2.2}$$

A vector in $\mathcal{H}$ represents the quantum state of a physical system and is denoted using the Dirac notation $|\psi\rangle$. The inner product of the vectors $|a\rangle$ with $|b\rangle$ is written $\langle a|b\rangle$.

Two vectors are said orthogonal if

$$\langle a|b\rangle = 0. \tag{2.3}$$

A collection of linearly independent vectors $\{|e_n\rangle\}_{n\in\mathbb{N}}$ form a basis of $\mathcal{H}$ provided any $|a\rangle$ in $\mathcal{H}$ can be written as a linear combination:

$$|a\rangle = \sum_{n\in\mathcal{N}} \alpha_n |e_n\rangle \ \ , \forall\, |a\rangle \in \mathcal{H}. \tag{2.4}$$

The number d of vectors forming the basis is the dimension of $\mathcal{H}$, written as $dim(\mathcal{H})$, and does not depend on the choice of basis.

A basis is orthonormal if

$$\langle e_n|e_m\rangle = \delta_{nm}, \tag{2.5}$$

where δ_{nm} is the Kronecker delta defined by

$$\delta_{nm} = \begin{cases} 1 & , n = m. \\ 0 & , n \neq m. \end{cases} \tag{2.6}$$

If we consider the Gram-Schmidt orthogonalization process we can obtain an orthonormal basis $\{|v_n\rangle\}_{n=1,\ldots,d}$ from an non-orthonormal basis $\{|w_n\rangle\}_{n=1,\ldots,d}$. Thus, any finite Hilbert space has an orthonormal basis. Therefore, the equation (2.4) becomes

$$|a\rangle = \sum_{n=1}^{d} \alpha_n |v_n\rangle , \tag{2.7}$$

where $\alpha_n = \langle v_n|a\rangle$. Besides, it can be written in matrix representation, that is,

$$|a\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_d \end{pmatrix} = \begin{pmatrix} \langle v_1|a\rangle \\ \langle v_2|a\rangle \\ \vdots \\ \langle v_d|a\rangle \end{pmatrix} \in \mathbb{C}^d. \tag{2.8}$$

For any linear operator A, the trace of A is defined be the sum of its diagonal elements,

$$\mathrm{Tr}(A) = \sum_{i=1}^{d} \langle i|A|i\rangle . \tag{2.9}$$

2.1.2 Qubit

In classical computing, the smallest unit of information storage and processing is the bit, which can have two possible values: 0 or 1. A qubit, on the other hand, is a two-dimensional quantum system that represents the minimal unit of information storage in quantum computing. Like a bit, a qubit can assume the values 0 or 1, denoted as $|0\rangle$ and $|1\rangle$, which form a basis for the space $\mathcal{H}$. The quantum state describing a qubit is given by

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.10}$$

where α and β are complex coefficients so $|\alpha|^2+|\beta|^2 = 1$. We can observe that a qubit allows a superposition state between $|0\rangle$ and $|1\rangle$.

The general state of a qubit in dimension 2 is given by

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle\,, \tag{2.11}$$

where θ and φ are coordinates on the Bloch sphere, a graphical representation of quantum states. In general, a d dimensional state is called a qudit.

An alternative approach to describing a quantum system, particularly in scenarios where a comprehensive understanding of the system is unavailable, involves using the density matrix, defined by the equation

$$\rho = \sum_{i=1}^{n} p_i\,|\psi_i\rangle\langle\psi_i|\,, \tag{2.12}$$

where $|\psi_i\rangle$ are the states necessary to describe the system and p_i are their respective probabilities. The matrix density must satisfy the following conditions:

- The trace of ρ is equal to 1. That is, $\mathrm{Tr}(\rho) = 1$.
- ρ is a positive semidefinite operator. That is, $\langle\varphi|\rho|\varphi\rangle \geq 0$, with φ an arbitrary vector.

If there exists a vector $|\psi\rangle$ such that $\rho = |\psi\rangle\langle\psi|$, then the state is pure. In any other case, we say that the state is mixed. A state ρ can be determined as pure or mixed by evaluating the purity $\mathrm{Tr}(\rho^2)$. A state ρ is pure if and only if $\mathrm{Tr}(\rho^2) = 1$, located on the surface of the

Bloch sphere. The mixed states have $\mathrm{Tr}(\rho^2) < 1$ and are located in the interior of the Bloch sphere.

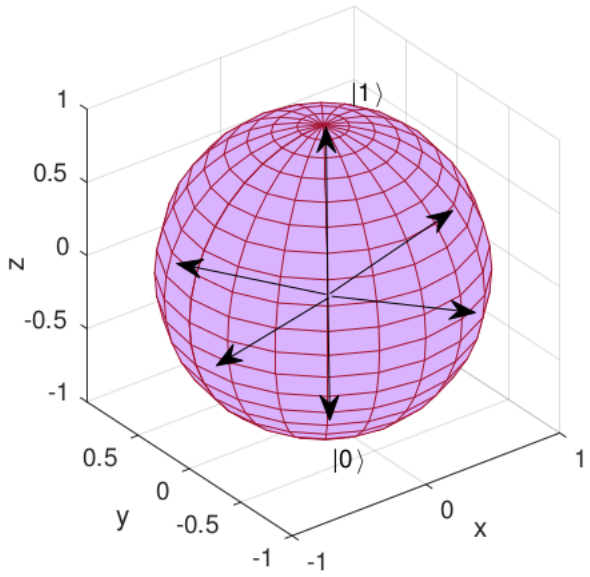

Figure 2.1: Bloch sphere, a graphical representation of the qubits. Each point represents a different density matrix.

2.1.3 Measurement

A major difference between classical and quantum physics is the measurement process by which information about a system is obtained. In classical physics, the properties of a system do not change after a measurement is made. In contrast, in quantum physics, measurements can yield different results, which disturb the state of the system and preclude the possibility of knowing other properties. The measurement postulate explains this and describes what happens at the moment of measurement.

Postulate: *Quantum measurements are described by a set of operators* $\{M_m\}_{m=1,\ldots,n}$*, where* m *refers to the results of the measurement that may occur in a experiment. If the state of a certain physical system immediately before a measurement is* $|\psi\rangle$*, then the probability*

that result m occurs is

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle\,, \tag{2.13}$$

where $M_m^\dagger$ is the transposed conjugate of M_m and the state of the system immediately after the measurement is

$$|\psi^m\rangle = \frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{2.14}$$

Expressed as a function of the density matrix ρ, the probability of an outcome m is given by

$$\begin{aligned} p(m) &= \sum_{i=1}^{n'} p(m|i)p_i && (2.15)\\ &= \sum_{i=1}^{n'} \langle\psi_i|\, M_m^\dagger M_m\,|\psi_i\rangle\, p_i && (2.16)\\ &= \sum_{i=1}^{n'} \mathrm{Tr}\big(M_m^\dagger M_m\,|\psi_i\rangle\langle\psi_i|\big)p_i && (2.17)\\ &= \mathrm{Tr}\left(M_m^\dagger M_m \sum_{i=1}^{n'} p_i\,|\psi_i\rangle\langle\psi_i|\right) && (2.18)\\ &= \mathrm{Tr}\big(M_m^\dagger M_m\rho\big), && (2.19) \end{aligned}$$

where $p(m|i)$ is the conditional probability of m if the initial state was $|\psi_i\rangle$. Then, the states of the ensemble after the measurement are

$$|\psi_i^m\rangle = \frac{M_m\,|\psi_i\rangle}{\sqrt{\langle\psi_i|\, M_m^\dagger M_m\,|\psi_i\rangle}}. \tag{2.20}$$

Then, the density matrix after the measurement is

$$\rho^m = \frac{M_m\rho M_m^\dagger}{\mathrm{Tr}\Big(M_m^\dagger M_m\rho\Big)}. \tag{2.21}$$

The measurement operators $\{M_m\}_{m=1,\ldots,n}$ satisfy the completeness relation

$$\sum_{m=1}^{n} M_m^\dagger M_m = \mathbb{I}. \tag{2.22}$$

The simplest type of measurement is the projective measurement. A set of d projective measurements is associated to a hermitian operator called an observable. An observable O has a spectral decomposition

$$O = \sum_{m=1}^{d} \lambda_m \left|\phi_m\right\rangle\!\left\langle\phi_m\right|, \tag{2.23}$$

where λ_m and $|\phi_m\rangle$ are its respective eigenvalues and eigenvectors. Then, because the projectors $\tau_m = |\phi_m\rangle\langle\phi_m|$ are hermitian, the probability to obtain an outcome m measurement the state $|\psi\rangle$ is

$$p(m) = \mathrm{Tr}\left(\tau_m^\dagger \tau_m \rho\right) = \mathrm{Tr}(\tau_m \rho) = \langle\phi_m|\rho|\phi_m\rangle, \tag{2.24}$$

and the density matrix after the measurement is

$$\rho^m = \frac{\tau_m \rho \tau_m^\dagger}{\mathrm{Tr}\left(\tau_m^\dagger \tau_m \rho\right)} = \frac{\langle\phi_m|\rho|\phi_m\rangle \left|\phi_m\right\rangle\!\left\langle\phi_m\right|}{\langle\phi_m|\rho|\phi_m\rangle} = \left|\phi_m\right\rangle\!\left\langle\phi_m\right|. \tag{2.25}$$

The most general measurement on a density matrix is the Positive Operators Values Measure or POVM. The POVMs are used when the post-measurement state is unimportant and the probabilities are the main interest. A POVM is a set $\{A_m\}_{m=1,\ldots,n}$, such that the operator A_m are positive and satisfy the relation $\sum_{m=1}^{n} A_m = \mathbb{I}$. We can consider $M_m = \sqrt{A_m}$ such that $A_m = M_m^\dagger M_m$. Then we see that the POVM satisfies the equation (2.22) $\sum_{m=1}^{n} M_m^\dagger M_m = \sum_{m=1}^{n} A_m = \mathbb{I}$, and therefore the set $\{M_m\}_{m=1,\ldots,n}$ describe a measurement with POVM $\{A_m\}_{m=1,\ldots,n}$. The probability of outcome m is given by

$$p(m) = \mathrm{Tr}(A_m \rho). \tag{2.26}$$

2.2 Random numbers

The generation of random numbers is arguably one of the most practical applications of Quantum Mechanics, with uses in fields such as cryptography, communications, gambling, and numerical simulations of physical or biological systems, among others [11]. Random numbers are produced by a device that generates bits that are accessible to the user. The

process of generating random numbers, defined as numbers produced through a completely unpredictable process, should not depend on the specific device used.

Randomness must be generated by devices that replicate an intrinsically random process. Some generators rely on pseudorandom algorithms, which expand a random base string known as the seed. This seed serves as the input for a process that generates a long sequence of bits, adhering to the statistical properties of a uniform distribution. These pseudorandom number generators (PRNGs) are typically faster than other random number generation methods, and their results are reproducible. For example, knowing the seed allows for the exact replication of a simulation. However, this can be problematic for certain applications where the numbers need to be unpredictable.

Other methods rely on physical processes that are difficult to predict, using their results to generate a random sequence. These are known as true random number generators (TRNGs). There are physical TRNGs that operate based on various principles, such as chaotic systems, thermal noise in electronic circuits, or biometric parameters, among other examples. A key distinction between pseudorandom number generators and physical random number generators lies in their emphasis on product versus process randomness. In pseudorandom number generators, the evaluation is confined to the output strings, with the focus placed on the product of the deterministic algorithm. The aim is to determine whether the resulting sequence exhibits the characteristics of randomness. To evaluate product randomness, the output strings are analyzed and subjected to specific statistical tests. In contrast, physical random number generators emphasize process randomness, seeking to identify a process that inherently generates random outputs. The objective is to produce true random numbers from fundamentally unpredictable physical phenomena, where randomness is typically defined as unpredictability.

Usually, it is acceptable to use an unpredictable physical system as a source of randomness. However, there remains a question as to whether the underlying physical process is truly random, or if we have an incomplete understanding of the system.

These methods can yield acceptable results for certain applications; however, some devices may be vulnerable to tapping by providers or malicious actors, compromising the security of the generated results and increasing susceptibility to information theft. To achieve a

higher level of randomness suitable for secure applications, quantum-based generators are required. This necessity has led to the development of quantum random number generators (QRNGs) [12], which are devices that use quantum mechanical effects to produce random numbers. Statistical tests [13] are commonly used to verify that the generated numbers follow a uniform probability distribution. However, there remains uncertainty regarding the implications of a given bit string passing these tests. Furthermore, it is inherently impossible to certify true randomness with finite computational resources.

Quantum mechanics is characterized by its probabilistic nature, which inherently incorporates randomness as an intrinsic feature. However, implementing certain schemes often requires consideration of imperfections in devices or external factors that may affect their performance. One approach to addressing these challenges is the Device-Independent (DI) approach, which provides protocols to certify randomness based on general assumptions about the experimental setup, without requiring detailed knowledge of the internal workings of the devices [14]. A distinguishing feature of DI protocols is their reliance on observed statistics to infer the operation of the devices [15]. This characteristic ensures that the devices need not be fully characterized, and the protocol's security remains robust even if the devices' origin is untrusted, effectively mitigating concerns about detector attacks.

Despite the use of defective devices, DI-QRNG faces the challenge of achieving a low bit generation rate, with a maximum recorded value of 114 bits/s [16], in addition to requiring high efficiency. To address these limitations, several semi-DI schemes have been proposed [17–20], including Measurement Device-Independent Quantum Random Number Generation (MDI-QRNG). This approach relies on a reliable preparation device and an unknown measurement device [21], which prepare different quantum states $|\omega_x\rangle$ and produce an output a. At the end of the process, the probability $p(a|\omega_x)$ can be determined. This scheme relies solely on the statistics of the obtained results, increases transmission distances, offers a high generation rate, and is immune to detector attacks. This is particularly relevant in the present day, as detectors are susceptible to side-channel attacks, which has also motivated similar approaches in quantum key distribution (QKD) [14]. In MDI, since we rely on the preparation device, different states are generated to test the proper functioning of the measurement device in real time.

All of these devices employ quantum processes to generate randomness, so users must

adhere to the laws of Quantum Mechanics.

2.3 Entropy

Entropy, in its various forms, provides a convenient way to measure randomness. Different types of entropy offer a mathematical measure of how unexpected a value is [22].

For a random variable X with a probability distribution P_X, where $P_X(x)$ represents the probability of obtaining the outcome x from a discrete set A containing N possible values for x, the Shannon entropy of X, $H(X)$, is defined as:

$$H(X) = -\sum_{x \in A} P_X(x) \log_2[P_X(x)].$$

Shannon entropy gives the average number of bits of information that can be obtained from an individual measurement. If the cardinality of the set of possible outputs is N, and a uniform probability distribution, all the outputs are equally likely and we need $H(x) = \log_2(N)$ bits to describe them [23].

Shannon entropy provides an approximate measure of randomness. The ideal scenario is achieving an entropy value equal to or very close to $\log_2(N)$. High entropy indicates that a distribution is nearly uniform, allowing a larger number of bits to be extracted during the process.

Chapter 3

SDM technology

In this chapter, we will describe the experimental setup of this thesis, including the devices used in the configuration.

The experimental scheme is based on a prepare-and-measure scenario, where a device receives an input x, generates a system in a ρ_x state, and sends it to the measurement device. The measurement device then performs one of several possible measurements, y, and returns a result b [24].

3.1 Beam splitter

A beam splitter (BS) is an optical device that splits a beam of light into two parts. It is used in a variety of experiments and can consist of a glass prism, a semi-transparent mirror, or an optical fiber.

The BS performs a transformation on state $|\psi\rangle$, initially in modes k_1 and k_2, through a unitary matrix, resulting in an output state with modes k_1' and k_2' :

$$\begin{pmatrix} k_1' \\ k_2' \end{pmatrix} = \begin{pmatrix} e^{i\phi}\sin\omega & e^{i\phi}\cos\omega \\ \cos\omega & \sin\omega \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \end{pmatrix}, \tag{3.1}$$

where ϕ is the relative phase between the modes, $\sin\omega$ represents the reflectance, and $\cos\omega$ represents the transmittance of the beam splitter.

3.2 Optical fiber

The accelerated development of quantum information experiments can be attributed to the use of devices originally designed for classical communication [25, 26]. One such device is the optical fiber, a medium for light transmission that has been extensively utilized in telecommunications due to its ability to transmit large amounts of data over long distances. An optical fiber consists of multiple layers that protect the core, through which the light propagates. The core of the optical fiber is made of glass, with impurities that increase its refractive index, ensuring that the light remains confined within the fiber. The transmission window in telecommunications and the use of existing technology require the employment of commercial fibers at a wavelength of $\lambda = 1550$ nm.

In order to increase transmission capacity, a technique called space-division multiplexing (SDM) is employed, where fibers can support different spatial modes of propagation [27]. These include multi-core fibers (MCF) [28, 29], which consist of several single-mode (SM) cores embedded in a common cladding. These cores are sufficiently separated from each other to prevent light coupling between them and are used individually, and few-mode fibers (FMF) [30], a specific class of multimode fibers that have a single core capable of supporting multiple modes. Each mode exhibits minimal crosstalk with others and can therefore be used to transmit information independently.

The employment of SDM fibers is currently preferred due to their effective manipulation and transmission of high-dimensional quantum states over long distances, as well as their application in quantum information processing (QIP), which facilitates the integration of classical and quantum systems [31]. The presence of multiple cores within a single cladding results in equal fluctuations between them, thereby improving the fiber's stability against mechanical or thermal variations. In this context, MCFs offer a distinct advantage in the fabrication of Mach-Zehnder (MZ) interferometers, which exhibit enhanced sensitivity to phase changes.

The Mach-Zehnder interferometer works by splitting a light source into two independent beams that follow separate paths. Then, both beams are recombined to form an interference pattern. The light passing through each path can be altered in various ways (for example, by changing the phase of one of the beams), which will affect the interference pattern at the final detector. This type of interferometer has various applications, including phase measurements, telecommunications, sensors, quantum computing, and integrated optics.

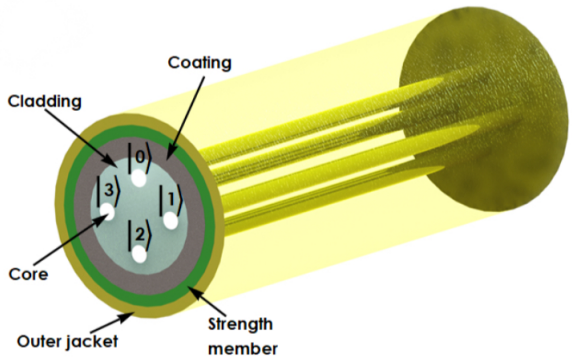

Figure 3.1: 4×4 multi-core fiber.

In a multi-core fiber, a state is defined as a coherent superposition given by

$$|\psi\rangle = \frac{1}{\sqrt{k}} \sum_{0}^{k} e^{i\phi_k} |k\rangle \,, \tag{3.2}$$

where $|k\rangle$ corresponds to the state of the photon transmitted through nucleus k and ϕ_k is the relative phase acquired during propagation through nucleus k.

3.3 Multi-core beam splitter

MCFs offer a distinct advantage in that they facilitate the fabrication of high-dimensional beam splitters, compatible with existing multi-core technology. This capability enables the construction of N-path interferometers, which can be used in various quantum information schemes.

While a multi-path interferometer can be constructed with a known number of beam splitters (BSs), there are certain advantages to using multi-core beam splitters (MBSs) over

2-path BS grids. Specifically, the fabrication of MBSs requires only two MBSs with $N \times N$ cores, whereas the smaller number of BSs required is $N(N-1)/2$ [32]. Moreover, the use of MBSs has been shown to yield more stable interferometers, as evidenced by the fact that a 2-MBS scheme can be controlled by modifying the control methods of a 2-path interferometer. Conversely, a BS mesh necessitates the parallel control of multiple interferometers.

This device is crucial for quantum-information processing because it allows for the generation and measurement of a general class of quantum states. The MBS is fabricated directly within a multicore fiber, using a tapering technique for MCFs [33]. By tapering the fiber, the cores are brought together and, due to evanescent effects, there is light coupling from one core to the others. Due to the symmetry of the MCF structure, the splitting ratio can be made balanced for all core-to-core combinations.

High-quality 4×4 MBSs are constructed directly in a four-core optical fiber through a tapering technique recently introduced in [33]. The objective of that work was to build multi-arm MZ interferometers for multi-parameter estimation. The proposed approach involved the use of a heterogeneous multi-core fiber, which has lower refractive index "trenches" around the cores, to minimize inter-core coupling. In such fibers, at least two orthogonal modes propagate over one core of the fiber, and under normal circumstances, these modes never interfere. However, by tapering the fiber, an overlap between these modes was created due to strong evanescence effects in the tapered zone. From the interference observed, parameter estimation was possible. Interference was used to estimate different parameters of a sample, effectively transforming the fiber into an instrument composed of several two-path MZ interferometers. In the tapered region, the inter-coupling between different cores was severely reduced by such trenches.

In this study, we demonstrate that by utilizing the aforementioned technique, but with homogeneous MCFs—that is, fibers where the N cores are not constrained by refractive index trenches—it is possible to construct high-quality $N \times N$ MBSs. The tapering process entails local heating of a small transverse region of the fiber with length L, in conjunction with the application of controlled longitudinal stretching tension. The fiber's mechanical state, characterized by partial softness, will undergo a transformation, becoming thinner with a final diameter, D_w, at the center of the heated region. Consequently, the cores will 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. The splitting ratio can be balanced by monitoring the transmission of a $\lambda = 1550$ nm laser beam through the four-core fiber while tapering it. Finally, given that the MBS is directly constructed on a MCF, it is compatible for connection with other MCFs by direct contact.

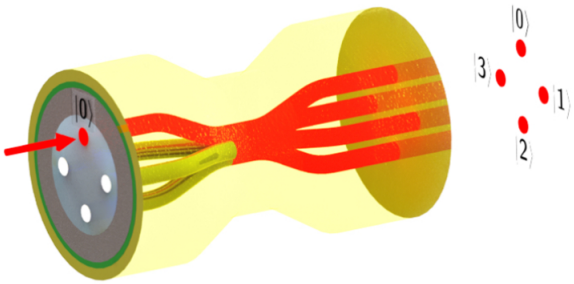

Figure 3.2: 4×4 Multi-core beam-splitter.

The fabricated four-core MBSs were tested by first illuminating one of the cores of a MCF. This fiber was connected to the MBS under test, and at the output, the light was split across the other cores. The output power per core was then measured individually with p-i-n photodiodes. The power at each core was found to be very stable, and the observed average split ratio was (0.248 ± 0.01). The insertion loss of the 4×4 MBSs is calculated to be $4.3 \pm 0.06\%$.

In general, symmetric 4×4 MBSs are parameterized in terms of the unitary operation given by [32, 34]

$$V = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{i\phi} & -1 & -e^{i\phi} \\ 1 & -1 & 1 & -1 \\ 1 & -e^{i\phi} & 1 & e^{i\phi} \end{pmatrix}. \tag{3.3}$$

Since the cores are equally distant from 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 [35]. 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. 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 MBSs. At the MBS output ports, the probabilities of recording the photon are given by $p(k|j) = \frac{1}{2} \left[u_{k1}^2 + u_{kj}^2 + 2u_{k1}u_{kj} \cos(\varphi + \phi_{kj} - \phi_{k1})\right]$. Hence, by recording these probabilities with respect to φ, we acquire the relative phases $\phi_{kj} - \phi_{k1}$.

Using the scheme described below to characterize the 4×4 MCF MBS gives the following experimental estimate:

$$\tilde{U} = \begin{pmatrix} 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.493 + 0.07i & -0.497 - 0.05i & -0.499 - 0.01i \\ 0.5 & -0.496 - 0.06i & 0.499 + 0.03i & -0.499 + 0.03i \\ 0.5 & -0.5 & -0.496 + 0.06i & 0.499 - 0.03i \end{pmatrix}, \tag{3.4}$$

while the corresponding unitary one is

$$\hat{U} = \begin{pmatrix} 0.499 & 0.501 & 0.499 & 0.499 \\ 0.501 & 0.491 + 0.08i & -0.496 - 0.06i & -0.498 - 0.01i \\ 0.499 & -0.495 - 0.06i & 0.498 + 0.03i & -0.499 + 0.03i \\ 0.499 & -0.499 - 0.01i & -0.499 + 0.03i & 0.499 - 0.01i \end{pmatrix}. \tag{3.5}$$

The fidelity between the experimental estimate and the unitary estimate is

$$F(\tilde{U}, \hat{U}) = 0.999 \pm 0.001.$$

Note that the unitary estimate is almost a symmetric unitary matrix, or equivalently, the absolute value of each coefficient of the matrix is approximately $1/2$. Comparing the unitary estimate with the symmetric unitary matrix (3.3) with $\phi = 0$, we have the fidelity

$$F(\hat{U}, V_{\phi=0}) = 0.995 \pm 0.003.$$

Chapter 4

MDI randomness generation

In this chapter, we detail the use of a high-quality multicore beam splitter with four cores, constructed from commercial multicore fibers, in the fabrication of a programmable quantum circuit. This circuit consists of a four-path Mach-Zehnder interferometer in optical fiber, where we generate on-path encoded qudits, which are then transmitted through the circuit. The detection results are subsequently stored and analyzed.

A high-dimensional scheme confers several advantages, including the increased amount of information transmitted by a multicore fiber and the minimal thermal and phase variations in each core.

4.1 Experimental scheme

In this scheme, we use a continuous-wave laser with a wavelength of 1546 nm as the source, which is externally modulated by a Mach-Zehnder electro-optical device with a bandwidth of 10 GHz to generate optical pulses 5 ns wide. Optical attenuators are employed to reduce the average number of photons per μ pulse, thereby generating coherent states [25]. In our experiment, we implemented average photon numbers per pulse of $\mu = 0.4$ and $\mu = 0.2$. In this case, the probability of having non-zero pulses, i.e., pulses containing at least one photon, is $P(\mu = 0.4) = 26.8\%$.

The multi-arm interferometer works with a repetition rate of 2 MHz and has an integration time of 0.1 s.

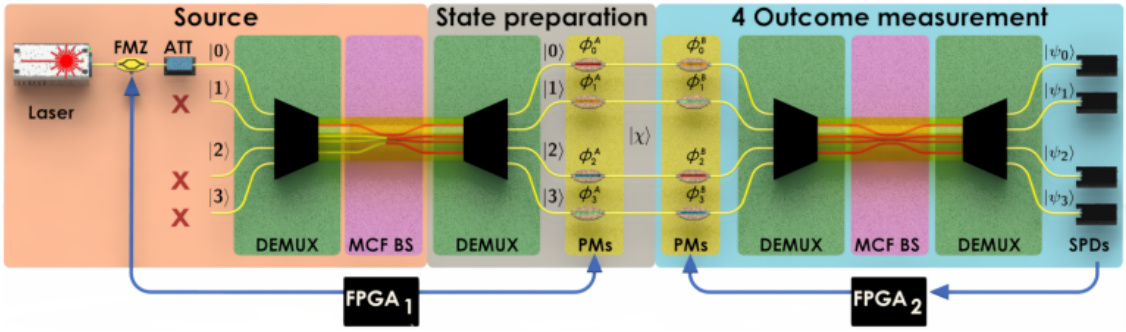

Figure 4.1: Schematics of the experimental setup implementing the programmable quantum circuit for HD quantum information processing. FMZ: fiber-pigtailed amplitude modulator, ATT: optical attenuators, DEMUX: spatial demultiplexer unit, MCF BS: multi-core fiber beam splitter, PMs: phase modulators, SPDs: single-photon detection modules.

The attenuated pulses are transmitted to a spatial demultiplexer (DEMUX) [36], which is used to combine and separate the different transverse optical modes supported by the SM fiber. The DEMUX consists of four independent SMFs connected to a four-core MCF, with each individual fiber coupled to one of the cores of the MCF. After the DEMUX, only one of the cores is illuminated. This multi-core fiber is connected to a 4-path MBS, which, in turn, is connected to a second DEMUX via its MCF, separating each core into independent SMFs. The state of the transmitted photon within the MCF is a coherent superposition given by $|\Psi\rangle = \frac{1}{2}\sum_{k=1}^{4} e^{i\phi_k} |k\rangle$, where $|k\rangle$ represents the state of the photon transmitted through the k-th mode, and ϕ_k is the relative phase acquired during propagation in the k-th mode.

Each path is equipped with two 10 GHz bandwidth phase modulators (PMs), which facilitate the preparation and measurement of a more general class of qudits. Each PM is equipped with a polarizer that aligns the photon's polarization state, ensuring the indistinguishability of the modes and preserving the interferometer's visibility [37, 38]. The first set of PMs is controlled by a programmable unit or FPGA1 and are used for state preparation.

The general form of the states that are prepared is

$$|\chi\rangle = \frac{1}{2}(e^{i\phi_0^A} |0\rangle + e^{i\phi_1^A} |1\rangle + e^{i\phi_2^A} |2\rangle + e^{i\phi_3^A} |3\rangle), \tag{4.1}$$

where ϕ_k^A is the phase applied by the first modulator in mode k and $|k\rangle$ is the photon state transmitted by the mode k.

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. In this case, the matrix that represents the 4-path MBS is given by [34]

$$BS = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}. \tag{4.2}$$

Thus, considering the second set of PM independently controlled by the FPGA2, the form of the measurement basis states at the end of the circuit are given by

$$|\psi_0\rangle = \frac{1}{2}(e^{i\phi_0^B}|0\rangle + e^{i\phi_1^B}|1\rangle + e^{i\phi_2^B}|2\rangle + e^{i\phi_3^B}|3\rangle), \tag{4.3}$$

$$|\psi_1\rangle = \frac{1}{2}(e^{i\phi_0^B}|0\rangle + e^{i\phi_1^B}|1\rangle - e^{i\phi_2^B}|2\rangle - e^{i\phi_3^B}|3\rangle), \tag{4.4}$$

$$|\psi_2\rangle = \frac{1}{2}(e^{i\phi_0^B}|0\rangle - e^{i\phi_1^B}|1\rangle - e^{i\phi_2^B}|2\rangle + e^{i\phi_3^B}|3\rangle), \tag{4.5}$$

$$|\psi_3\rangle = \frac{1}{2}(e^{i\phi_0^B}|0\rangle - e^{i\phi_1^B}|1\rangle + e^{i\phi_2^B}|2\rangle - e^{i\phi_3^B}|3\rangle). \tag{4.6}$$

where ϕ_k^B is the phase applied by the second modulator in the core mode k.

In orden 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 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.

The interferometer is thermally insulated to minimize additional random phase drifts between the single-mode fibers. Nevertheless, long-term phase drifts are presents, so 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 [39]. Each applied phase can be decomposed as

$$\phi_k^B = \phi_k^{bias} + \phi_k^{mod}, \tag{4.7}$$

where the employed voltage driver is capable of supplying the sum of two independent voltages V_{bias} y 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

$$\phi_k^B = \phi_k^{bias} + \phi_k^{mod} + \phi_k^n, \tag{4.8}$$

the phase drift compensation algorithm running in FPGA2 will perturb the kth PM to make $\phi_k^{bias} = -\phi_k^n$, 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.

4.2 Operation and stabilization

When the system is initialized, the stabilization control typically takes around 15 s to align the interferometer, 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 measurement 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 hours continuously.

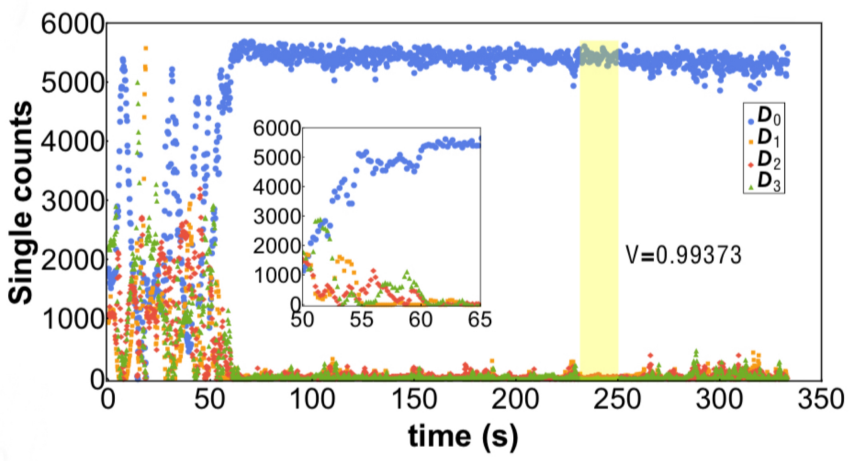

Figure 4.2: Active stabilization of the multi-arm interferometer.

To show the quality of the MCF-based multi-arm interferometer, we gradually generate the quantum states associated with each outcome of the interferometer when all ϕ_k^B are set to zero, obtaining the traditional interference curves. Based on the obtained results, the visibility is calculated as $V_k = |(C_{Dk}^{max} - C_{Dk}^{min})/(C_{Dk}^{max} + C_{Dk}^{min})|$, where C_{Dk} indicates the single counts given by the detector Dk $(k = 0, 1, 2, 3)$, so the average visibility recorded is 0.992 ± 0.0015, showing that path qudit states can be prepared and measured with high fidelities in out scheme.

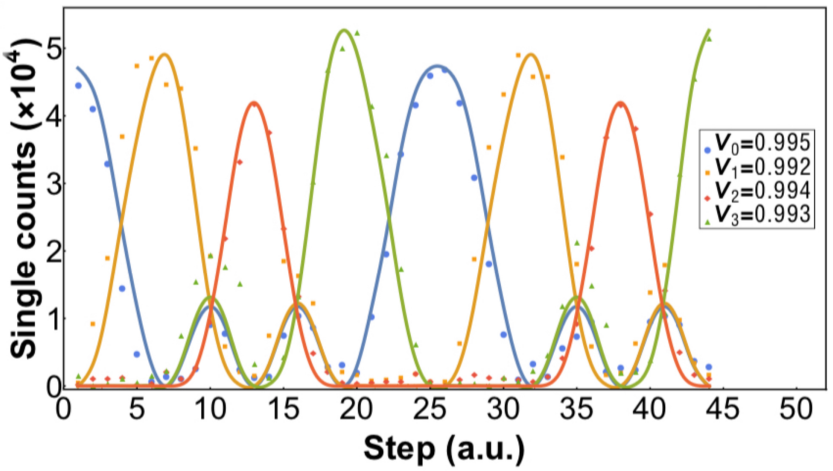

Figure 4.3: Detection rate as a function of modulated phases ϕ_k^A.

One relevant 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.

4.3 Weak coherent pulses

The implementation of the experiment requires the utilization of a source that approximates a single photon. However, such a source is not readily available, necessitating the use of weak coherent pulses as an alternative. These pulses are generated by attenuating a laser beam, a technique that allows the system to operate closer to the single-photon regime. This approach is employed to minimize the risk of information leakage or theft. The photon number probability distribution of these pulses follows a Poisson distribution, as described by

$$P(\mu, \lambda) = \frac{e^{-\mu}\mu^{\lambda}}{\lambda!}, \tag{4.9}$$

where $\mu > 0$ is the expected number for a certain phenomenon to occur and $\lambda = 0, 1, 2, ...$ how many times the phenomenon occurs. We seek $\mu \ll 1$, where the probability of generating a pulse of two or more photons is very low.

4.4 Measurement device independent protocol

In the scenario of MDI RNG, an user in need of random numbers possesses a characterized preparation device and an uncharacterized measurement device $\mathcal{M}$ [21]. This scenario is relevant, as single-photon detectors are prone to side-channel attacks, which has motivated the development of similar approaches in quantum key distribution [14]. The preparation

device is used to prepare quantum quantum states ω_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 $p(a|\omega_x)$. $\mathcal{M}$ could have been constructed by an eavesdropper, who aims to predict the outcome a. The eavesdropper 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 the eavesdropper makes a measurement on her part of ρ^{AE} to guess the bit generated.

The maximal probability $P_g(x^*)$ that the eavesdropper 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 [21, 40]. Finally, the amount of randomness that is certified per round under the assumption that the eavesdropper carries out individual attacks is given by the min-entropy of P_g :

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

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 $|\langle\omega_x|\omega_4\rangle|^2 = 1/4, \forall x = 0, ..., 3$. 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 for this ideal implementation gives $H_{min}(x = 4) = 2$, showing that two bits of randomness per round can be generated.

Chapter 5

Results

In chapter 4 we show that the probability of emitting j photons per pulse is characterized by the mean photon number μ such that $P(j) = \frac{e^{-\mu}\mu^j}{j!}$. 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. Tipically, 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. An eavesdropper can take advantage of the multi-photon components, which decreases the amount of private randomness that can be produced. We partially overcome this by using the multi-photon detection events in addition to single-photon events to generate randomness. 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 for:

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

where $p(1) + p(2) = 1, \left|\omega_{x=0}\right\rangle = \left|0\right\rangle, ..., \left|\omega_{x=3}\right\rangle = \left|3\right\rangle$ are the states corresponding to one photon traveling in each mode $x, \left|\omega_4\right\rangle = (\left|0\right\rangle - \left|1\right\rangle + \left|2\right\rangle + \left|3\right\rangle)/2$ is the mutually unbiased state, and $\left|\phi_x^{(2)}\right\rangle$ refers to states where two photons are generated in a single pulse. In this experiment, we observe 10 measurement outcomes: four single clicks corresponding to photon detection at one of the four detectors $D_i (i = 0, ..., 3)$, 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 $\rho_{x=0}, ..., \rho_{x=3}$. 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 $\left(\bar{p} = \frac{1}{4}\sum_{x=0}^{3} p(x|\rho_x)\right)$. 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 would achieve.

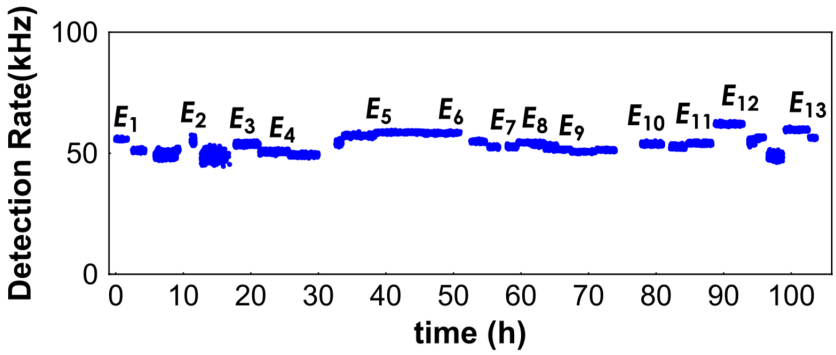

Figure 5.1: Single count detection rate considering only the selected sample.

This figures shows a fragment of the recorded data while the random number generator is operating with $\mu = 0.4$. The points in 5.1 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 $i = \{1, 2, ..., 13\}$ 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.

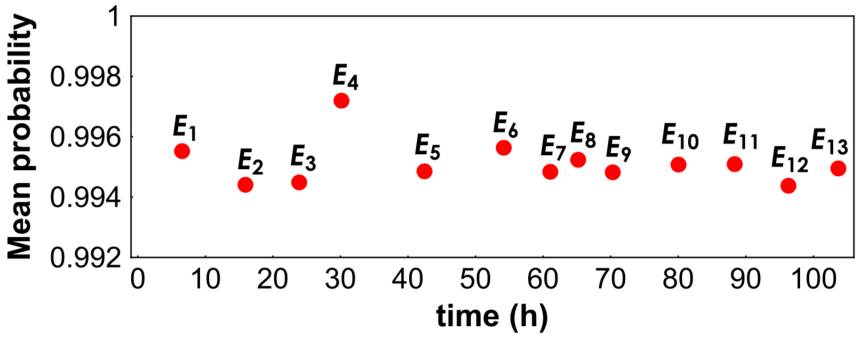

Figure 5.2: Observed average success probability for each zone E_i.

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.

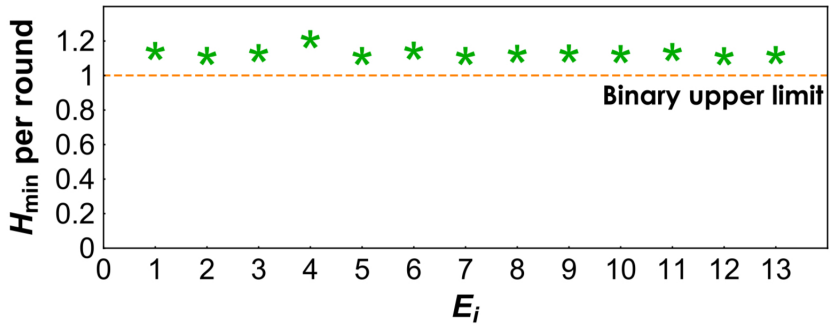

Figure 5.3: Average obtained randomness per experimental round for each zone E_i. The dashed line represents the theoretical upper bound allowed for binary RNG protocols.

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 $\mu = 0.2$.

Chapter 6

Conclusion

This research presents a significant advancement in the application of high-dimensional quantum information processing using multiport beam splitters based on multicore optical fiber technology. We use a 4×4 MBS 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 demostrate the versatility and advantages of the circuit, we have demostrated a MDI quantum randon number generator using four-dimensional photonics 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 al 2 MHz repetition rate, generating about $6 \cdot 10^4$ 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 demonstrate that the space-division multiplexing technique offers a significant advantage for high-dimensional quantum information processing. It is crucial as a robust new platform for implementing universal programmable optical circuits, enabling the achievement of high visibility.

Appendix A

Self-Testing Mutually Unbiased Bases in Higher Dimensions with Space-Division Multiplexing Optical Fiber Technology [41].

Self-Testing Mutually Unbiased Bases in Higher Dimensions with Space-Division Multiplexing Optical Fiber Technology

Máté Farkas,[1,2,3] Nayda Guerrero,[4,5] Jaime Cariñe,[6,5] Gustavo Cañas,[7,*] and Gustavo Lima[4,5]

[1] *Institute of Theoretical Physics and Astrophysics, National Quantum Information Center, Faculty of Mathematics, Physics and Informatics, University of Gdansk, 80-952 Gdansk, Poland*

[2] *International Center for Theory of Quantum Technologies, University of Gdansk, 80-308 Gdansk, Poland*

[3] *ICFO—Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels Barcelona, Spain*

[4] *Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile*

[5] *Millennium Institute for Research in Optics, Universidad de Concepción, 160-C Concepción, Chile*

[6] *Departamento de Ingeniería Eléctrica, Universidad Católica de la Santísima Concepción, Concepción, Chile*

[7] *Departamento de Física, Universidad del Bío-Bío, Collao 1202, Casilla 5C, Concepción, Chile*

(Received 11 June 2020; revised 15 November 2020; accepted 15 December 2020; published 15 January 2021)

In the device-independent quantum-information approach, the implementation of a given task can be self-tested solely from the recorded statistics and without detailed models for the employed devices. Even though experimentally demanding, it provides appealing verification schemes for advanced quantum technologies that naturally fulfil the associated requirements. In this work, we experimentally study whether self-testing protocols can be adopted to certify the proper functioning of quantum devices built with modern space-division multiplexing optical fiber technology. Specifically, we consider the prepare-and-measure protocol of Farkas and Kaniewski [Phys. Rev. A 99, 032316 (2019)] for self-testing measurements corresponding to mutually unbiased bases (MUBs) in a dimension $d > 2$. In our scheme, the state preparation and measurement stages are implemented using a multiarm interferometer built with multicore optical fibers and related components. Due to the high overlap of the interferometer's optical modes achieved with this technology, we are able to reach the required visibilities for self-testing the implementation of two four-dimensional MUBs. We also quantify two operational quantities of the measurements: (i) the incompatibility robustness, connected to Bell violations, and (ii) the randomness extractable from the outcomes. Since MUBs lie at the core of several quantum-information protocols, our results are of practical interest for future quantum works relying on space-division multiplexing optical fibers.

DOI: 10.1103/PhysRevApplied.15.014028

I. INTRODUCTION

The advent of quantum-information technologies comes with promises such as exponential computational speed-up compared to currently existing classical algorithms [1,2] or unconditionally secure quantum communication [3,4]. However, the success of these protocols relies on certification methods to verify that the used devices perform the tasks they are promised to perform. Furthermore, it should be possible to perform these verification methods efficiently and using only classical resources. Consequently, they are currently the subject of intensive study in the quantum-information community [5–12], where they are commonly referred to as self-testing protocols. The strongest method is known as the "device-independent approach," which involves two parties sharing an entangled quantum state, and the only considered assumption for self-testing the proper implementation of a given task is that these parties are spacelike separated. The certification is based solely on the recorded measurement statistics of the two parties [13]. This method, however, comes with a few drawbacks. First, it is rather challenging to implement experimentally, as it requires the production of entangled states with very high fidelities. Second, in dimensions larger than two, the theoretical treatment becomes complex as well. Accordingly, there are only a few theoretical results available for high-dimensional quantum states (qudits) [14,15] and the method has never been experimentally demonstrated.

Nonetheless, the use of qudit systems is advantageous for several quantum-information tasks. For example, they allow for larger violations of Bell inequalities [16],

*gustavocanascardona@gmail.com

improvement on quantum computation and communication complexity tasks [17,18], and higher randomness-generation rates [19]. Thus, there is a current need for more practical self-testing protocols in higher dimensions. In order to alleviate the difficulties mentioned above, several relaxations of the demanding device-independent scheme have been introduced. One generic direction is to move to the experimentally less demanding prepare-and-measure scenario, in which instead of sharing an entangled state, one party prepares a state and sends it to the other party, who then measures it. In this scenario, further reasonable assumptions are necessary to devise certification methods. These include bounds on the average energy of the quantum states [20] or the indistinguishability of the different states prepared [21]. Perhaps the most traditional such relaxation is to fix the dimension of the quantum states [6,22–24].

Recently, in Ref. [25], a method has been proposed for self-testing high-dimensional measurements corresponding to mutually unbiased bases (MUBs) in the prepare-and-measure scenario, under the dimension assumption. MUBs constitute a particularly useful family of quantum measurements, with myriad applications in quantum information. Among other tasks, they optimize state determination [26,27], generate the maximal amount of randomness [28], and give rise to secure cryptographic protocols [3] (for a survey, see Ref. [29]). The authors of Ref. [25] anticipate that their certification method can be performed with currently available technologies in dimensions larger than two. This is precisely the aim of the current work, in which we experimentally study whether self-testing certification methods can be adopted in the platform of space-division multiplexing (SDM) optical fiber technology to quantum-information processing [30]. In our scheme, we use single-photon path-encoded four-dimensional quantum systems (ququarts) and the state preparation and measurement stages are implemented by resorting to an advanced four-arm interferometer built of multicore optical fibers and related technology, which we present next. As observed in Ref. [19], this scheme should, in principle, attain the optical quality required for implementing self-testing protocols. Indeed, here, in our test of Ref. [25], we are able to record the corresponding data with an average visibility of $99.89 \pm 0.03\%$, which allows us to self-test the proper implementation of a pair of four-dimensional MUBs. Moreover, we also certify the incompatibility of our implemented measurements and the randomness extractable from their outcomes. Note that while this same type of protocol has already been implemented experimentally in higher dimensions [31–34], the error rates have never been suppressed to a level that would allow the self-testing of the measurements performed.

Our results highlight the advantages of modern SDM technologies for high-dimensional quantum-information processing, by demonstrating that devices based on this technology can be self-tested. This means that state preparations and measurements can be performed on this platform with very high fidelity. Furthermore, the self-tested MUB measurements are widely useful in quantum-information processing, proving this technology to be of broad relevance in the field. Lastly, we note that the self-testing protocol adopted can be regarded as a generalization of the quantum key distribution protocol of Ref. [35].

II. THEORY

Formally, a pair of MUBs in dimension d corresponds to two rank-1 measurements projecting onto the orthonormal bases $\{|a_i\rangle\}_{i=1}^d$ and $\{|b_j\rangle\}_{j=1}^d$ on $\mathbb{C}^d$. We say that these bases are mutually unbiased if

$$|\langle a_i|b_j\rangle|^2 = \frac{1}{d} \; \forall i,j \in \{1,\ldots,d\}, \tag{1}$$

that is, every pair of vectors from different bases has the same overlap. One simple example is the eigenbases of the Pauli X and Z operators on a qubit.

The prepare-and-measure self-testing method used in Ref. [25] to certify d-dimensional MUB measurements is based on the so-called $2^d \to 1$ quantum-random-access-code (QRAC) protocol. In a QRAC, the preparation side (Alice) receives two uniformly random classical dits, $i,j \in \{1,\ldots,d\}$. Based on this input, Alice prepares the d-dimensional quantum state, ρ_{ij}, and sends it to Bob on the measurement side. Bob receives a uniformly random classical bit, $y \in \{1,2\}$, based on which he decides which observable to measure on the state ρ_{ij}. If $y = 1$, his measurement is a d-outcome positive-operator-valued measure (POVM), the measurement operators of which are denoted by A_i. Similarly, for $y = 2$, he measures B_j. Recall that for POVMs we have that $A_i, B_j \geq 0$ and $\sum_{i=1}^d A_i = \sum_{j=1}^d B_j = \mathbb{I}$. That is, a d-outcome POVM is a set of d positive semidefinite operators that add up to the identity operator. Let us denote the outcome of Bob's measurement by $b \in \{1,\ldots,d\}$. The common aim of the parties is that when $y = 1$, Bob's output equals Alice's first input, that is, $b = i$, and when $y = 2$, they have $b = j$. To quantify their success rate, we employ the *average success probability* (ASP) $\bar{p} = \frac{1}{2}[P(b = i|y = 1) + P(b = j|y = 2)]$ as the figure of merit. According to the Born rule, the probability of Bob outputting b when Alice's input is i,j and Bob's input is $y = 1$ is $\mathrm{tr}(\rho_{ij}A_b)$ and, similarly, it is $\mathrm{tr}(\rho_{ij}B_b)$ when $y = 2$. That is, the ASP for a generic encoding scheme ρ_{ij} and measurement choice A_i and B_j can be written as

$$\bar{p} = \frac{1}{2d^2} \sum_{i,j=1}^{d} \mathrm{tr}\left[\rho_{ij}(A_i + B_j)\right]. \tag{2}$$

In Ref. [25], the authors provide certificates for MUBs based only on the recorded ASP in a QRAC. They show that in dimension d, $\bar{p} \leq \frac{1}{2}(1 + 1/\sqrt{d}) =: \bar{p}_Q$ and this maximum can only be attained if Bob's measurements correspond to a pair of MUBs. Moreover, even for suboptimal $\bar{p}$, one can certify the closeness of the employed measurements to a pair of MUBs. Specifically, one can bound the entropy of the generalized overlaps of the two measurements and the sum of the individual operator norms. These two measures together—having sufficiently high values—imply that the measurement operators have close-to-uniform overlaps and are close to being rank-1 projectors, that is, they are close to MUBs.

Specifically, the first quantity employed is the *overlap entropy*, $H_S(A,B) = H_{\frac{1}{2}}\left\{\left[\mathrm{tr}(\mathrm{A_i B_j})/\mathrm{d}\right]_{ij}\right\}$, where $H_{1/2}$ is the $\frac{1}{2}$-Rényi entropy [note that for projective measurements, $\mathrm{tr}(\mathrm{A_i B_j}) = |\langle \mathrm{a_i}|\mathrm{b_j}\rangle|^2$]. It has been shown that given an observed ASP $\bar{p}$, it holds for the measurements A and B that [25]

$$H_S(A,B) \geq 2\log\left[d\sqrt{d}(2\bar{p} - 1)\right]. \tag{3}$$

The maximal possible value of the overlap entropy, $\log d^2$, is reached by MUBs and can be certified upon observing $\bar{p} = \bar{p}_Q$.

The second quantity is the *sum of the norms*, $N(A) = \sum_{i=1}^{d} \|A_i\|$. It has also been shown in Ref. [25] that

$$N(A) \geq d - \frac{2+\sqrt{2}}{d}\left[1 - \sqrt{d^3(2\bar{p}-1)^2 - (d^2-1)}\right], \tag{4}$$

and the same holds for B. The maximal possible value of the sum of the norms, d, is reached if and only if the measurements are rank-1 projective and this can be certified upon observing $\bar{p} = \bar{p}_Q$.

Putting the above two bounds together, observing $\bar{p} = \bar{p}_Q$ implies that $\mathrm{tr}(\mathrm{A_i B_j}) = 1/\mathrm{d}$ for all i,j and that the measurements are rank-1 projective. In other words, $\bar{p} = \bar{p}_Q$ certifies that Bob's measurements correspond to a pair of MUBs. By the continuity of the bounds in $\bar{p}$, it follows that if the observed ASP is suboptimal, $\bar{p} < \bar{p}_Q$, but close to optimal, then the overlap entropy and the sum of the norms are both close to their unique MUB values. This serves as a certificate that the employed measurements are close to MUBs.

Lastly, the authors of Ref. [25] derive certificates for two useful properties of the measurements: incompatibility robustness and the amount of randomness generated. The former, briefly speaking, is the maximal visibility of the measurements at which they are jointly measurable (compatible) [36]. Clearly, for compatible measurements pairs, this maximal visibility is 1 and the lower the value, the more incompatible the pair is. Jointly measurable observables are of no use in nonlocal and steering scenarios [37] and therefore it is important to quantify the extent to which a pair of measurements is incompatible. In Ref. [25], the authors show that the incompatibility robustness of A and B is bounded by

$$\eta^* \leq \frac{\frac{1}{2}d^2(1 + s_{\max}) - \frac{N(A)^2}{d}}{N(A)^2 - d - [d - N(A)][d - N(A) + 1]}, \tag{5}$$

where $s_{\max} = \max_{ij} \|\sqrt{A_i}\sqrt{B_j}\|$. Using the bounds in Eqs. (3) and (4), one can then bound the incompatibility robustness by the observed ASP. The value corresponding to a pair of MUBs, $\eta^* = \frac{1}{2}\left[1 + 1/(\sqrt{d}+1)\right]$, can be certified upon observing $\bar{p} = \bar{p}_Q$.

The second quantity to certify is the amount of uncertainty produced in the outcome of the measurements, formulated as an entropic uncertainty relation [38]. This amounts to a lower bound on the entropy of the measurement outcome probabilities in a state-independent fashion. Let us denote the Shannon entropy of the outcome probabilities of the measurement A on the state ρ by $H(A)_\rho$. Then, it has been shown in Ref. [25] that given a QRAC ASP $\bar{p}$, it holds that

$$H(A)_\rho + H(B)_\rho \geq -2\log\left(2\bar{p} - 1 + \frac{1}{d}\sqrt{d(d^2-1)[1 - d(2\bar{p}-1)^2]}\right), \tag{6}$$

for any state ρ. Note that the maximal value for rank-1 projective measurements, $\log d$, can again be certified upon observing $\bar{p} = \bar{p}_Q$.

III. SPACE-DIVISION MULTIPLEXING TECHNOLOGY

SDM is a classical telecommunication technique that uses multiple transverse optical modes for increasing data-communication capacity. The SDM technique is implemented for optical communication links in both free space and fiber optics [39,40]. It is considered a crucial solution to overcome the so-called "capacity crunch" of fiber-optic communications [40]. In this case, SDM technology is typically based on few-mode fibers (FMFs) [41–43], ring-core fibers (RCFs) [44], and multicore fibers (MCFs) [45,46]. These are schematically represented in Fig. 1.

FMFs are a particular class of multimode fibers (MMFs), which support only a few linearly polarized transverse optical modes [41–43]. Each mode that is supported in a FMF has very low crosstalk to the others and, therefore, can be used as an independent data channel. RCFs are optical fibers with an annular refractive index profile that supports multiple Laguerre-Gaussian beams

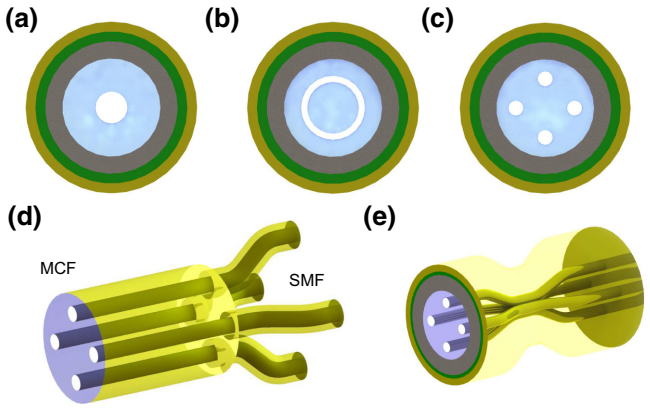

FIG. 1. The fibers and components typically used in the SDM approach for fiber-optics communication. A schematic representation of the cross section of (a) a few-mode fiber, (b) a ring-core fiber, and (c) a multicore fiber (with four cores). Each of them is composed of a core (white), cladding (light blue), a coating (gray), a strength member (green), and an outer jacket (yellow). A FMF supports the propagation of a few linearly polarized modes. A RCF has an annular core that supports, for instance, the propagation of some Laguerre-Gaussian optical modes. The MCF is a single fiber with several single-mode cores within its cladding. (d) The schematics of demultiplexer devices used for efficiently coupling light into multicore fibers (insertion loss <0.7 dB). (e) An example of a four-core fiber-integrated multiport beam splitter.

carrying orbital angular momentum (OAM) [47]. Lastly, there are MCFs, which are considered to be the most promising solution for SDM, since their fabrication is cost effective [46]. An MCF is a single fiber containing multiple cores within the same cladding, which are sufficiently separated from each other to avoid light coupling between them. Typically, crosstalk between the cores is negligible with more than 60 dB of attenuation [46].

Together with the development of these fibers, several related components have been built to improve the efficiency of SDM techniques. For instance, there are multiplexer-demultiplexer (DEMUX) devices, used to combine and separate the different transverse optical modes supported by the SDM fiber. Typically, these devices have N independent single-mode fibers connected to the SDM fiber, mapping N transverse Gaussian modes onto the N particular optical modes supported by the SDM fiber. For FMFs, DEMUXs called photonic lanterns are used [48]. For RCFs, these devices are called mode sorters. They are usually built with bulk optics [49] but an important recent development is an all-fiber mode sorter [50]. Finally, the DEMUXs used for MCFs are devices composed of single-mode fibers (SMFs), each one connected to one core of the MCF. These devices are already commercially available and are built using a fiber-bundle polishing-and-tapering technique, presented in Refs. [51,52]. In Fig. 1(d), we show, as an example, the schematics of a MCF DEMUX.

Our experimental setup is based on MCFs and in this case another important device is the multicore fiber-integrated multiport beam splitter (MBS), recently presented in Ref. [19] [see Fig. 1(e)]. This device is crucial for quantum-information processing because it allows one to implement distinct unitary operations representing the change of basis from the logical basis to a basis that is mutually unbiased to it. Thus, it allows for the generation and measurement of a general class of quantum states, as we explain in the next section. The MBS is fabricated directly within a multicore fiber, using a tapering technique for MCFs [53]. By tapering the fiber, the cores are brought together and, due to evanescent effects, there is light coupling from one core to the others. Due to the symmetry of the MCF structure, the splitting ratio can be made balanced for all core-to-core combinations.

IV. EXPERIMENT

Recently, the technology developed for SDM has become a platform for high-dimensional quantum-information processing [30]. Initial efforts, based on path-encoded qudits and multicore fibers [54–58], have now been expanded to different types of fibers and encoding schemes [59–62]. Nonetheless, this platform has not yet been demonstrated to be compatible with modern self-testing protocols of quantum states and circuits. Here, we fill this gap by extensively studying the protocol of Ref. [25]. Specifically, we measure the QRAC ASP and bound all the quantities of Eqs. (3)–(6) with a four-arm Mach-Zehnder (MZ) interferometer built of MCFs and the related technology discussed above.

The state preparations in the QRAC protocol are realized by photonic states. The initial photon source is a continuous-wave telecom laser, operating at 1546 nm (see Fig. 2). It is connected to an external fiber-pigtailed amplitude modulator (FMZ), which is controlled by a field-programmable gate array (FPGA) electronic unit to generate 5-ns-wide pulses. Then, we use optical attenuators (ATT) to create weak coherent states. The attenuators are calibrated to set the average number of photons per pulse to $\mu = 0.2$. In this case, the probability of having pulses containing at least one photon is $P(n \geq 1|\mu = 0.2) \approx 18\%$. Most of the non-null pulses contain only one photon and represent 90.3% of the experimental runs. Therefore, our source can be seen as a good approximation of a non-deterministic source of single photons [63]. We note that coincidence detections are not discarded in our analysis and that the proportion of events where coincidence detections occurs is much smaller than 1.81%. It corresponds to only 0.045%, which is a consequence, for instance, of the fact that, in some cases, both photons go to the same

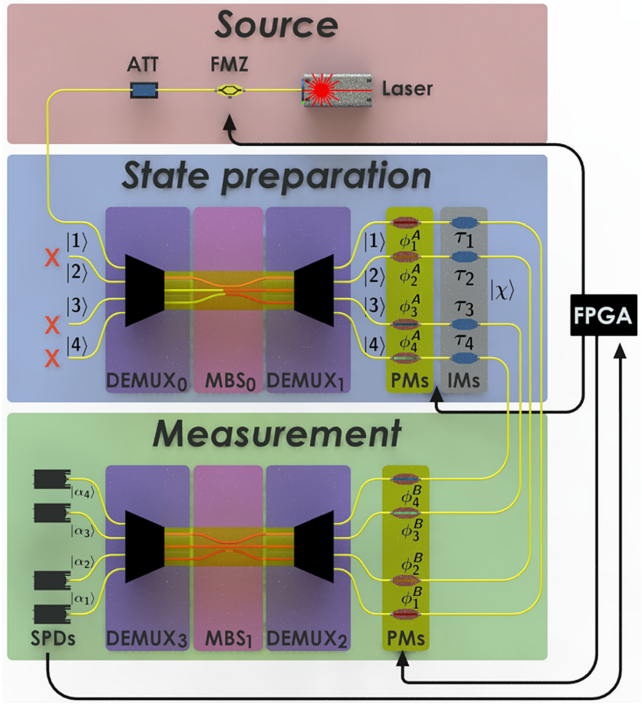

FIG. 2. The experimental setup is based on a four-arm Mach-Zehnder interferometer built of four-core multicore fibers (MCF) and related technology (see Sec. III). The interferometer is used for preparing and measuring path-encoded ququart states. At the state-preparation stage, the initial state is prepared by a set composed of a 4×4 MCF based multiport beam splitter (MBS_0) and phase (PM) and amplitude (IM) fiber-pigtailed modulators. The measurement is achieved using another set of PMs and a second MBS_1 connected to four single-photon detection (SPD) modules. The field-programmable gate array (FPGA) electronic unit automatically controls the protocol implementation. See the main text for details.

detector—or to the more general fact that, in most of the cases, one photon is detected and the other is not.

The signal from the source is sent to a commercial-fiber built-in DEMUX unit ($DEMUX_0$), which consists of four independent single-mode fibers, each of them connected to one core of a four-core MCF. The source is connected through one of the four SMFs of $DEMUX_0$; therefore, only one core of the MCF is illuminated. $DEMUX_0$ is then connected to a MCF-based 4×4 MBS (denoted MBS_0), the matrix representation of which is given by [19]

$$U_{\mathrm{MBS}} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{7}$$

in the logical basis. In our scheme, the logical states are defined in terms of the core modes available for the photon propagation over the multicore fiber [19,55]. Therefore, the 4×4 MBS corresponds to a Hadamard gate in dimension four.

MBS_0 is then coupled to a second DEMUX (denoted $DEMUX_1$) via their respective MCFs. In order to control the initial quantum state entering the interferometer, we connect phase (PM) and amplitude (IM) fiber-pigtailed modulators to each SMF of $DEMUX_1$, these being controlled by the FPGA. The general path-encoded ququart state that we can prepare in the first part of the MZ is then given by

$$|\chi\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^{4} \tau_k e^{i\phi_k^A} |k\rangle, \tag{8}$$

where $|k\rangle$ represents the state of the photon transmitted in the kth core (i.e., the kth logical state). τ_k and ϕ_k^A are the transmissivity and relative phase, respectively, of core k and N is the normalization constant.

Having prepared the state, the measurements are performed in a similar fashion, using a second set of PMs, $DEMUX_2$ and MBS_1 [19]. The resulting unitary operation implemented is

$$U_M = \frac{1}{2}\begin{bmatrix} e^{i\phi_1^B} & e^{i\phi_1^B} & e^{i\phi_1^B} & e^{i\phi_1^B} \\ e^{i\phi_2^B} & e^{i\phi_2^B} & -e^{i\phi_2^B} & -e^{i\phi_2^B} \\ e^{i\phi_3^B} & -e^{i\phi_3^B} & e^{i\phi_3^B} & -e^{i\phi_3^B} \\ e^{i\phi_4^B} & -e^{i\phi_4^B} & -e^{i\phi_4^B} & e^{i\phi_4^B} \end{bmatrix}, \tag{9}$$

where ϕ_k^B is the phase applied in the core mode k at the measurement side. After applying the phases, we conclude the projective measurement using a final DEMUX (denoted $DEMUX_3$), to send the outcomes of MBS_1 to four single-photon detectors (SPD). The detectors are triggered commercial single-photon detection modules, configured with 5-ns detection gates and 10% of detection efficiency. The detection counts are recorded by the FPGA unit. The measurement corresponding to the above procedure is the rank-1 projective measurement given by the states

$$\begin{aligned} |\alpha_1\rangle &= \frac{1}{2}(e^{i\phi_1^B}|1\rangle + e^{i\phi_2^B}|2\rangle + e^{i\phi_3^B}|3\rangle + e^{i\phi_4^B}|4\rangle), \\ |\alpha_2\rangle &= \frac{1}{2}(e^{i\phi_1^B}|1\rangle + e^{i\phi_2^B}|2\rangle - e^{i\phi_3^B}|3\rangle - e^{i\phi_4^B}|4\rangle), \\ |\alpha_3\rangle &= \frac{1}{2}(e^{i\phi_1^B}|1\rangle - e^{i\phi_2^B}|2\rangle + e^{i\phi_3^B}|3\rangle - e^{i\phi_4^B}|4\rangle), \\ |\alpha_4\rangle &= \frac{1}{2}(e^{i\phi_1^B}|1\rangle - e^{i\phi_2^B}|2\rangle - e^{i\phi_3^B}|3\rangle + e^{i\phi_4^B}|4\rangle). \end{aligned} \tag{10}$$

That is, photon detection in path k corresponds to the measurement outcome associated with $|\alpha_k\rangle$.

Therefore, in our experiment, we can prepare the state of Eq. (8) and measure it in the basis defined by the

orthorgonal states of Eq. (10). The PMs, DEMUXs, and MBSs present an average insertion loss of 2.05 dB, 0.4 dB, and 0.2 dB, respectively, contributing to a total 3.66 dB of insertion loss for the entire measurement stage. Fiber-based polarization controllers (PCs) (not shown for the sake of simplicity) are used in each path to guarantee the indistinguishability of the core modes, such that there is no path information available to compromise the visibility of the interferometer [64,65]. These PCs are placed at the input of DEMUX_2 and are calibrated before each experimental round, keeping the polarization aligned for hours in the laboratory environment.

The most destructive disturbance in the setup is a time-dependent phase noise between the different arms of the interferometer, which arises due to thermal and mechanical fluctuations in the SMFs. For the preparation stage, the total applied phase is modeled considering that $\phi_k^A = \phi_k^n + \phi_k^c + \phi_k^s$. Here, ϕ_k^n represents the phase noise, ϕ_k^c the phase-noise suppressor, which we control by a continuous low-speed voltage signal, and ϕ_k^s the phase used to prepare the desired state, which we control by a high-speed voltage. Both voltages are controlled by the FPGA unit through a power driver (for more details, see the Appendix). The phase noise is canceled out by controlling ϕ_k^c: a control algorithm in the FPGA sets $\tau_k = 1$ and $\phi_k^s = 0$, ideally preparing $|\chi^{\max}\rangle = \frac{1}{2}(|1\rangle + |2\rangle + |3\rangle + |4\rangle)$ and, simultaneously, sets $\phi_k^B = 0$, ideally measuring in the basis A of Eq. (12). With these settings, if the phase noise is null, the photon always arrives at SPD_1, that is, $p_1 = |\langle\alpha_1|\chi^{\max}\rangle|^2 = 1$. Similarly, by preparing the state $|\chi^{\min}\rangle = \frac{1}{2}(|1\rangle + |2\rangle - |3\rangle - |4\rangle)$, the expected probability of photon detection at SPD_1 is $p_1 = |\langle\alpha_1|\chi^{\min}\rangle|^2 = 0$. Therefore, we expect maximal counts for $|\chi^{\max}\rangle$ and minimal counts for $|\chi^{\min}\rangle$. By collecting data at SPD_1 for these two settings, we can calculated the setup visibility, defined as

$$V_{\mathrm{SPD}_1} = \frac{\mathrm{SC}^{\max}_{\mathrm{SDP}_1} - \mathrm{SC}^{\min}_{\mathrm{SDP}_1}}{\mathrm{SC}^{\max}_{\mathrm{SDP}_1} + \mathrm{SC}^{\min}_{\mathrm{SDP}_1}}, \tag{11}$$

where $\mathrm{SC}^{\max}_{\mathrm{SDP}_1}$ ($\mathrm{SC}^{\min}_{\mathrm{SDP}_1}$) is the number of accumulated single counts of SPD_1 given the state preparation $|\chi^{\max}\rangle$ ($|\chi^{\min}\rangle$). The algorithm sets a threshold visibility $V_{\mathrm{SPD}_1} = 99.7\%$ and adjusts the control phases ϕ_k^c until this threshold is achieved. This algorithm is known as *perturb and observe maximum power point tracking* [66]. Once the threshold is reached (corresponding to $\phi_k^c \approx -\phi_k^n$), the suppressor phase ϕ_k^c is held to begin the experimental round and the experiment is performed using the fast-switching phases ϕ_k^s and ϕ_k^B for preparing and measuring the states in the protocol, respectively. To maintain high optical quality, the system defines an interval of 0.1 s for the experimental data collection, after which it calibrates ϕ_k^c again to counteract the time-dependent phase noise. The FPGA unit controls and synchronizes the preparation and measurement stages, both working at a repetition rate of 2 MHz, achieving around 60 000 detections during a time interval of 1 s.

The measurements, which we aim to certify, correspond to a pair of MUBs, which we choose such that they can be implemented in our setup using only phase modulation, without the need for amplitude modulation. Specifically, the two bases $\{|a_i\rangle\}_{i=1}^4$ and $\{|b_j\rangle\}_{j=1}^4$ are given by the columns of the matrices

$$A = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \tag{12}$$

$$B = \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{13}$$

According to Eq. (9), A can be performed by setting the phases $\phi_k^B = 0$ for all $k = 1,2,3,4$, while B can be performed by setting $\phi_1^B = \pi$ and keeping the other phases equal to zero. In the QRAC protocol described above, Bob chooses the measurement basis A or B according to his input y. In our experiment, we perform this basis choice simply by changing ϕ_1^B: when $y = 1$, we choose $\phi_1^B = 0$ and when $y = 2$, we choose $\phi_1^B = \pi$.

The optimal state preparation for Alice's input i,j is the pure state [25]:

$$|\psi_{ij}\rangle = \frac{1}{\sqrt{3}}[|a_i\rangle + \mathrm{sgn}\left(\langle a_i|b_j\rangle\right)|b_j\rangle], \tag{14}$$

which we can produce according to Eq. (8). The QRAC protocol is then carried out by randomly preparing the 16 different states $|\psi_{ij}\rangle$ with $i,j \in \{1,2,3,4\}$, randomly measuring them in the bases A or B and collecting the measurement statistics to estimate the average success probability in Eq. (2). The choices of states and measurements are implemented directly in the FPGA by resorting to a pseudorandom-number-generation algorithm.

V. RESULTS

We present the recorded experimental data in two parts, corresponding to the success probabilities related to the measurements A and B of Eq. (2). In the experiment, data are accumulated over 565 s, recording a total of 32 628 502 detections, with an average experimental detection rate of 57 883 detections per second. Figure 3(a) contains the outcome probabilities for the interferometer's outcomes 1, 2, 3, and 4 for each state $|\psi_{ij}\rangle$ upon measuring A. In Fig.

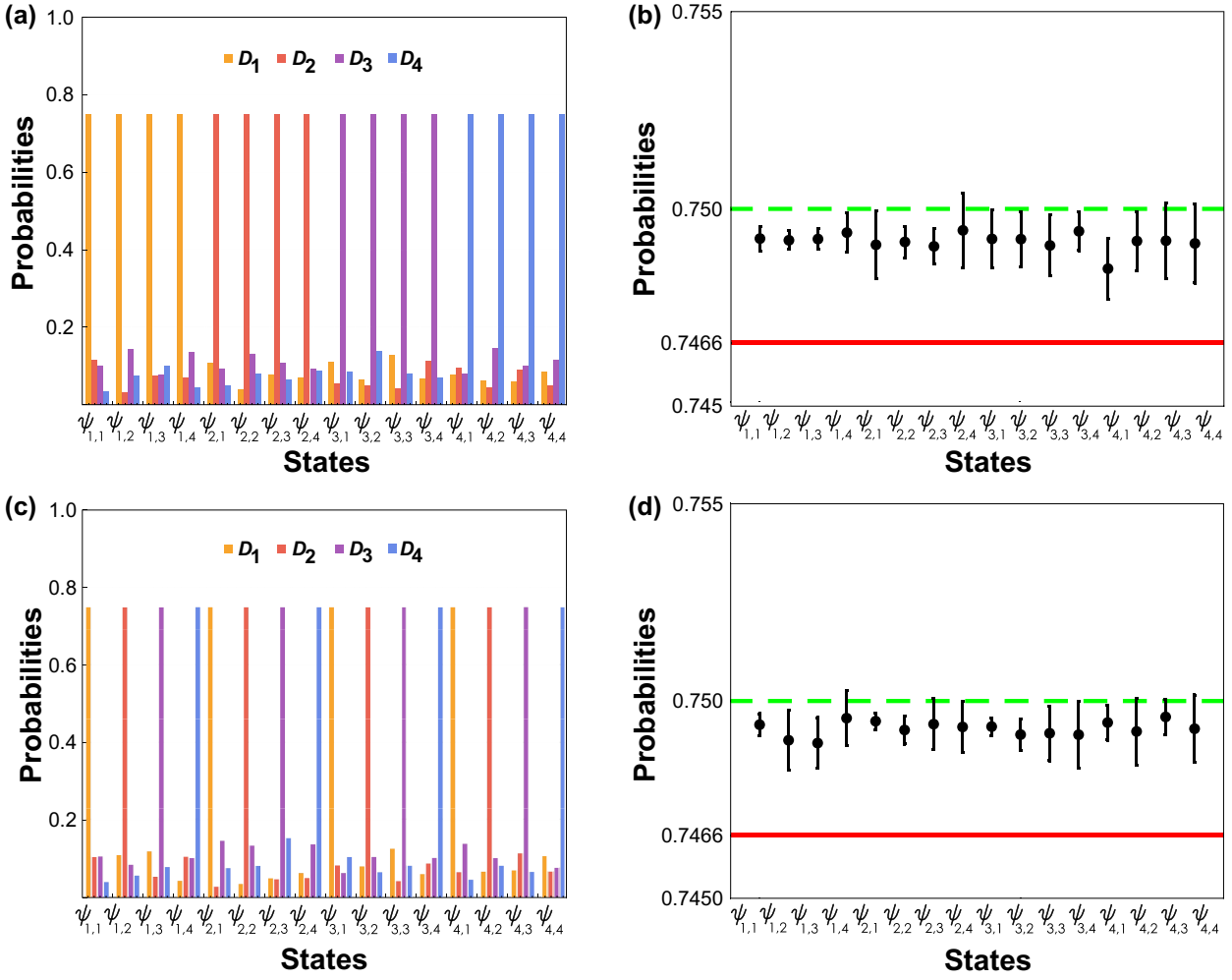

FIG. 3. (a),(c) The outcome probabilities of the measurements A and B, respectively, for each state $|\psi_{ij}\rangle$. (b),(d) The ASP for each state $|\psi_{ij}\rangle$ upon measuring A and B, respectively. The green line corresponds to the optimal ASP $\bar{p} = 0.75$, while the red line corresponds to the minimal ASP such that the most demanding quantity, η^*, can be self-tested.

3(b), we show the ASP for each state $|\psi_{ij}\rangle$ upon measuring A. On average, we observe an ASP of $\bar{p}_A = 0.7491 \pm 0.0002$ for this measurement, where the error is calculated using the Poissonian distribution for the number of photon detections. The analogous data for the measurement B are depicted in Figs. 3(c) and 3(d), yielding an ASP of $\bar{p}_B = 0.7493 \pm 0.0001$ in this case.

Putting the above values together, the overall ASP is $\bar{p} = 0.7492 \pm 0.0001$. Using this result and Gaussian error propagation, from Eq. (3) we obtain that $H_S(A,B) \geq 3.991 \pm 0.001$. From Eq. (4), we obtain that $N(A) \geq 3.957 \pm 0.006$. These two results, together, self-test the fact that the measurements are close to a pair of MUBs [$H_S(A,B) = 4$ and $N(A) = 4$].

Concerning the operational quantities, from Eq. (5), we obtain $\eta^* \leq 0.80 \pm 0.01$. Therefore, we certify a nontrivial bound on the critical visibility of our measurements at which they become compatible. This confirms that the measurements used in the experiment are indeed incompatible and therefore will be useful in future Bell and steering experiments [58].

Lastly, from Eq. (6), we can bound the entropic uncertainty: $H(A)_\rho + H(B)_\rho \geq 1.25 \pm 0.05$. That is, we obtain a minimal entropy that can be extracted from the outcomes of our measurements on *any* quantum state. This can be used for secure random-number generation or quantum key distribution protocols.

VI. CONCLUSIONS

With the development of quantum technologies, there is a current need for certification schemes for preparing high-dimensional quantum states and measurements. Since self-testing methods in nonlocal scenarios are complicated both in theory and practice, recently proposed methods for self-testing quantum devices in the prepare-and-measure scenario become relevant. In this work, we

demonstrate the viability of adopting such type of protocols in higher dimensions to validate the proper functioning of quantum devices built with modern SDM technology. Specifically, we self-test the proper implementation of measurements corresponding to mutually unbiased bases in dimension $d = 4$. This technology can be scaled to perform quantum-information processing protocols up to dimension 32 [67–69].

Our results show that SDM is an advantageous platform for high-dimensional quantum-information processing, achieving an exceptionally high optical quality with visibilities greater than 99%. While experiments implementing the same protocol have previously been performed [31–33], our technique allows us not only to certify the quantum advantage in random access coding but to self-test the measurements under the dimension assumption, as well as to certify their level of incompatibility and the amount of randomness that can be extracted from their outcomes. These results are of practical relevance for future experiments relying on this technology, since mutually unbiased measurements lie at the core of several quantum-information protocols.

ACKNOWLEDGMENTS

This work was supported by the Fondo Nacional de Desarrollo Científico y Tecnológico (FONDECYT) under Grants No. 1190933 and No. 1200859 and by the National Agency of Research and Development (ANID) Millennium Science Initiative program ICN17_012. J.C. acknowledges support from ANID/REC/PAI77190088. M.F. acknowledges support from the Polish National Science Center (NCN), under Grant No. Sonata UMO-2014/14/E/ST2/00020, from the project of the Polish National Agency for Academic Exchange "International scholarship exchange of PhD candidates and academic staff," Project No. POWR.03.03.00-IP.08-00-P13/18, from the European Research Council (ERC) Advanced Grant (AdG) "Certification of quantum technologies" project (CERQUTE), from the Government of Spain (FIS2020-TRANQI and Severo Ochoa CEX2019-000910-S), and from the Fundació Cellex, Fundació Mir-Puig, Generalitat de Catalunya (CERCA, AGAUR SGR 1381).

APPENDIX: EXPERIMENTAL DETAILS OF THE INNER WORKING OF THE FPGA

The FPGA electronic unit used in our experiment is based on the scheme shown in Fig. 4. Inside the FPGA, there are the following six main modules: the central processing unit (CPU), detection control (DC), phase-noise control (PNC), the preparation stage (PS), the measurement stage (MS), and a pseudorandom-number generator (RNG). The CPU module connects the FPGA unit with the user, synchronizes all internal modules (including a trigger for the single-photon source), controls the PNC

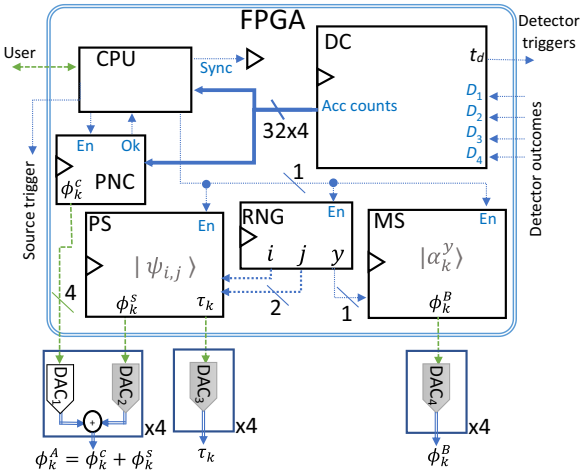

FIG. 4. The electronic diagram inside the FPGA.

module process, and executes the QRAC protocol. The RNG module is configured to randomly select the values of the three variables, i, j, and y, from a preset pseudorandom sequence. Note that the variables i and j are two bits each, while y is a single bit. The variables i and j are used by the PS module to prepare the desired state, while the MS module uses the variable y to select the corresponding measurement basis. The DC module synchronizes the four SPDs with the trigger signal, records their detection counts, and saves these data in four registers of 32 bits. The experimental probabilities are calculated from these data and they also provide the probability p_1 to the PNC module. The PNC module then uses these data to disturb the control phases ϕ_k^c [66].

As described in the main text, if the visibility is greater than a threshold, the phase-noise control (ϕ_k^c) is fixed to the values found and then the PS and MS modules are enabled. These modules prepare the required phases and transmissions based on the three variables (i, j, and y) that correspond to preset voltages to prepare the state and measurement basis needed in this protocol. The modules work at a repetition rate of 2 MHz. After 0.1 s of experimental run, the PS and MS modules are disabled in order for the PNC module to check visibility again.

The digital signals from the FPGA unit are converted using two different digital-to-analog converters (DACs) (see Fig. 4). Here, DAC_1 is 12-bits serial and the others are 4-bits parallel for high speeds. Note that four drivers are required for each set of phases (ϕ_k^A and ϕ_k^B) and transmissions (τ_k).

[1] P. W. Shor, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (IEEE, Santa Fe, NM, USA, 1994), p. 124.

[2] R. P. Feynman, Simulating physics with computers, Int. J. Theor. Phys. **21**, 467 (1982).

[3] C. H. Bennett and G. Brassard, in *Proceedings Of The IEEE International Conference On Computers, Systems And Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[4] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[5] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[6] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **105**, 230501 (2010).

[7] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Device-Independent Witnesses of Genuine Multipartite Entanglement, Phys. Rev. Lett. **106**, 250404 (2011).

[8] R. Rabelo, L. Y. Zhi, and V. Scarani, Device-Independent Bounds for Hardy's Experiment, Phys. Rev. Lett. **109**, 180401 (2012).

[9] T. H. Yang and M. Navascués, Robust self-testing of unknown quantum systems into any entangled two-qubit states, Phys. Rev. A **87**, 050102(R) (2013).

[10] M. Ho, J.-D. Bancal, and V. Scarani, Device-independent certification of the teleportation of a qubit, Phys. Rev. A **88**, 052318 (2013).

[11] E. S. Gómez, S. Gómez, P. González, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi, and G. Lima, Device-Independent Certification of a Nonprojective Qubit Measurement, Phys. Rev. Lett. **117**, 260401 (2016).

[12] S. Gómez, A. Mattar, I. Machuca, E. S. Gómez, D. Cavalcanti, O. J. Farías, A. Acín, and G. Lima, Experimental investigation of partially entangled states for device-independent randomness generation and self-testing protocols, Phys. Rev. A **99**, 032108 (2019).

[13] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, Quantum **4**, 337 (2020).

[14] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems, Quantum **3**, 198 (2019).

[15] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, Self-testing quantum systems of arbitrary local dimension with minimal number of measurements, arXiv:1909.12722 (2019).

[16] 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 (2000).

[17] M. Araújo, F. Costa, and Č. Brukner, Computational Advantage from Quantum-Controlled Ordering of Gates, Phys. Rev. Lett. **113**, 250402 (2014).

[18] 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).

[19] J. Cariñe, G. Cañas, P. Skrzypczyk, I. Šupić, N. Guerrero, T. Garcia, L. Pereira, M. A. S. Prosser, G. B. Xavier, A. Delgado, S. P. Walborn, D. Cavalcanti, and G. Lima, Multi-core fiber integrated multi-port beam splitters for quantum information processing, Optica **7**, 542 (2020).

[20] 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).

[21] 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).

[22] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Experimental estimation of the dimension of classical and quantum systems, Nat. Phys. **8**, 588 (2012).

[23] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Experimental device-independent tests of classical and quantum dimensions, Nat. Phys. **8**, 592 (2012).

[24] V. D'Ambrosio, F. Bisesto, F. Sciarrino, J. F. Barra, G. Lima, and A. Cabello, Device-Independent Certification of High-Dimensional Quantum Systems, Phys. Rev. Lett. **112**, 140503 (2014).

[25] M. Farkas and J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, Phys. Rev. A **99**, 032316 (2019).

[26] I. D. Ivanovic, Geometrical description of quantal state determination, J. Phys. A: Math. Gen. **14**, 3241 (1981).

[27] G. Lima, L. Neves, R. Guzmán, E. S. Gómez, W. A. T. Nogueira, A. Delgado, A. Vargas, and C. Saavedra, Experimental quantum tomography of photonic qudits via mutually unbiased basis, Opt. Express **19**, 3542 (2011).

[28] H. Maassen and J. B. M. Uffink, Generalized Entropic Uncertainty Relations, Phys. Rev. Lett. **60**, 1103 (1988).

[29] T. Durt, B. Englert, I. Bengtsson, and K. Życzkowski, On mutually unbiased bases, Int. J. Quantum Inf. **8**, 535 (2010).

[30] G. B. Xavier and G. Lima, Quantum information processing with space-division multiplexing optical fibres, Commun. Phys. **3**, 9 (2020).

[31] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Single d-Level Systems, Phys. Rev. Lett. **114**, 170502 (2015).

[32] M. J. Kewming, S. Shrapnel, A. G. White, and J. Romero, Hiding Ignorance Using High Dimensions, Phys. Rev. Lett. **124**, 250401 (2020).

[33] 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).

[34] P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, M. Pawłowski, and M. Bourennane, Increased certification of semi-device independent random numbers using many inputs and more post- processing, New J. Phys. **18**, 065004 (2016).

[35] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).

[36] T. Heinosaari, J. Kiukas, and D. Reitzner, Noise robustness of the incompatibility of quantum measurements, Phys. Rev. A **92**, 022115 (2015).

[37] M. T. Quintino, T. Vértesi, and N. Brunner, Joint Measurability, Einstein-Podolsky-Rosen Steering, and Bell Nonlocality, Phys. Rev. Lett. **113**, 160402 (2014).

[38] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, Rev. Mod. Phys. **89**, 015002 (2017).

[39] Z. Pan, K.-K. Wong, and T.-S. Ng, Generalized multiuser orthogonal space-division multiplexing, IEEE Trans. Wireless Commun. **3**, 1969 (2004).

[40] D. J. Richardson, J. M. Fini, and L. E. Nelson, Space-division multiplexing in optical fibres, Nat. Photonics **7**, 354 (2013).

[41] P. Sillard, M. Bigot-Astruc, and D. Molin, Few-mode fibers for mode-division-multiplexed systems, J. Lightwave Technol. **32**, 2824 (2014).

[42] G. Rademacher, R. S. Luís, B. J. Puttnam, T. A. Eriksson, R. Ryf, E. Agrell, R. Maruyama, K. Aikawa, Y. Awaji, H. Furukawa, and N. Wada, High capacity transmission with few-mode fibers, J. Lightwave Technol. **37**, 425 (2019).

[43] K. Kitayama and N. Diamantopoulos, Few-mode optical fibers: Original motivation and recent progress, IEEE Commun. Mag. **55**, 163 (2017).

[44] 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).

[45] S. Inao, T. Sato, S. Sentsui, T. Kuroha, and Y. Nishimura, in *Optical Fiber Communication*, 1979 OSA Technical Digest Series (Optical Society of America, Washington, D.C., 1979), paper WB1.

[46] K. Saitoh and S. Matsuo, Multicore fiber technology, J. Lightwave Technol. **34**, 55 (2016).

[47] 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 (2018).

[48] T. A. Birks, I. Gris-Sánchez, S. Yerolatsitis, S. G. Leon-Saval, and R. R. Thomson, The photonic lantern, Adv. Opt. Photon. **7**, 107 (2015).

[49] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, Efficient Sorting of Orbital Angular Momentum States of Light, Phys. Rev. Lett. **105**, 153601 (2010).

[50] X. Zeng, Y. Li, L. Feng, S. Wu, C. Yang, W. Li, W. Tong, and J. Wu, All-fiber orbital angular momentum mode multiplexer based on a mode-selective photonic lantern and a mode polarization controller, Opt. Lett. **43**, 4779 (2018).

[51] K. Watanabe, T. Saito, K. Imamura, and M. Shiino, in *2012 17th Opto-Electronics and Communications Conference* (IEEE, Busan, 2012), p. 475.

[52] Y. Tottori, T. Kobayashi, and M. Watanabe, Low loss optical connection module for seven-core multicore fiber and seven single-mode fibers, IEEE Photonics Technol. Lett. **24**, 1926 (2012).

[53] 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 Photonics J. **8**, 1 (2016).

[54] 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 (2016).

[55] 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. F. da Silva, G. B. Xavier, and G. Lima, High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers, Phys. Rev. A **96**, 022317 (2017).

[56] 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).

[57] 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).

[58] E. S. Gómez, S. Gómez, I. Machuca, A. Cabello, S. Pádua, S. P. Walborn, and G. Lima, Multi-dimensional entanglement generation with multi-core optical fibers, arXiv:2005.07847 (2020).

[59] L. Cui, J. Su, X. Li, and Z. Y. Ou, Distribution of entangled photon pairs over few-mode fibers, Sci. Rep. **7**, 14954 (2017).

[60] A. Sit, R. Fickler, F. Alsaiari, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, and E. Karimi, Quantum cryptography with structured photons through a vortex fiber, Opt. Lett. **43**, 4108 (2018).

[61] H. Cao, S.-C. Gao, C. Zhang, J. Wang, D.-Y. He, B.-H. Liu, Z.-W. Zhou, Y.-J. Chen, Z.-H. Li, S.-Y. Yu, J. Romero, Y.-F. Huang, C.-F. Li, and G.-C. Guo, Distribution of high-dimensional orbital angular momentum entanglement over a 1 km few-mode fiber, Optica **7**, 232 (2020).

[62] D. Cozzolino, E. Polino, M. Valeri, G. Carvacho, D. Bacco, N. Spagnolo, L. K. K. Oxenløwe, and F. Sciarrino, Air-core fiber distribution of hybrid vector vortex-polarization entangled states, Adv. Photonics **1**, 046005 (2019).

[63] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[64] S. P. Walborn, M. O. Terra Cunha, S. Pádua, and C. H. Monken, Double-slit quantum eraser, Phys. Rev. A **65**, 033818 (2002).

[65] F. A. Torres-Ruiz, G. Lima, A. Delgado, S. Pádua, and C. Saavedra, Decoherence in a double-slit quantum eraser, Phys. Rev. A **81**, 042104 (2010).

[66] W. Liu, C. Liu, L. Ma, Y. Lin, and J. Ma, Maximum power point tracking of photovoltaic generation based on forecasting model, J. Softw. **8**, 2569 (2013).

[67] K. Takenaga, S. Matsuo, K. Saitoh, T. Morioka, and Y. Miyamoto, in *Optical Fiber Communications Conference and Exhibition (OFC)* (Optical Society of America, Anaheim, CA, 2016), p. 1.

[68] B. J. Puttnam, R. S. Luís, G. Rademacher, A. Alfredsson, W. Klaus, J. Sakaguchi, Y. Awaji, E. Agrell, and N. Wada, Characteristics of homogeneous multi-core fibers for SDM transmission, APL Photonics **4**, 022804 (2019).

[69] T. Mizuno, K. Shibahara, F. Ye, Y. Sasaki, Y. Amma, K. Takenaga, Y. Jung, K. Pulverer, H. Ono, Y. Abe, M. Yamada, K. Saitoh, S. Matsuo, K. Aikawa, M. Bohn, D. J. Richardson, Y. Miyamoto, and T. Morioka, Long-haul dense space-division multiplexed transmission over low-crosstalk heterogeneous 32-core transmission line using a partial recirculating loop system, J. Lightwave Technol. **35**, 488 (2017).

Appendix B

Computational Advantage from the Quantum Superposition of Multiple Temporal Orders of Photonic Gates [42].

Computational Advantage from the Quantum Superposition of Multiple Temporal Orders of Photonic Gates

Márcio M. Taddei,[1,2,*] Jaime Cariñe,[3,4,5] Daniel Martínez,[3,4] Tania García,[3,4] Nayda Guerrero,[3,4] Alastair A. Abbott,[6,7] Mateus Araújo,[8] Cyril Branciard,[9] Esteban S. Gómez,[3] Stephen P. Walborn,[3,4] Leandro Aolita,[1,10] and Gustavo Lima[3,4]

[1] *Instituto de Física, Federal University of Rio de Janeiro, P. O. Box 68528, Rio de Janeiro 21941-972, Brazil*

[2] *ICFO – Institut de Ciencies Fotòniques, The Barcelona Institute of Science and Technology, Castelldefels, Barcelona 08860, Spain*

[3] *Departamento de Física, Universidad de Concepción, Concepción 160-C, Chile*

[4] *ANID – Millennium Science Initiative Program – Millennium Institute for Research in Optics, Universidad de Concepción, Concepción 160-C, Chile*

[5] *Departamento de Ingeniería Eléctrica, Universidad Católica de la Santísima Concepción, Alonso de Ribera 2850, Concepción, Chile*

[6] *Department of Applied Physics, University of Geneva, Geneva 1211, Switzerland*

[7] *Univ. Grenoble Alpes, Inria, Grenoble 3800, France*

[8] *Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, Vienna 1090, Austria*

[9] *Univ. Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, Grenoble 38000, France*

[10] *Quantum Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates*

(Received 11 April 2020; revised 10 August 2020; accepted 12 January 2021; published 8 February 2021; corrected 31 March 2021)

Models for quantum computation with circuit connections subject to the quantum superposition principle have recently been proposed. In them, a control quantum system can coherently determine the order in which a target quantum system undergoes N gate operations. This process, known as the quantum N-switch, is a resource for several information-processing tasks. In particular, it provides a computational advantage—over fixed-gate-order quantum circuits—for phase-estimation problems involving N unknown unitary gates. However, the corresponding algorithm requires an experimentally unfeasible target-system dimension (super)exponential in N. Here, we introduce a promise problem for which the quantum N-switch gives an equivalent computational speedup with target-system dimension as small as 2 regardless of N. We use state-of-the-art multicore optical-fiber technology to experimentally demonstrate the quantum N-switch with $N = 4$ gates acting on a photonic-polarization qubit. This is the first observation of a quantum superposition of more than $N = 2$ temporal orders, demonstrating its usefulness for efficient phase estimation.

DOI: 10.1103/PRXQuantum.2.010320

I. INTRODUCTION

Quantum mechanics allows for processes where two or more events take place in a quantum superposition of different temporal orders. This exotic phenomenon results in causal nonseparability [1–3], and it is likely to be especially relevant in quantum treatments of gravity [4–6]. In fact, quantum control of temporal orders could be realized with quantum circuits exploiting hypothetical closed timelike curves [7,8], and it would also arise naturally due to the spacetime warping that macroscopic spatial superpositions of massive bodies would cause [9].

From a more practical perspective, advanced quantum computational models without definite gate orders have sparked a great deal of fundamental interest, as they do not fit into the usual paradigm of circuits with fixed gate connections [6,7,10–13]. The best-known example is the celebrated quantum N-switch gate S_N, which coherently applies a different permutation of N given gates on a target quantum system conditioned on the state of a control quantum system [7,13,14]. The quantum N-switch

*marciotaddei@gmail.com

has been identified as a resource for a number of exciting information-theoretic tasks. For instance, for $N = 2$, it allows one to deterministically distinguish pairs of commuting versus anticommuting unitaries [12]; remarkably, this translates into an exponential advantage in a communication complexity problem [15,16].

In general, circuits that synthesize S_N with a fixed gate order are known, but at the expense of quadratically more queries to (i.e., uses of) the gates [12–14,17]. As a consequence thereof, S_N allows one to solve a promise problem [12,14] on the permutations of N unknown unitary gates with quadratically fewer queries in N than all known circuits with fixed gate order. More precisely, the permutation sequences of the gates are promised to differ only by a phase factor, and S_N efficiently estimates these phase differences. However, the algorithm for this problem [12,14] requires the target-system dimension to grow (super)exponentially with N, making it experimentally demanding. In fact, all experimental realizations of the quantum N-switch reported so far are restricted to the simplest case of $N = 2$ gate orders [16,18–22].

In this work, we introduce a novel algorithm that exploits the quantum N-switch and experimentally demonstrate it for $N = 4$ unitary gates. Specifically, we find a variant of the above phase-estimation problem, which we name the Hadamard promise problem, for which the quantum N-switch is also a resource but with considerably milder constraints on the target-system dimension. On the one hand, this problem plays a role in computation with indefinite gate orders analogous to Deutsch-Jozsa's [23] or Simon's [24] problems in the beginnings of quantum computation: a proof of principle of improvements over a previous paradigm. On the other hand, there are reasons to expect that practical applications of the Hadamard promise problem will be developed, both because closely related phase-estimation problems already have many applications, and because it involves the quantum Fourier transform, which is an important subroutine for a variety of quantum algorithms with practical applications [25]. The problem's promise is that the products of the N unknown gates applied in P different orders differ only in $+$ or $-$ signs that are encoded into one of the columns of a given $(P\times P)$-dimensional Hadamard matrix; the problem consists of finding which column it is.

The algorithm to solve this problem exploits the quantum N-switch—consuming N queries to the gates—to deterministically find the column. This represents a speedup quadratic in N in query complexity (i.e., number of queries) with respect to all known algorithms exploiting circuits with fixed gate orders (see Refs. [14,26,27] for a discussion of how to count queries in a quantum switch). Hence, the algorithm is not only an interesting computational primitive on its own but also a practical tool to benchmark experimental realizations of S_N, because the quantum N-switch is the only known process for which the algorithm succeeds with unit probability for all gates satisfying the promise while only consuming N gate queries. To demonstrate the practicability of the algorithm, we implement it with a quantum N-switch of $N = 4$ gates using modern multicore optical-fiber technology [28–31]. The four gates are implemented on the target polarization qubits using programmable liquid-crystal devices, and the spatial degree of freedom of a single photon is used as the control system. We obtain an average success probability for the algorithm, over different sets of gates, of $p_{succ} \approx 0.95$. Our results represent the first demonstration of the quantum N-switch gate for N larger than 2, as well as of its efficiency for phase-estimation problems involving multiple unknown gates.

II. PRELIMINARIES

A. Quantum control of gate orders

In quantum computation, a quantum switch can be described by a special type of controlled operation that applies a particular unitary gate Π_x to a target system (t) for each different state of a control system (c). We define the quantum N-switch gate as

$$S_N \left|x\right\rangle_c \left|\Psi\right\rangle_t = \left|x\right\rangle_c \Pi_x \left|\Psi\right\rangle_t , \tag{1}$$

where $|x\rangle_c$ is the xth member of the computational basis of the control system and $|\Psi\rangle_t$ is an arbitrary state of the target system. The heart of the quantum N-switch is the operator $\Pi_x := U_{\sigma_x(N-1)} \cdots U_{\sigma_x(1)} U_{\sigma_x(0)}$, which is a product of the N unitary gates in a fixed set $\mathsf{U} := \{U_A, U_B, \ldots\}$ in their xth ordering. More precisely, σ_x is a vector with N elements specifying the xth permutation of the N gates in U, i.e., it specifies the ordering sequence of the unitaries, so that $\sigma_x(j)$ is the jth element in the xth permutation. To control the implementation of P, different permutations of gates requires a control system of at least dimension P. The dimension of the target system can be arbitrary and we denote it as d. With S_N defined as in Eq. (1), it is clear that c coherently controls the order of the N unitary gates applied to system t, which explains the name "quantum control of gate orders" (QCGO). We note that the usual definition [13,14] of the quantum N-switch deals only with the specific case of all $N!$ permutations of the gates in U. However, here (as in Refs. [32,33]) we are interested in the more general case $P \leq N!$.

Clearly, the general definition of QCGO is independent of the specific choice of gates in U. A convenient mathematical tool to capture that is the quantum N-switch process W_N, which produces the quantum N-switch gate S_N when given the set of gates U as input. For the technical definition of processes, we refer the reader to Refs. [1–3,34]. Intuitively, one can think of a process as the quantum evolution generated by an experimental arrangement with open slots for gates on the

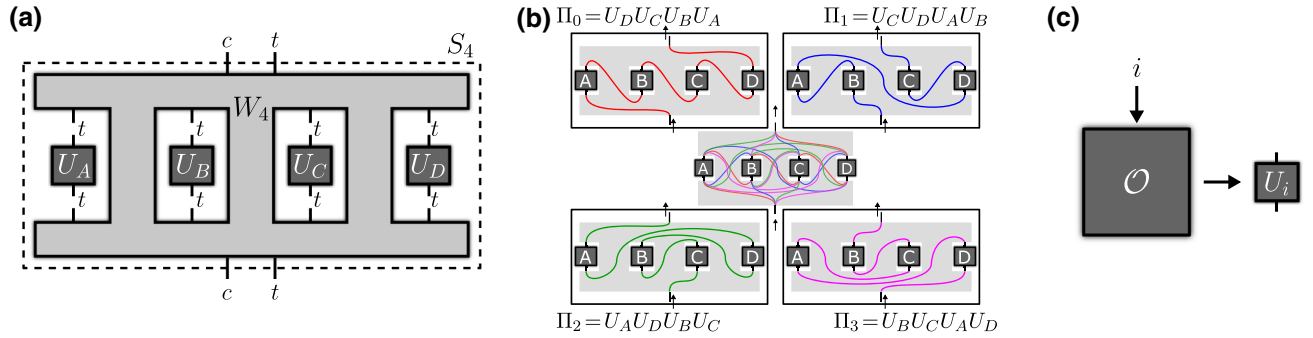

FIG. 1. (a) Abstract representation of the quantum N-switch for the case of $N = 4$. The process, W_4 (light-gray region), can be thought of as an experimental setup (e.g., a quantum circuit or interferometer) through which the composite control-target system goes and with open slots for target-subsystem gates U_i (dark-gray boxes) for $i = A$, B, C, or D to be inserted. Inside W_4, the connections between these gates are coherently controlled by the control subsystem, an effect known as quantum control of gate orders. This property is a physical resource for certain quantum computations (phase-estimation problems), and W_4 is the resourceful object that bears it. The concatenation of W_4 with the inserted gates yields the quantum 4-switch gate S_4, a joint unitary operation on the composite system. (b) Concrete schematics of the specific variant of the quantum 4-switch process experimentally implemented in this work. The target subsystem undergoes the four-gate sequence in a quantum superposition (center) of $P = 4$ different orderings (permutations of the string $ABCD$): $ABCD, BADC, CBDA, DACB$. Each permutation is shown individually in a different color and panel. (c) In the abovementioned computations, the target-subsystem gates are unknown. For the purpose of complexity analysis, they can be thought of as produced upon request by a quantum oracle $\mathcal{O}$. This takes as input $i = A$, B, C, or D and outputs a black-box device implementing the unknown gate U_i. Each such call to the oracle counts as an oracle query. The N-switch process allows one to solve computational problems on the phase relationships between permutations of the black-box gates with considerably fewer oracle queries—i.e., lower query complexity—than any process with fixed (or classically controlled) gate connections.

target system to be inserted [10,11], as represented in Fig. 1(a). Inside the process, the connections between the inserted gates may be subject to the quantum superposition principle. For instance, in Fig. 1(b) we pictorially represent our experimental implementation of the quantum 4-switch gate S_4, with a coherent quantum superposition of $P = 4$ different gate connections (each one in a different color) for the particular choice of permutation set $\{ABCD, BADC, CBDA, DACB\}$. Such superpositions give rise to QCGO, which corresponds to a specific type of quantum control of causal orders [35] (and both phenomena are in turn contained within the general notion of causal nonseparability [1–3]). In particular, QCGO takes place when those gate connections are coherently controlled by a control system, as in Eq. (1). Aside from being a fundamentally interesting phenomenon, QCGO turns out to be a physical resource for interesting phase-estimation problems, as we discuss next.

B. The Araújo-Costa-Brukner algorithm

The quantum N-switch process provides an advantage for solving a particular phase-estimation problem [12,14] to which we here refer as the Fourier promise problem. In this type of problem, one has access to a quantum oracle $\mathcal{O}$ for U, i.e., a black-box device that delivers a gate $U_i \in \mathsf{U}$ every time it is queried. See Fig. 1(c). No information about the gates is available except for the promise that, for the constant phase factor $\omega := e^{i2\pi/P}$ and all $x \in [P]$, they satisfy the property that

$$\Pi_x = \omega^{xy} \Pi_0 \tag{2}$$

for some fixed, unknown $y \in [P]$, where the shorthand notation $[P] := \{0, 1, \ldots, P-1\}$ has been introduced. The task is to determine which one of the properties holds, i.e., to find y.

The Araújo-Costa-Brukner algorithm to solve this problem is based on the standard Hadamard test [36], and shares similarities with the Kitaev phase-estimation algorithm [37]. The control system is initialized in the computational-basis reference state $|0\rangle_c$, while the target system starts in an arbitrary state $|\Psi\rangle_t$. A P-dimensional quantum Fourier transform F_P on c maps it to a uniform superposition of all computational-basis states. Then, the quantum N-switch gate is applied. Because of property (2), this introduces the phase factor ω^{xy} to each computational-basis state $|x\rangle_c$ in the superposition, while the state $\Pi_0 |\Psi\rangle_t$ of the target system factorizes. The value of y is thus encoded into the phases of the superposition state of the control system. To map it back to the computational basis, one uncomputes the Fourier transform (applying its inverse $F_P^{-1} = F_P^\dagger$). In symbols [14],

$$F_P^{-1} S_N F_P |0\rangle_c |\Psi\rangle_t = |y\rangle_c \Pi_0 |\Psi\rangle_t . \tag{3}$$

Then, y is finally read out by a single-shot computational-basis measurement on c.

To apply S_N, one must consume N queries to $\mathcal{O}$. Therefore, the query complexity—i.e., total number of oracle queries—of the algorithm is $Q = N$ for all $P \leq N!$. Remarkably, causally ordered processes (i.e., those produced by circuits with fixed, or classically controlled, gate connections) require considerably more queries to solve the same problem. For instance, for $P = N!$, the best causally ordered process displays query complexity $Q = \Omega(N^2)$ [13,14,17], i.e., quadratically higher in N. A downside of the algorithm, however, is that the target-system dimension d must grow with the number P of gate orders. This can be seen [14] by taking the determinant of both sides of Eq. (2). For $y = 1$, and since $\det \Pi_x = \det \Pi_0$, this imposes $\det \Pi_0 = \omega^{xd} \det \Pi_0$ (and, hence, $1 = e^{i2\pi xd/P}$) for all $x \in [P]$, which is possible only if $d \geq P$. This constraint is especially significant for experimental realizations, where coherently manipulating high-dimensional target systems together with high-dimensional control systems is challenging [16]. For example, this limitation implies that, if the polarization of a single photon ($d = 2$) is used as the target system, the algorithm is useful only for $P = 2$, despite the fact that the spatial degree of freedom of the photon is amenable to encode much higher-dimensional control systems [38]. To overcome this, we next introduce another variant of the phase-estimation problem that is considerably less sensitive to the determinant constraint.

III. A NEW COMPUTATIONAL PRIMITIVE: THE HADAMARD PROMISE PROBLEM

We consider a different promise on the gates that the oracle $\mathcal{O}$ outputs. Given a known $(P\times P)$-dimensional square matrix M_P of entries $m_{x,y} = \pm 1$, we require that the black-box unitaries in U satisfy, for all $x \in [P]$, the property that

$$\Pi_x = m_{x,y} \Pi_0 \tag{4}$$

for some fixed, *a priori* unknown matrix column $y \in [P]$. The task is, again, to find y. In contrast to the complex-phase relation of Eq. (2), the constraint that this real-phase relation imposes on d is much softer. As one can see taking the determinant of both sides of Eq. (4), the only requirement that arises now is that $(m_{x,y})^d = 1$ for all $x, y \in [P]$, which is satisfied by any even d. With this, the promise problem finds application even when the target system is a simple qubit, regardless of the number of permutations P. Instead of a single complex phase factor, the value of y is now encoded in a string of P real phase factors (i.e., a column of M_P). The question, then, is how to decode that information. Luckily, the value of y can be mapped back onto the computational basis of c with a simple procedure, similar to that in Eq. (3), provided that M_P is a *Hadamard matrix* [36].

A Hadamard matrix (of order P) is a $(P\times P)$-dimensional square matrix M_P with entries $m_{x,y} = \pm 1$ and whose columns (or, equivalently, whose rows) are all mutually orthogonal. The transpose M_P^T of M_P is proportional to its inverse: $(1/P) M_P \cdot M_P^\mathsf{T} = \mathbb{1}$, with $\mathbb{1}$ the identity matrix. Such matrices can only exist for P equal to 1, 2, or integer multiples of 4, and are conjectured to exist for all such dimensions. In fact, they can be generated recursively for any $P = 2^k$ with $k \in \mathbb{N}$. Here we are actually interested in the subset of Hadamard matrices with all $+1$s in the first row ($x = 0$) and column ($y = 0$). The former condition is required by Eq. (4), whereas the latter condition is necessary in our algorithm below for correct encoding (see Appendix A 1 for details). With this, we can formally rephrase this promise problem as follows.

Problem 1 (Hadamard promise problem). *Given a Hadamard matrix M_P with all $+1$ entries along its first row and column and a unitary-gate oracle $\mathcal{O}$ fulfilling the promise, i.e., Eq. (4) for some column $y \in [P]$ of M_P, compute y.*

The algorithm to solve it with the quantum N-switch gate is similar to the Araújo-Costa-Brukner algorithm but with the quantum Hadamard gate H_P associated to M_P playing the role of F_P. The matrix representation of H_P in the computational basis is $H_P := M_P/\sqrt{P}$. Then, the following algorithm solves Problem 1.

Algorithm 1. *Initialize the joint system in the state $|0\rangle_c |\Psi\rangle_t$, with $|\Psi\rangle_t$ an arbitrary target state. Then, apply H_P on c. Then, apply S_N on the joint control-target system. Then, apply $H_P^{-1} (= H_P^\mathsf{T})$ on c. This gives the state*

$$H_P^{-1} S_N H_P |0\rangle_c |\Psi\rangle_t = |y\rangle_c \Pi_0 |\Psi\rangle_t . \tag{5}$$

Finally, read out y as the outcome of a single-shot computational-basis measurement on c.

This algorithm thus provides the desired phase relation between the P different permutations of the N unknown unitaries under consideration. The validity of Eq. (5) is proven explicitly in Appendix A 1. The query complexity of the algorithm is the same as that of the Araújo-Costa-Brukner algorithm: $Q = N$ for all $P \leq N!$. The crucial resource for Algorithm III is the quantum N-switch process. Similarly to the Fourier promise problem [14], no causally ordered process is known to solve Problem 1 in general (i.e., for any arbitrary set U of unknown gates fulfilling the promise) with a query complexity linear in N. In fact, the (querywise) optimal causally ordered processes known to solve the problem in general are simply the fixed-gate circuits that simulate the quantum N-switch exactly (see Sec. VII), but these require considerably more queries [13,14,17]. For instance, in the case where all gate permutations are considered ($P = N!$), simulating the quantum N-switch exactly in the black-box

scenario requires $Q = \Omega(N^2)$ oracle queries, i.e., quadratically higher in N. Another concrete example is the quantum 4-switch process for the $P = 4$ permutations in the set $\{ABCD, BADC, CBDA, DACB\}$ [shown in Fig. 1(b)], whose experimental implementation we describe below. The optimal circuit to simulate it exactly in the black-box scenario requires $Q = 9$ oracle queries, i.e., more than twice as many as with S_4 (see Appendix A 2).

IV. EXPERIMENTAL QUANTUM CONTROL OF THE ORDER OF MULTIPLE GATE OPERATIONS

The experiment is illustrated in Fig. 2(a). It is based on multicore optical fibers and new related technology [28], which was recently introduced as a toolbox for quantum information processing [29–31]. In our implementation of the quantum 4 switch, the control system corresponds to the spatial mode of a single photon, while the target is its polarization. Following Algorithm III, a conventional illumination scheme (see Sec. VII) is used to generate single photons propagating over a single-mode fiber in the initial spatial mode state $|0\rangle_c$. The photons are then sent through a 4CF-BS, which has been shown to realize with high fidelity the $H_4 = M_4/2$ Hadamard operation given by [39]

$$H_4 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}. \tag{6}$$

Note that this matrix is self-inverse. The 4CF-BS is placed between commercial spatial multiplexer/demultiplexer units [40,41], which couple four single-mode fibers (yellow fibers) to the four cores of the multicore fibers (green

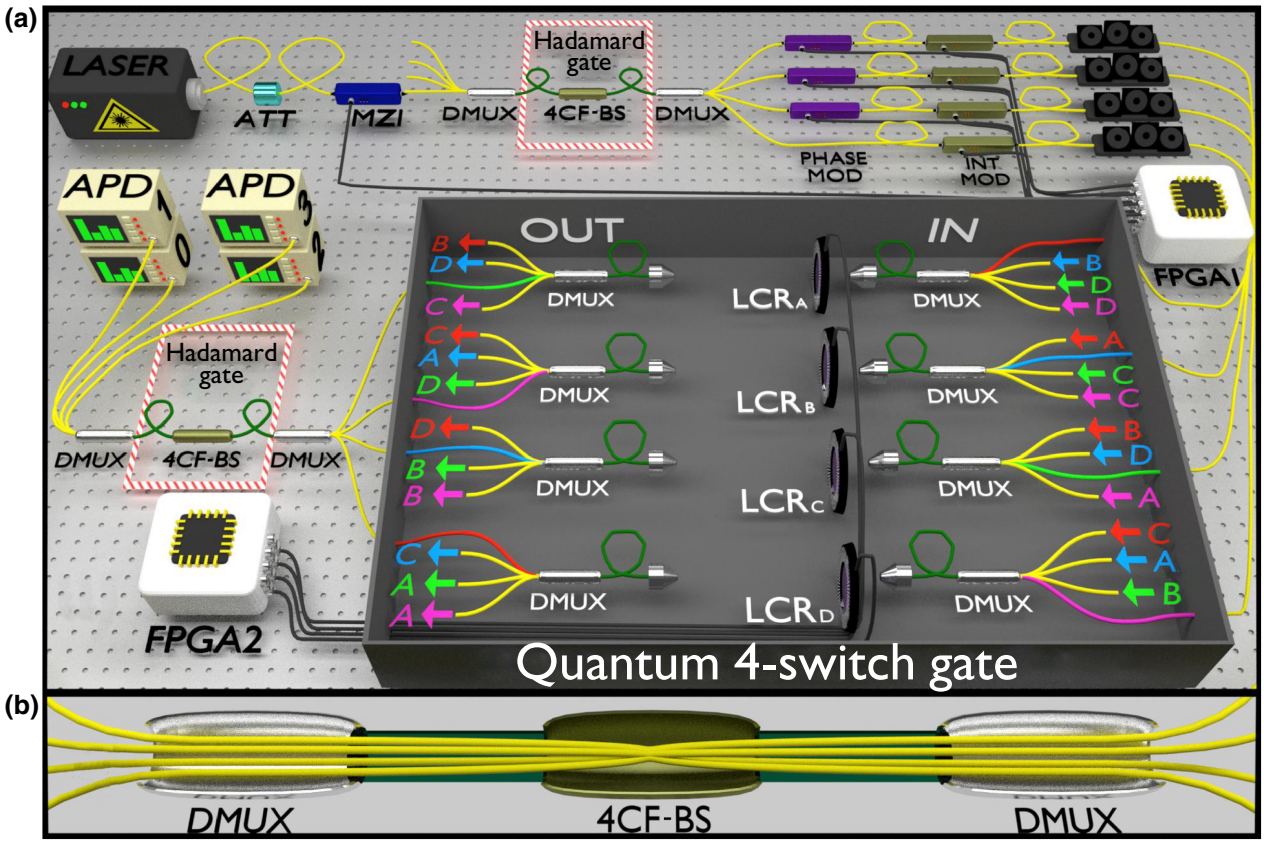

FIG. 2. (a) Illustration of our implementation of the quantum 4-switch gate (S_4). An input photon is divided coherently between four spatial modes using a four-core-fiber beam splitter (4CF-BS), placed between commercial multiplexer/demultiplexer (DMUX) units, as shown in (b). The four output modes are then sent to the quantum 4-switch gate S_4. Each spatial mode is related to a unique permutation of the four unitary polarization operations applied by S_4 and indicated by a different color. The photons enter through the IN side (right) and exit through the OUT side (left), where, for example, the notation "$\leftarrow A$" means "from A" and "$A \leftarrow$" means "to A." One can follow a certain path by looking at the output labels. For instance, the green input mode enters in C and continues to "B, then D, then A, and finally exits," corresponding to the operation of the four polarization unitaries in the order $CBDA$. After S_4, the four spatial modes are then recombined using a second 4CF-BS. Each output 0–3 is connected directly to a single-photon detector (APD). The detection of a single-photon in the yth ($y = 0, 1, 2, 3$) output detector identifies in a single shot the phase relation y of the four unitaries implemented in the quantum 4-switch gate. See the main text and Sec. VII for further details.

fibers). These units connect to the 4CF-BS through the multicore fibers [see the details in Fig. 2(b)].

After transmission through the 4CF-BS, the photon is sent to the quantum 4-switch gate S_4, which will coherently apply different permutations of four unitary operations U_i on the target system (photon polarization), depending on the spatial mode. To see this, note that each output of the 4CF-BS routes the photon through a different ordering of the polarization operations U_i, which are realized with controllable liquid crystal retarders (LCRs). To control the implementation order of the U_i, we take advantage of the DMUX units. Each single-mode fiber input to the quantum 4-switch gate is connected to a different four-core fiber on the IN side of S_4 using a DMUX unit. The other end of each 4CF is attached to a fiber launcher. The photon leaves the launcher in free space passing through the LCR and is coupled back into another 4CF on the OUT side. The OUT 4CF is connected (via another DMUX) to single mode fibers, which are then connected to the next 4CF (exploiting the already installed DMUXs) back on the 4-switch's IN side, following the ordering showed in Fig. 2(a). For example, a photon in the green input undergoes the operation of the four unitaries in the order $C \to B \to D \to A$, resulting in the product unitary $\Pi_2 = U_A U_D U_B U_C$. The other three inputs lead the photon through one of the other three permutations shown in Fig. 1(b). After S_4, a second Hadamard operation is applied to the control system using a second set of DMUX+4CF-BS+DMUX, in accordance with Algorithm III. The setup is thus a four-arm interferometer with each output directly connected to an InGaAs APD, working in gated mode and configured with 10% overall detection efficiency, and 5 ns gate width. The detection of a single photon in the yth ($y = 0, 1, 2, 3$) output detector univocally identifies in a single shot the property y, indicating the phase relations of the four unitaries implemented in the quantum 4-switch gate.

Before implementing the quantum 4-switch process, an initial alignment procedure using a polarimeter is performed. In-fiber polarization controllers (not shown in Fig. 2) are used in all single-mode fibers of the quantum 4 switch to ensure that every fiber corresponds to an identity operation on the polarization. They are also used at the final set of DMUX+4CF-BS+DMUX to guarantee the indistinguishability of the core modes, such that there is no path information available that would compromise the visibility of the interferometer [42,43]. The LCRs implementing the unitaries can be adjusted between identity and a half-wave plate by controlling the input voltage. In this way, we can toggle between an identity operation $\mathbb{1}$ and one of the Pauli operators Z, $(Z+X)/\sqrt{2}$ or X, when the orientation angle of the LCR is 0°, 22.5°, or 45°, respectively. Importantly, we note that the LCRs are placed at the far-field plane of the 4CF launchers

TABLE I. Tables of polarization unitaries used for the implementations of two different quantum 4-switch gates (both with the same set of gate permutations $\{ABCD, BADC, CBDA, DACB\}$; here $\mathbb{1}$ is the identity, Z and X are the Pauli operators). For both tables, each column provides a different set U of oracle gates. In turn, each such set exhibits the phase relations encoded—via Eq. (4)—in the corresponding column y of the matrix in Eq. (6). That is, the implemented oracle gates fulfil the problem's promise with respect to the experimentally implemented Hadamard matrix and the chosen set of permutations.

Table 1(a)

	y			
	0	1	2	3
U_A	$\mathbb{1}$	Z	$\mathbb{1}$	Z
U_B	X	X	X	X
U_C	$\mathbb{1}$	Z	Z	$\mathbb{1}$
U_D	X	X	X	X

Table 1(b)

	y			
	0	1	2	3
U_A	$(Z+X)/\sqrt{2}$	$\mathbb{1}$	Z	Z
U_B	$(Z+X)/\sqrt{2}$	X	X	X
U_C	$\mathbb{1}$	Z	$\mathbb{1}$	$\mathbb{1}$
U_D	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	X

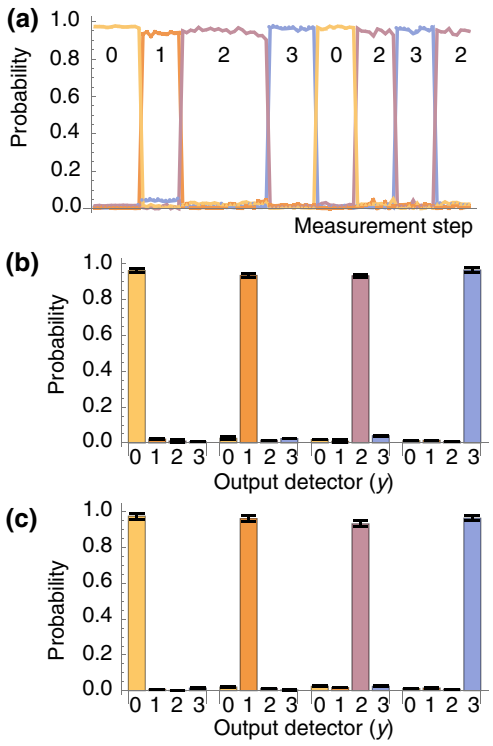

FIG. 3. (a) A sequence of about 8 min of measurement results with our quantum 4-switch process taken in real time. Measurements of 0.1 s duration are taken continuously, realized within the phase stabilization routine (see Sec. VII), in which the four sets of unitaries given each by the yth column of Table 1(a) are toggled randomly every minute. The number labels correspond to the columns of Table 1(a). Summary of experimentally obtained success probabilities to identify the commutation relations of the unitary operations in Table 1(a) [panel (b)] and Table 1(b) [panel (c)]. See the text for more details.

and that this guarantees that the unitary operations U_i are indistinguishable when applied in different orders (see Sec. VII). A computer-controlled field-programmable gate array (FPGA2) unit is used to control the LCRs.

In Table I we list the polarization operations U_i for two different implementations of the quantum 4-switch process. Table 1(a) corresponds to orthogonal operations (for each given column), while Table 1(b) includes nonorthogonal operations, which makes it more difficult to mimic the quantum N-switch with a causally ordered process (see below and Appendix A 3). In each table, the yth column defines a different set U of the target-system unitary gates and corresponds to the yth column of the Hadamard matrix in Eq. (6) (see Sec. VII). In our experiment, by exploiting the controlled LCRs, we are able to toggle between the different sets U of unitaries in real time. In Fig. 3(a) we show an example of the results recorded while switching randomly (with uniform probabilities) between operations corresponding to different columns of Table 1(a), about every minute. In each 0.1 s measurement we detected a total of about 6000 events. In Figs. 3(b) and 3(c) we show a summary of experimentally obtained success probabilities (each obtained from about 3×10^4 events) to identify the relative-phase relations between the different permutations of the unitary operations in Table 1(a) and Table 1(b), respectively. For Table 1(a), we obtain an average success probability of $p_{succ} = 0.948 \pm 0.005$, whereas for Table 1(b), we obtain $p_{succ} = 0.959 \pm 0.008$. Error bars correspond to one standard deviation, and are obtained by error propagation of the Poissonian count statistics. These results demonstrate the successful implementation of the quantum 4-switch process.

V. BENCHMARKING EXPERIMENTAL QUANTUM CONTROL OF MULTIPLE GATE ORDERS

To benchmark the realization of QCGO, it is useful to imagine a verification scenario, in which a verifier controls the oracle, while the process is implemented by a prover. The prover wishes to prove to the verifier that the process does display QCGO, and the verifier can test this by asking the prover to compute properties of oracles involving different gates. The quantum N-switch process allows the prover to solve the computations with considerably fewer oracle queries than any process with fixed (or classically controlled) gate connections. Indeed, it is the only process known to provide a unit success probability for Problem 1 in general (i.e., for any set of black-box gates satisfying the promise) with only N queries to the oracle. This can be used to give the verifier evidence in favor of the prover's honesty. However, if the table of oracle gates has a small number of columns—e.g., as in Table I—a dishonest prover with side information about the table can attain $p_{succ} = 1$ with a causally ordered process (see Appendix A 3), thus deceiving the verifier.

One way to benchmark experimental quantum switches with minimal assumptions is by measuring so-called causal witnesses [2,44]. Interestingly, by increasing the number of columns in the oracle-gate table (i.e., of possible choices for the gate sets U) and suitably choosing their prior probability distribution, Algorithm III can be turned into a causal witness for the quantum switch. That is, for sufficiently large oracle-gate tables and an appropriate prior distribution for the gate sets U, an upper bound p_{succ}^{CCGO} strictly smaller than 1 can be found for the probability of success attainable by processes with *classical* control of gate orders (CCGO). This provides us with a gap from the probability of success obtained by the quantum switch, which always remains unity in the noiseless case. Details on our search for witnesses are given in Appendix A 4.

Unfortunately, the number of measurement settings required to measure such witnesses is prohibitively high in practice for this experimental setup. For instance, the best witness for W_4 we can obtain with the abovementioned approach gives $p_{succ}^{CCGO} \approx 0.89$, but requires an oracle-gate table with 300 columns. Alternatively, weaker witnesses with $p_{succ}^{CCGO} \approx 0.92$ can also be found, but these still require 60 columns. Our LCR-based setup cannot switch among so many gates in a practical way. Nevertheless, it is yet a remarkable feature of our experiment that we do reach values of p_{succ} significantly higher than both bounds, which would conclusively benchmark W_4 for a higher number of settings. In addition, we note that witnesses with similarly high numbers of settings (259) have indeed been measured in other platforms, though with much slower switching times [19].

Alternatively, smaller oracle-gate tables suffice if the verifier can actively reduce the prover's potential knowledge about the tables. One way to do this is by allowing the verifier to apply a random basis rotation to each gate before delivering it to the prover. For instance, in this scenario, an upper bound $p_{succ}^{CCGO} \approx 0.84$ can be obtained for an oracle-gate table with only 30 columns (see Appendix A 4). Unfortunately, implementing such a causal witness would require the ability to switch among a continuum of gates, which is again experimentally infeasible. Nevertheless, here we are mainly interested in benchmarking our implementation of W_4 against experimental imperfections, rather than against hypothetical malicious provers exploiting side information about the gates' bases. In this regard, the experimentally obtained values in Fig. 3 are in the range $p_{succ} \approx 0.93$–0.97, which suggests that our setup should be capable of obtaining average success probabilities that are larger than the thresholds mentioned above, for a larger number of settings. Though not yet conclusive, this provides encouraging evidence for the QCGO of the implemented process.

VI. DISCUSSION

Here we introduce the "Hadamard promise problem," a novel computational primitive involving the relative phases between different permutations of multiple unknown gates. We present an algorithm to solve it efficiently, illustrating a quantum computational advantage associated to the coherent quantum control of the order in which a sequence of N unitary operations is applied. Our algorithm, which we implement experimentally for $N = 4$, exploits the quantum N-switch process to solve the problem with N applications of the unitary gates, whereas the known methods exploiting fixed gate orders use the gates $O(N^2)$ times. Both the problem and algorithm have the advantage that the target system needs only be two dimensional, as opposed to $N!$ dimensional as in previous proposals. This could inspire new approaches for exploiting indefinite causal order in quantum computation and communication, as well as for studying causal nonseparability in physical systems.

We experimentally implement the algorithm by constructing a quantum 4-switch process that coherently controls four different gate orderings with high fidelity, showing success probabilities for the algorithm of approximately 0.95. The all-optical setup involves a four-path interferometer constructed with new multicore optical fiber technology. As discussed in Sec. VII, the best-known quantum circuit with fixed gate orders solves this problem with 9 gate queries. Our experiment thus corresponds to a five-query improvement. Moreover, this is, to the best of our knowledge, the first report of a quantum superposition of more than 2 temporal orders. In addition, our implementation presents some technical advantages as well. On the one hand, it is versatile in that the gate orders can be modified in a practical fashion by switching the optical fiber connections and that the unitary gates themselves can be automatically controlled through the liquid crystal polarization retarders. On the other hand, the setup can be scaled up to higher control-system dimensions in a straightforward fashion. This work constitutes a key step towards realizing and verifying causal nonseparability among a large number of parties, and should play an important role in developing methods to exploit this resource.

VII. METHODS

A. Query complexity analysis

One may argue that implementing S_N is not the only way to solve Problem 1 (which is also true for the Fourier promise problem [14]). Here, we estimate the query complexity of other plausible approaches.

A natural approach one may attempt is to tomographically reconstruct the N unitary gates and then multiply them to estimate the Π_x, from which one can infer y. Since each Π_x is an N-fold product of the U_i, the overall error ε in its estimation is $\varepsilon = \Omega(N\epsilon)$, where ϵ is the statistical error of the reconstruction of each U_i. To attain a constant overall error, one thus needs $\epsilon = O(1/N)$, which, by virtue of Hoeffding's bound, in turn requires $q = O(1/\epsilon^2) = O(N^2)$ queries to each U_i. Moreover, since there are N gates to reconstruct, the overall query complexity is $Q = O(Nq) = O(N^3)$, i.e., cubically worse in N than with the quantum N-switch. Another alternative is to tomographically reconstruct each Π_x directly, and from that infer y. However, to query each N-fold product Π_x, one must query all N unitaries, and there are P such products. Hence, the overall query complexity is $Q = O(NP) \geq O(N^2)$ if one considers $P \geq N$ (as we did in our experimental demonstration), i.e., quadratically worse in N than with the quantum N-switch. A third possibility could be to directly estimate the signs of the commutators between the Π_x, and from that infer y. A canonical tool for that is the well-known Hadamard test [36]. This allows one to estimate overlaps of the form $\langle\Psi|_t \Pi_x |\Psi\rangle_t$ or $\langle\Psi|_t \Pi_x^\dagger \Pi_{x'} \Pi_x |\Psi\rangle_t$ directly from queries to Π_x or Π_x and $\Pi_{x'}$, respectively, for any state $|\Psi\rangle_t$. As before, each query to Π_x accounts for N queries to the gates, and the overall query complexity is again $Q = O(NP) \geq O(N^2)$.

Finally, one can simulate S_N exactly with a circuit with fixed gate orders. For the usual case where all $P = N!$ permutations are considered, the optimal causally ordered circuit that synthesizes S_N in the black-box scenario displays complexity $Q = \Omega(N^2)$ [13,14,17]. For the concrete case experimentally studied here, $P = N = 4$, the optimal causally ordered circuit that synthesizes S_4 requires 9 queries (see Appendix A 2). In fact, this is the reason why we choose the particular permutation set $\{ABCD, BADC, CBDA, DACB\}$. Through a brute-force search, we find that, from all quartets of permutations, most of them require 7 queries or less with the simulation strategy presented in Appendix A 2, some other 8 queries, and a few of them (including the one chosen here) require the maximum of 9 queries. Thus, the specific version of the quantum 4-switch process implemented here provides a gap of $9 - 4 = 5$ queries with respect to all causally ordered processes.

B. Experimental details

1. Single-photon source

The single-photon light source is composed of a semiconductor distributed feedback telecom laser ($\lambda = 1546$ nm) connected to an external fiber-pigtailed amplitude modulator (Mach-Zehnder interferometer, MZI). An FPGA unit (FPGA1) is used with the MZI to externally modulate the laser and generate optical pulses 5 ns wide. Optical attenuators (ATTs) are used before the MZI to create weak coherent states with a mean photon number per pulse of $\mu = 0.2$. In this case, 90% of the

non-null pulses generated contain a single photon. Thus, our source is a good approximation to a nondeterministic single-photon source, which is commonly adopted in quantum communications [45]. FPGA1 also controls the active phase stabilization of the system and registration of single-photon counts at each of the four detectors during the measurement procedure (see below).

2. Indistinguishability of the multigate operations in different orders

The four unitary operators U_i $(i = A, B, C, D)$ are realized using birefringent liquid crystal retarders. An important aspect of the experiment is to guarantee the realization of the same unitary operation U_i for all different orders considered. That is, the implementation of U_i must be independent of the illuminated core on the corresponding 4CF at the IN side of the oracle. To achieve this, the LCRs are placed in the Fourier plane of the objective lenses of the 4CF fiber launchers [see Fig. 4(a)]. At the exit face of this fiber, the output single mode of each core is given by a Gaussian function $g(\vec{r})$ centered at the core position $\vec{r}_c$. At the Fourier plane of the launcher lens, the spatial distribution of each core is given by the Fourier transform $\mathcal{F}[g(\vec{r}-\vec{r}_c)](\vec{s}) \propto \exp(ik\vec{s}\cdot\vec{r}_c/f\,)g(\vec{s})$. Therefore, irrespective of the illuminated core, all core modes overlap at the same central point with the intensity proportional to $|g(\vec{s})|^2$. This avoids spatial distinctions as in certain implementations for $N = 2$ gates [18,19]. To guarantee this condition for our experiment, we used a CCD camera to record the intensity distributions at the Fourier plane (with the LCRs removed), as shown in Fig. 4(b). The images, obtained with an intense laser, show the centering of the light distribution when a single core is connected. The resulting interference pattern when all cores are illuminated shows high visibility, confirming spatial indistinguishability. This guarantees that the unitary operations U_i are indistinguishable when applied in different orders—a crucial requirement for a valid implementation of an N-switch [20].

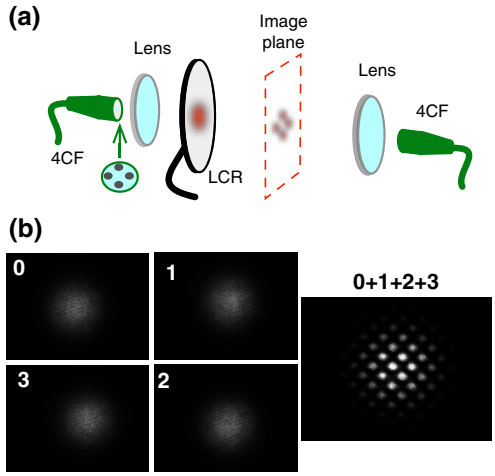

FIG. 4. (a) Illustration of the 4CF launchers and the LCRs implementing the unitaries U_i. The LCRs are placed at the Fourier plane of the output coupling lenses. (b) Images recorded at the LCRs plane, of each core alone, as well as the output when all cores are connected, showing large spatial overlap between the cores modes. This guarantees that the U_i are indistinguishable when applied in different orders.

3. Phase stabilization and measurement procedure

Phase (PHASE MOD) and intensity modulators (INT MOD) are used after the first 4CF-BS, on each arm of the interferometer [see Fig. 2(a)], to set the relative phases between the four spatial modes to zero, and to adjust the amplitudes. The FPGA1 unit is used to implement a control system to actively compensate phase drifts in the quantum 4-switch process. The control is based on a perturb and observe power point tracking method [39,46]. Basically, the phase drift compensation algorithm will perturb the kth phase modulator to cancel any phase noise using a high-speed signal. The algorithm does this sequentially to each phase modulator and in each step it maximizes the number of photocounts in the output detector "0" with the LCRs set to realize column $y = 0$ of one of the tables in Table I. When the counts achieve a given threshold value for the success probability, the voltages applied to the phase modulators are maintained constant, and an ON signal is sent to FPGA2 to activate the LCRs by applying a constant voltage, realizing any one of the four columns of the respective table in Table I, chosen by the user. After a 0.2 s deadtime to allow for the LCRs voltages to reach the desired value, a 0.1 s measurement stage is realized. After a single measurement window, an OFF signal is sent to return the LCRs to column 0. In this way, we can switch rapidly between columns 0–3 of the tables. The control system monitors the phase stabilization of the interferometer in real time after every measurement.

We have used this phase stabilization routine in other work [39], and obtained visibilities over 99%. Here, our success probability is limited to about 95% due to slightly imperfect polarization rotations of the LCRs, as well as the difficulty in achieving proper alignment of the polarization state for the different LCR combinations in each path, which we observed in the initial alignment procedure using the polarimeter (see Sec. IV).

ACKNOWLEDGMENTS

We thank Barbara Amaral, Johanna Barra, Fabio Costa, and Časlav Brukner for helpful insights. M.M.T. and L.A. acknowledge financial support from the Brazilian agencies CNPq (PQ Grant No. 311416/2015-2 and INCT-IQ), FAPERJ (PDR10 E-26/202.802/2016 and JCN E-26/202.701/2018), CAPES (PROCAD2013), and the Serrapilheira Institute (Grant No. Serra-1709-17173). This

work is also supported by Fondo Nacional de Desarrollo Científico y Tecnológico (ANID) (Grants No. 3200779, No. 1190901, No. 1200266, and No. 1200859) and ANID – Millennium Science Initiative Program – ICN17_012. J.C. is supported by ANID/REC/PAI77190088. A.A. is supported by the Swiss National Science Foundation (Starting Grant DIAQ and NCCR SwissMAP). M.A. received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant No 801110 and the Austrian Federal Ministry of Education, Science and Research (BMBWF). The paper reflects only the authors' views, the EU agency is not responsible for any use that may be made of the information it contains.

APPENDIX

1. Proof of Eq. (5)

First, note that (just like the Fourier transform) the Hadamard gate H_P maps $|0\rangle_c$ to the uniform superposition of all computational-basis states (under the assumption that the corresponding Hadamard matrix M_P only has $+1$ values along the first column):

$$H_P\,|0\rangle_c\,|\Psi\rangle_t = \frac{1}{\sqrt{P}}\sum_{x\in[P]}|x\rangle_c\,|\Psi\rangle_t\,. \tag{A1}$$

Then, the quantum N-switch gate introduces the sign $m_{x,y}$ to each computational-basis state $|x\rangle_c$ in the superposition

$$\begin{aligned} S_N H_P\,|0\rangle_c\,|\Psi\rangle_t &= \frac{1}{\sqrt{P}}\sum_{x\in[P]}|x\rangle_c\,\Pi_x\,|\Psi\rangle_t \\ &= \left(\frac{1}{\sqrt{P}}\sum_{x\in[P]} m_{x,y}\,|x\rangle_c\right)\Pi_0\,|\Psi\rangle_t\,, \end{aligned} \tag{A2}$$

where the second equality follows from Eq. (4). Now, by definition, the state within the brackets is $H_P\,|y\rangle_c$. Hence, applying H_P^{-1} to both sides of Eq. (A2) yields Eq. (5).

2. Exact simulation of the quantum N-switch with a fixed-gate-order circuit

It is possible to simulate the quantum N-switch—i.e., produce the same superposition of unitaries $\{\Pi_x\}_{x\in[P]}$ as the quantum N-switch for whatever unitaries U_i are inserted at its open slots—with a causally ordered circuit at the cost of making more uses (queries) of each unitary. The basic idea behind such a circuit is to apply the unitaries coherently controlled by a qudit. However, this is not a straightforward task with black-box unitaries [26,47–51]. A workaround is to use ancillas and controlled swap gates that coherently control whether each target-system gate is effectively applied to the target system or to an ancilla. This can be done with a circuit such as in Fig. 5, which uses a P-dimensional control qudit and N d-dimensional ancilla systems (one for each gate U_i). Importantly, as the reader may verify, all N ancillas experience the same overall gate sequence for all input states of the control register, which guarantees that the ancillas disentangle from the target and control systems by the end of the circuit. For instance,

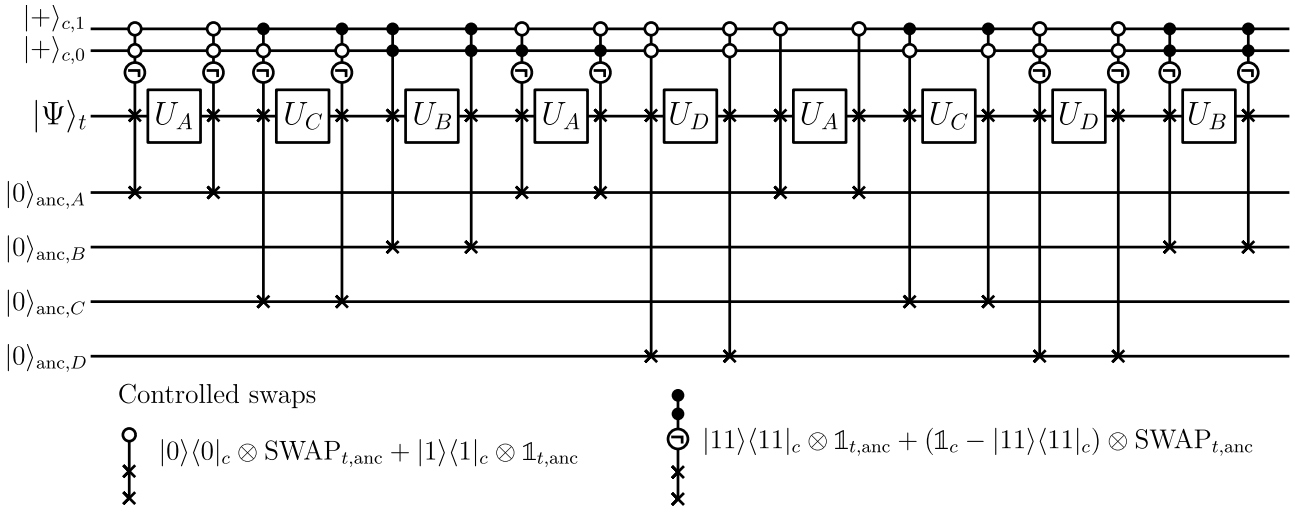

FIG. 5. Fixed-gate-order circuit that simulates the quantum 4-switch process that is realized experimentally, i.e., with quantum control of the four gate sequences $\Pi_0 = U_D U_C U_B U_A$, $\Pi_1 = U_C U_D U_A U_B$, $\Pi_2 = U_A U_D U_B U_C$, and $\Pi_3 = U_B U_C U_A U_D$. Before and after each unitary U_i, a pair of controlled swap gates controls whether U_i is applied to the target system or to an ancilla; the control qudit has dimension $P = 4$, here represented as two qubits (with $x = 0, 1, 2$, and 3 encoded as 00, 01, 10, and 11, respectively). Filled circles indicate an operation conditioned on the $|1\rangle_c$ state; open circles indicate an operation conditioned on the $|0\rangle_c$ state. Conditioning on negation of certain states is also needed, as exemplified in the legend below the circuit.

for the circuit in Fig. 5, the final state of the ancillas is $U_A^2 |0\rangle_{\text{anc},A} U_B |0\rangle_{\text{anc},B} U_C |0\rangle_{\text{anc},C} U_D |0\rangle_{\text{anc},D}$.

With this circuit scheme, the problem of simulating the superposition of unitaries produced by a quantum N-switch reduces to finding a supersequence that includes all the desired permutations as subsequences; the query complexity of this scheme is then given by the length of the shortest such supersequence [17,52]. In the experiment and Fig. 5, *ACBADACDB* is the supersequence to the quartet of permutations $\{ABCD, BADC, CBDA, DACB\}$ (note that the subsequences need not be contiguous). We have made an extensive numerical search of all quartets of permutations of A, B, C, D. There are $(N! - 1 \quad P - 1) = (23 \quad 3) = 1771$ unique quartets, where quartets that differ only by relabeling are disconsidered (this amounts to, for instance, only considering quartets that include some fixed permutation, e.g., *ABCD*). Of those, most require a supersequence of length 8 or less (37 unique quartets require length 6; 946 require length 7; 779 require length 8) and only 9 require length 9. Since the higher the supersequence length, the higher the query complexity of the simulation by fixed-gate-order circuit, we chose one of the latter nine quartets for our experiment (as well as Fig. 5). Note that all nine black boxes are queried once, irrespective of whether they are effectively used in the superposition or not; hence, the query complexity of this simulation of the quantum 4-switch process is 9.

3. Fixed-gate circuit algorithms for the Hadamard promise problem exploiting side information about the gates

Let us revisit the adversarial scenario of a verifier who controls the oracle and poses the Hadamard promise problem to a prover. The prover thus receives unknown (to them) unitaries and uses them to the best of their abilities to solve the problem and output the correct answer to the verifier. As we showed, a prover in possession of a quantum N-switch can solve the problem with 100% success rate using only a single query from each unitary. We now ask: can a prover solve the problem with access only to fixed-gate-order circuits?

By performing the simulations in the previous section, they are also able to solve the Hadamard promise problem with 100% success rate. However, they must request additional queries of the oracle to the verifier, a tell-tale sign to the latter that the quantum N-switch has not been realized.

We now explore the case of a prover with side information on the unitaries from the oracle. More specifically, let us suppose that they know the table of unitaries that the verifier uses (Table I), but not which column is selected in each run. This information aids the prover, who may no longer need to produce the superposition of unitaries from the previous section.

If Table 1(a) is used, the prover's strategy is relatively simple. By inputting a $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ state to black box U_A, the output state will be either $|+\rangle$ if $U_A = \mathbb{1}$ or $|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$ if $U_A = Z$. With a measurement of the output in the X basis, they can identify U_A (we call this an X-basis test on U_A). Doing the same procedure on U_C, they identify this unitary as well and discover the column y of Table 1(a) being used. Since only 1 query or less of each unitary is needed, the prover can in fact deceive the verifier in this case.

If instead Table 1(b) is used, the prover requires a slightly more complex fixed-gate-order circuit to deceive the verifier. It begins with an X-basis test applied to U_C, which reveals the content of that black box. In turn, U_D is revealed with an analogous Z-basis test, with input state $|0\rangle$ and measurement of output in the Z basis. If one of these two black boxes is revealed to be a Pauli operator (Z or X) then that run of the promise problem has been solved ($y = 1$ or 3, respectively). However, if both $U_C = \mathbb{1}$ and $U_D = \mathbb{1}$, both $y = 0$ and $y = 2$ are possible, and the black boxes U_A, U_B need to be used. Since the quantum N-switch finds the correct value of y with probability 1, so is the goal of the prover here. However, the two possible unitaries for U_A $[(Z + X)/\sqrt{2}, Z]$ are not orthogonal, i.e., not perfectly distinguishable, and the same happens with U_B. No independent use of U_A and U_B can tell the columns apart with certainty. There is a viable strategy, though, using U_A and U_B in sequence. Indeed, note that $U_B U_A = \mathbb{1}$ for column 0 and $U_B U_A = -iY$ for column 2. A Z- or X-basis test applied to the sequence of the two unitaries U_A and U_B can distinguish these two possibilities, again solving the problem with certainty.

If the prover does not know whether the verifier uses Table 1(a) or 1(b), the former needs to first identify which table is used. This table identification can be done with a Z-basis test on U_D, which reveals whether $U_D = X$ or $U_D = \mathbb{1}$. The strategy for Table 1(a) is applied in the former case, that for Table 1(b) in the latter case (note that column $y = 3$ is the same for both tables).

4. Causal witnesses for the 4-switch process

In order to certify, via the Hadamard promise problem, that a given process exhibits some QCGO, one may look for the maximal probability of success p_{succ}^{CCGO} that processes with CCGO can reach: if this upper bound is strictly smaller than 1, it becomes possible to experimentally obtain a probability of success $p_{succ} > p_{succ}^{CCGO}$ and thus prove that these results cannot be explained by CCGO.

For a fixed choice of gate permutations and of the Hadamard matrix under consideration, the "causal bound" p_{succ}^{CCGO} still depends on the specific choice of possible sets U, and of the prior distribution with which each set is chosen in each experimental run. Considering different possible sets U_k, each satisfying the promise of Eq. (4)

for some value $y = y_k$ and chosen with probability q_k, the probability of success (i.e., of obtaining the correct value $y = y_k$) of the Hadamard promise problem is obtained as

$$p_{\text{succ}} = \sum_k q_k \text{Prob}(y = y_k \mid \mathsf{U} = \mathsf{U}_k). \tag{A3}$$

To compute the above probabilities, and to obtain the causal bound p_{succ}^{CCGO}, we use the so-called "process matrix framework" [1]. In this framework the process under consideration (i.e., in our case, the circuit that connects the four unitaries and the final measurement) is described by the "process matrix" W, acting on the tensor product of all input and output Hilbert spaces of the four unitaries and of the final measurement. When the four qubit unitaries from some quartet $\mathsf{U}_k = \{U_A^{(k)}, U_B^{(k)}, U_C^{(k)}, U_D^{(k)}\}$ are applied, the probability $\text{Prob}(y = y_k \mid \mathsf{U} = \mathsf{U}_k)$ that the final measurement in the computational basis $\{|y\rangle_c\}_{y\in[4]}$ of $\mathbb{H}_c$ gives the outcome y_k for an arbitrary process matrix W is obtained as

$$\text{Prob}(y = y_k \mid \mathsf{U} = \mathsf{U}_k) = \text{Tr}[(|\mathsf{U}_k\rangle\!\rangle\langle\!\langle \mathsf{U}_k|^\top \otimes |y_k\rangle\langle y_k|_c) W] \tag{A4}$$

with

$$|\mathsf{U}_k\rangle\!\rangle := |U_A^{(k)}\rangle\!\rangle |U_B^{(k)}\rangle\!\rangle |U_C^{(k)}\rangle\!\rangle |U_D^{(k)}\rangle\!\rangle. \tag{A5}$$

Here, "$\top$" denotes the transposition in the computational basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{H}_t$ and $|U_i^{(k)}\rangle\!\rangle \in \mathbb{H}_t \otimes \mathbb{H}_t$ is the Choi vector representation [53] of the ith unitary $U_i^{(k)}$ for $i = A, B, C$ or D, technically defined as $|U_i^{(k)}\rangle\!\rangle := \mathbb{1} \otimes U_i^{(k)} |\mathbb{1}\rangle\!\rangle$, with $|\mathbb{1}\rangle\!\rangle := |0\rangle|0\rangle + |1\rangle|1\rangle$. According to Eq. (A3), the success probability is then obtained as

$$\begin{aligned} p_{\text{succ}} &= \text{Tr}[GW] \\ \text{with } G &= \sum_k q_k |\mathsf{U}_k\rangle\!\rangle\langle\!\langle \mathsf{U}_k|^\top \otimes |y_k\rangle\langle y_k|_c . \end{aligned} \tag{A6}$$

The process matrix describing the ideal 4-switch process of Fig. 1(b) is given by $W_4 = |w_4\rangle\langle w_4|$ [2,3], where

$$\begin{aligned} |w_4\rangle = {} & |0\rangle^{c_p} |\mathbb{1}\rangle\!\rangle^{t_p A_I} |\mathbb{1}\rangle\!\rangle^{A_O B_I} |\mathbb{1}\rangle\!\rangle^{B_O C_I} |\mathbb{1}\rangle\!\rangle^{C_O D_I} |\mathbb{1}\rangle\!\rangle^{D_O t_f} |0\rangle^{c_f} \\ & + |1\rangle^{c_p} |\mathbb{1}\rangle\!\rangle^{t_p B_I} |\mathbb{1}\rangle\!\rangle^{B_O A_I} |\mathbb{1}\rangle\!\rangle^{A_O D_I} |\mathbb{1}\rangle\!\rangle^{D_O C_I} |\mathbb{1}\rangle\!\rangle^{C_O t_f} |1\rangle^{c_f} \\ & + |2\rangle^{c_p} |\mathbb{1}\rangle\!\rangle^{t_p C_I} |\mathbb{1}\rangle\!\rangle^{C_O B_I} |\mathbb{1}\rangle\!\rangle^{B_O D_I} |\mathbb{1}\rangle\!\rangle^{D_O A_I} |\mathbb{1}\rangle\!\rangle^{A_O t_f} |2\rangle^{c_f} \\ & + |3\rangle^{c_p} |\mathbb{1}\rangle\!\rangle^{t_p D_I} |\mathbb{1}\rangle\!\rangle^{D_O A_I} |\mathbb{1}\rangle\!\rangle^{A_O C_I} |\mathbb{1}\rangle\!\rangle^{C_O B_I} |\mathbb{1}\rangle\!\rangle^{B_O t_f} |3\rangle^{c_f} \end{aligned} \tag{A7}$$

and the superscripts indicate the Hilbert spaces in which the various states are defined: c_p, c_f refer to the past and the future of the control system, t_p, t_f refer to the past and the future of the target system, A_I and A_O refer to the input and output spaces of operation U_A, and similarly for the other parties. Note that, for the sake of clarity, in Fig. 1(a) we use a simplified notation based on the necessary isomorphism between t_p, t_f, A_I, A_O, and the other parties' inputs and outputs (as well as between c_p and c_f).

In Algorithm III we input the initial control state $H_P|0\rangle$ into c_p, the initial target state $|\Psi\rangle$ into t_p, and apply H_P^{-1} to the resulting state of the control system in c_f. These fixed steps can be incorporated into the process-matrix description. The resulting matrix that describes our effective process is then $W_4' = \text{Tr}_{t_f} |w_4'\rangle\langle w_4'|$ with

$$\begin{aligned} |w_4'\rangle = \tfrac{1}{2}[& |\Psi\rangle^{A_I} |\mathbb{1}\rangle\!\rangle^{A_O B_I} |\mathbb{1}\rangle\!\rangle^{B_O C_I} |\mathbb{1}\rangle\!\rangle^{C_O D_I} |\mathbb{1}\rangle\!\rangle^{D_O t_f} H_P^{-1} |0\rangle_c \\ & + |\Psi\rangle^{B_I} |\mathbb{1}\rangle\!\rangle^{B_O A_I} |\mathbb{1}\rangle\!\rangle^{A_O D_I} |\mathbb{1}\rangle\!\rangle^{D_O C_I} |\mathbb{1}\rangle\!\rangle^{C_O t_f} H_P^{-1} |1\rangle_c \\ & + |\Psi\rangle^{C_I} |\mathbb{1}\rangle\!\rangle^{C_O B_I} |\mathbb{1}\rangle\!\rangle^{B_O D_I} |\mathbb{1}\rangle\!\rangle^{D_O A_I} |\mathbb{1}\rangle\!\rangle^{A_O t_f} H_P^{-1} |2\rangle_c \\ & + |\Psi\rangle^{D_I} |\mathbb{1}\rangle\!\rangle^{D_O A_I} |\mathbb{1}\rangle\!\rangle^{A_O C_I} |\mathbb{1}\rangle\!\rangle^{C_O B_I} |\mathbb{1}\rangle\!\rangle^{B_O t_f} H_P^{-1} |3\rangle_c]. \end{aligned} \tag{A8}$$

Using this process matrix, we can verify that, for any set $\mathsf{U}_k = \{U_A^{(k)}, U_B^{(k)}, U_C^{(k)}, U_D^{(k)}\}$ satisfying promise (4) for some $y = y_k$, one has $\text{Tr}[(|\mathsf{U}_k\rangle\!\rangle\langle\!\langle \mathsf{U}_k|^\top \otimes |y_k\rangle\langle y_k|_c) W_4'] = 1$, so that the success probability of Algorithm III, using the 4-switch process, is indeed unity.

Processes that display CCGO, on the other hand, are described by process matrices from a particular subset of all possible matrices, with some specific structure. In Ref. [54], it was indeed shown that (in our scenario, with four operations and a final measurement) CCGO process matrices W must have a decomposition of the form

$$W = \sum_{(i,j,k,l)} W_{(i,j,k,l),c} \tag{A9}$$

in terms of positive semidefinite matrices (not necessarily valid process matrices) $W_{(i,j,k,l),c}$, for all $4! = 24$ permutations (i,j,k,l) of $\{A,B,C,D\}$ (hence with $i \neq j \neq k \neq l$). These must furthermore be such that the "reduced" matrices $W_{(i,j,k,l)} := \text{Tr}_c W_{(i,j,k,l),c}$ (where c refers to the space of the final measurement), $W_{(i,j,k)} := \text{Tr}_l W_{(i,j,k,l)}$ (where Tr_l corresponds to the partial trace over the input and output spaces of the operation U_l), $W_{(i,j)} := \sum_k \text{Tr}_k W_{(i,j,k)}$, and $W_{(i)} := \sum_j \text{Tr}_j W_{(i,j)}$ are of the form

$$\begin{aligned} W_{(i,j,k,l)} &= \widetilde{W}_{(i,j,k,l)} \otimes \mathbb{1}^{l_O}, & W_{(i,j,k)} &= \widetilde{W}_{(i,j,k)} \otimes \mathbb{1}^{k_O}, \\ W_{(i,j)} &= \widetilde{W}_{(i,j)} \otimes \mathbb{1}^{j_O}, & W_{(i)} &= \widetilde{W}_{(i)} \otimes \mathbb{1}^{i_O}, \end{aligned} \tag{A10}$$

for some matrices $\widetilde{W}_{(\cdot)}$ in the appropriate spaces. Here $\mathbb{1}^{l_O}$ denotes the identity operator on the output space of the operation U_l, and similarly for $\mathbb{1}^{k_O}$, $\mathbb{1}^{j_O}$, and $\mathbb{1}^{i_O}$.

To obtain the causal bound p_{succ}^{CCGO} for all CCGO processes—for a fixed choice of sets U_k and weights q_k, and hence a fixed operator G as defined in Eq. (A6)—one can then optimize the value of $p_{\text{succ}} = \text{Tr}[GW]$ for all W in

the class described by Eqs. (A9)–(A10) (which describes a closed convex cone, which we denote by $\mathcal{W}^{CCGO}$) and with the additional normalization condition [1,3,55] that $\mathrm{Tr}\, W = 2^4$:

$$p_{\mathrm{succ}}^{CCGO} = \max_{W} \mathrm{Tr}[GW] \quad \text{such that} W \in \mathcal{W}^{CCGO}, \quad \mathrm{Tr}\, W = 2^4. \tag{A11}$$

As it turns out, this optimization is a semidefinite programming (SDP) problem, which can in principle be solved faithfully [2,44,55].

Another possible "dual" approach—now just for a fixed choice of possible sets U_k—is to optimize the causal witness rather than the process matrix. Fixing the witness to be of the form of G in Eq. (A6) allows us to optimize the weights q_k for each U_k: indeed, the optimization problem can be written here (see Appendix H of Ref. [2]) as

$$p_{\mathrm{succ}}^{CCGO} = \min_{p,\{q_k\}_k} p \tag{A12a}$$

$$\text{such that } p\mathbb{1}/2^4 - G \in \mathcal{S}^{CCGO}, \tag{A12b}$$

$$G = \textstyle\sum_k q_k |\mathsf{U}_k\rangle\!\rangle\langle\!\langle \mathsf{U}_k|^\top \otimes |y_k\rangle\langle y_k|_c\,,$$

$$q_k \geq 0, \quad \sum_k q_k = 1, \tag{A12c}$$

where

$$\mathcal{S}^{CCGO} := (\mathcal{W}^{CCGO})^* := \{S \mid \text{for all } W \in \mathcal{W}^{CCGO},\ \mathrm{Tr}[SW] \geq 0\} \tag{A13}$$

is the convex cone dual to $\mathcal{W}^{CCGO}$, which can, like the latter, be described in terms of SDP constraints [2,44,55].

Let us note here that the above characterization of $\mathcal{W}^{CCGO}$ [via the decomposition of Eq. (A9), with the matrices $W_{(\cdot)}$ satisfying the constraints of Eq. (A10)] was shown [55] to be a sufficient condition for the process matrix to be "causally separable" [1,3,55]. It remains an open question whether or not the class of causally separable processes is strictly larger than that of CCGO. We nevertheless conjecture that the "causal bounds" p_{succ}^{CCGO} we obtain here hold for all causally separable processes.

a. Causal witnesses with finitely many settings

As is clear from the discussion in Appendix A 3, if one only uses the sets from Tables 1(a) and 1(b) in Table I, then one can only get a trivial causal bound $p_{succ}^{CCGO} = 1$. In order to get a nontrivial bound, one needs to consider some other possible sets of unitaries.

To this end, we consider unitaries taken from the set

$$\mathcal{G} = \left\{\mathbb{1}, Z, X, Y, \frac{Z+X}{\sqrt{2}}, \frac{Z+Y}{\sqrt{2}}, \frac{X+Y}{\sqrt{2}}, \frac{\mathbb{1}+iZ}{\sqrt{2}}, \frac{\mathbb{1}+iX}{\sqrt{2}}, \frac{\mathbb{1}+iY}{\sqrt{2}}\right\} \tag{A14}$$

(which have the nice property that their Choi matrices $|U\rangle\!\rangle\langle\!\langle U|$ span the full 10-dimensional space of all possible Choi matrices for qubit unitaries), and looked for which sets $\mathsf{U} = \{U_A, U_B, U_C, U_D\}$ with $U_i \in \mathcal{G}$ satisfy the promise of Eq. (4). We find 460 different such sets: 316 satisfying the promise for $y = 0$, 60 for $y = 1$, 42 for $y = 2$, and again 42 for $y = 3$.

SDP problem (A12) is large—indeed, G is a $2^{10} \times 2^{10}$ matrix and the characterization of $\mathcal{S}^{CCGO}$ imposes many constraints—making it at the limits of tractability. To simplify the problem further, we exploit an approach based on "quantum superinstruments" introduced in Ref. [54]. To this end, we first note that Eq. (A11) can be simplified by rewriting Eq. (A6) in the form

$$p_{\mathrm{succ}} = \sum_y \mathrm{Tr}[G^{[y]} W^{[y]}] \tag{A15a}$$

$$\text{with} \quad G^{[y]} = \textstyle\sum_k \delta_{y,y_k} q_k |\mathsf{U}_k\rangle\!\rangle\langle\!\langle \mathsf{U}_k|_c^\top, \quad W^{[y]} = \mathrm{Tr}_c[(\mathbb{1} \otimes |y\rangle\langle y|_c) W] \tag{A15b}$$

(where δ_{y,y_k} is the Kronecker delta). Here, one now only needs to optimize over the four smaller $2^8 \times 2^8$ matrices $W^{[y]}$. The fact that the $W^{[y]}$ must be obtained from some CCGO process as in the second equation of Eq. (A15b) implies similar SDP constraints as Eqs. (A9)–(A10) on the $W^{[y]}$ directly [54]; more formally, one has $\{W^{[y]}\}_y \in \overline{\mathcal{W}}^{CCGO}$, where $\overline{\mathcal{W}}^{CCGO}$ is again a closed convex cone. Dual approach (A12) can then also be rewritten in the simpler form

$$p_{\mathrm{succ}}^{CCGO} = \min_{p,\{q_k\}_k} p \tag{A16a}$$

$$\text{such that } \{p\mathbb{1}/2^4 - G^{[y]}\}_y \in \overline{\mathcal{S}}^{CCGO}, \tag{A16b}$$

$$G^{[y]} = \textstyle\sum_k \delta_{y,y_k} q_k |\mathsf{U}_k\rangle\!\rangle\langle\!\langle \mathsf{U}_k|_c^\top, \quad q_k \geq 0, \quad \sum_k q_k = 1, \tag{A16c}$$

where the dual cone

$$\overline{\mathcal{S}}^{CCGO} := (\overline{\mathcal{W}}^{CCGO})^* := \left\{ \{S^{[y]}\}_y \;\middle|\; \text{for all } \{W^{[y]}\}_y \in \overline{\mathcal{W}}^{CCGO}, \ \sum_y \mathrm{Tr}[S^{[y]} W^{[y]}] \geq 0 \right\} \tag{A17}$$

can again be described by SDP constraints [54].

We are able to solve the simpler SDP problem of Eq. (A16) using the 460 sets of unitaries from $\mathcal{G}$ with the splitting conic solver [56,57], obtaining a bound of $p_{succ}^{CCGO} \approx 0.92$. We then progressively set to zero the smallest weights and solve the SDP again, eventually reaching 60 nonzero weights with no change in p_{succ}^{CCGO} within numerical precision (36 corresponding to sets satisfying the promise for $y = 0$, 12 for $y = 1$, and 6 each for $y = 2$ and $y = 3$).

b. Causal witnesses with random rotations

The causal strategies described in Appendix A 3 exploit knowledge of the basis that the unknown unitaries are defined in. A possibility to obtain better bounds on p_{succ}^{CCGO} is therefore to allow the verifier to provide the unitaries in an unknown basis. Given a set $\mathsf{U} = \{U_A, U_B, U_C, U_D\}$, this corresponds formally to providing the operations $\mathsf{U}^{(V)} = \{VU_AV^\dagger, VU_BV^\dagger, VU_CV^\dagger, VU_DV^\dagger\}$ for some unknown unitary V. Note that if U obeys the promise of Eq. (4) then so does $\mathsf{U}^{(V)}$.

To construct better causal witnesses from this approach, we start as before with a fixed choice of sets U_k and then, in addition to choosing U_k with prior probability q_k, we randomly choose an unknown unitary V to be applied according to the Haar measure. Equation (A6) then becomes

$$p_{\text{succ}} = \text{Tr}[GW]$$
$$\text{with } G = \sum_k q_k \int \mathrm{d}\mu(V) |\mathsf{U}_k^{(V)}\rangle\!\rangle \langle\!\langle \mathsf{U}_k^{(V)}|^\top \otimes |y_k\rangle\langle y_k|_c \,, \tag{A18}$$

where $\mu(V)$ is the normalized Haar measure over SU(2). SDP problems (A11), (A12), and (A15) can then be solved in the same way as described above.

We again consider the 460 sets of unitaries U with each $U_i \in \mathcal{G}$ as in the previous section. The integration over the Haar measure can be performed analytically by taking an explicit parameterization of SU(2) unitaries. However, since the $|\mathsf{U}_k^{(V)}\rangle\!\rangle \langle\!\langle \mathsf{U}_k^{(V)}|^\top$ are $2^8 \times 2^8$ matrices, this procedure is nevertheless slow, even with automated symbolic integration using, e.g., *Mathematica*. To simplify matters, we exploit that fact that the Haar measure is unitary invariant [i.e., $d(V) = d(UV) = d(VU)$ for any unitary U], so sets U and U' that are equivalent up to a change of basis give $\int d\mu(V) |\mathsf{U}^{(V)}\rangle\!\rangle \langle\!\langle \mathsf{U}^{(V)}| = \int d\mu(V) |\mathsf{U}'^{(V)}_k\rangle\!\rangle \langle\!\langle \mathsf{U}'^{(V)}_k|$. We thereby find that there are 98 sets U that are inequivalent in this way and that satisfy one of the properties y_k.

Considering witnesses constructed from these sets, we solved the dual SDP problem given in Eq. (A16). For CCGO processes, we find the bound $p_{succ}^{CCGO} \approx 0.84$. Interestingly, we find that the same bound can be reached by considering the Haar randomization only over witnesses using sets U containing only Pauli matrices, rather than from the full set $\mathcal{G}$. Indeed, this bound can be obtained by randomizing over the 30 sets U given in Table II that we found to have nonzero weights in the optimal witness we obtained.

c. Derandomization

In order not to require the assumption that the prover does not know in which basis the verifier provided each set U, one could derandomize the approach above by using a weighted quantum t design [58]. This is a finite set of unitaries X together with weights w such that the average of any operator over them is equal to its average over the Haar measure up to order t. Since $|\mathsf{U}_k^{(V)}\rangle\!\rangle$ is an eighth-order expression on V, an 8 design allows us to reproduce exactly the witness with bound $p_{succ}^{CCGO} \approx 0.84$ with a finite, fixed set of unitaries. Unfortunately, t designs are rather large. It can be shown that the smallest size $|X|$ of a weighted 8 design for unitaries of dimension 2 is bounded by $165 \leq |X| \leq 968$, so the resulting witness would have at least 4950 settings, and therefore be of little relevance for experiments [59].

In order to obtain smaller witnesses, we instead sampled five random qubit unitaries from the Haar measure, and conjugated all 30 columns of Table II with these fixed unitaries, obtaining a witness using 150 settings.

Solving the SDP in Eq. (A11) with the splitting conic solver, fixing the prior probability of choosing each set $\mathsf{U}_k^{(V)}$ to be $q_k/5$, where q_k is the optimal weight obtained for the full randomization of U_k in the previous section, we obtained $p_{succ}^{CCGO} \approx 0.96$. By further optimizing over all

TABLE II. Table of 30 sets $\mathsf{U} = \{U_A, U_B, U_C, U_D\}$ involving the identity $\mathbb{1}$ and the orthogonal Pauli operators X, Y, Z only, satisfying the promise of Eq. (4) (for some value of y, indicated in the first row) for the gate permutations $\Sigma = \{ABCD, BADC, CBDA, DACB\}$ and the Hadamard matrix of Eq. (6).

	y																													
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	3	3	3	3
U_A	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	Z	$\mathbb{1}$	$\mathbb{1}$	Z	$\mathbb{1}$	Z	Z	$\mathbb{1}$	Z	Z	Z	Z	Z	$\mathbb{1}$	Z	Z	Z	Z	Z	$\mathbb{1}$	Z	Z	Z	$\mathbb{1}$	Z	Z	Z
U_B	$\mathbb{1}$	$\mathbb{1}$	Z	$\mathbb{1}$	$\mathbb{1}$	Z	$\mathbb{1}$	Z	$\mathbb{1}$	Z	Z	$\mathbb{1}$	Z	Z	Z	X	Z	$\mathbb{1}$	Z	X	X	X	Z	$\mathbb{1}$	X	Z	$\mathbb{1}$	X	X	X
U_C	$\mathbb{1}$	Z	$\mathbb{1}$	$\mathbb{1}$	Z	$\mathbb{1}$	$\mathbb{1}$	Z	Z	$\mathbb{1}$	Z	Z	$\mathbb{1}$	Z	Z	X	X	$\mathbb{1}$	X	Z	X	Y	X	Z	$\mathbb{1}$	X	Z	$\mathbb{1}$	Z	Y
U_D	Z	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	Z	Z	Z	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	Z	Z	Z	$\mathbb{1}$	Z	Z	$\mathbb{1}$	X	X	X	Y	Z	Z	X	$\mathbb{1}$	Y	X	X	$\mathbb{1}$	Y

150 weights using the dual SDP, we find that this can be improved to $p_{succ}^{CCGO} \approx 0.93$.

By using more than five random unitaries, this bound can be lowered further. For example, with 10 random unitaries we are able to obtain $p_{succ}^{CCGO} \approx 0.89$ (when optimizing over all 300 weights).

[1] O. Oreshkov, F. Costa, and Č. Brukner, Quantum correlations with no causal order, Nat. Commun. **3**, 1092 (2012).

[2] M. Araújo, C. Branciard, F. Costa, A. Feix, C. Giarmatzi, and Č. Brukner, Witnessing causal nonseparability, New J. Phys. **17**, 102001 (2015).

[3] O. Oreshkov and C. Giarmatzi, Causal and causally separable processes, New J. Phys. **18**, 093020 (2016).

[4] L. Hardy, Probability Theories with Dynamic Causal Structure: A New Framework for Quantum Gravity, arXiv:0509120 [gr-qc] (2005).

[5] L. Hardy, Towards quantum gravity: A framework for probabilistic theories with non-fixed causal structure, J. Phys. A: Math. Theor. **40**, 3081 (2007).

[6] L. Hardy, in *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony* (Springer Netherlands, Dordrecht, 2009), p. 379.

[7] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Quantum computations without definite causal structure, Phys. Rev. A **88**, 022318 (2013).

[8] M. Araújo, P. A. Guérin, and Ä. Baumeler, Quantum computation with indefinite causal structures, Phys. Rev. A **96**, 052315 (2017).

[9] M. Zych, F. Costa, I. Pikovski, and Č. Brukner, Bell's theorem for temporal order, Nat. Commun. **10**, 3772 (2019).

[10] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Quantum Circuit Architecture, Phys. Rev. Lett. **101**, 060401 (2008).

[11] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Theoretical framework for quantum networks, Phys. Rev. A **80**, 022339 (2009).

[12] G. Chiribella, Perfect discrimination of no-signalling channels via quantum superposition of causal structures, Phys. Rev. A **86**, 040301(R) (2012).

[13] T. Colnaghi, G. M. D'Ariano, S. Facchini, and P. Perinotti, Quantum computation with programmable connections between gates, Phys. Lett. A **376**, 2940 (2012).

[14] M. Araújo, F. Costa, and Č. Brukner, Computational Advantage from Quantum-Controlled Ordering of Gates, Phys. Rev. Lett. **113**, 250402 (2014).

[15] P. A. Guérin, A. Feix, M. Araújo, and Č. Brukner, Exponential Communication Complexity Advantage from Quantum Superposition of the Direction of Communication, Phys. Rev. Lett. **117**, 100502 (2016).

[16] K. Wei, N. Tischler, S.-r. Zhao, Y.-H. Li, J. M. Arrazola, Y. Liu, W. Zhang, H. Li, L. You, Z. Wang, Y.-a. Chen, B. C. Sanders, Q. Zhang, G. J. Pryde, F. Xu, and J.-W. Pan, Experimental Quantum Switching for Exponentially Superior Quantum Communication Complexity, Phys. Rev. Lett. **122**, 120504 (2019).

[17] S. Facchini and S. Perdrix, in *Theory and Applications of Models of Computation, Proceedings, Lecture Notes in Computer Science*, edited by R. Jain, S. Jain, and F. Stephan (Springer International Publishing, 2015), Vol. 9076, p. 324.

[18] L. M. Procopio, A. Moqanaki, M. Araújo, F. Costa, I. Alonso Calafell, E. G. Dowd, D. R. Hamel, L. A. Rozema, Č. Brukner, and P. Walther, Experimental superposition of orders of quantum gates, Nat. Commun. **6**, 7913 (2015).

[19] G. Rubino, L. A. Rozema, A. Feix, M. Araújo, J. M. Zeuner, L. M. Procopio, Č. Brukner, and P. Walther, Experimental verification of an indefinite causal order, Sci. Adv. **3**, e1602589 (2017).

[20] K. Goswami, C. Giarmatzi, M. Kewming, F. Costa, C. Branciard, J. Romero, and A. G. White, Indefinite Causal Order in a Quantum Switch, Phys. Rev. Lett. **121**, 090503 (2018).

[21] Y. Guo, X.-M. Hu, Z.-B. Hou, H. Cao, J.-M. Cui, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, and G. Chiribella, Experimental Transmission of Quantum Information Using a Superposition of Causal Orders, Phys. Rev. Lett. **124**, 030502 (2020).

[22] K. Goswami, Y. Cao, G. A. Paz-Silva, J. Romero, and A. G. White, Communicating via ignorance, arXiv:1807.07383 (2018).

[23] D. Deutsch and R. Jozsa, Rapid solution of problems by quantum computation, Proc. R. Soc. London Ser. A: Math. Phys. Sci. **439**, 553 (1992).

[24] D. R. Simon, On the power of quantum computation, SIAM J. Comput. **26**, 1474 (1997).

[25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).

[26] N. Friis, V. Dunjko, W. Dür, and H. J. Briegel, Implementing quantum control for unknown subroutines, Phys. Rev. A **89**, 030303(R) (2014).

[27] O. Oreshkov, Time-delocalized quantum subsystems and operations: On the existence of processes with indefinite causal structure in quantum mechanics, Quantum **3**, 206 (2019).

[28] D. J. Richardson, J. M. Fini, and L. E. Nelson, Space-division multiplexing in optical fibres, Nat. Photonics **7**, 354 (2013).

[29] 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. F. da Silva, G. B. Xavier, and G. Lima, High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers, Phys. Rev. A **96**, 22317 (2017).

[30] 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).

[31] G. B. Xavier and G. Lima, Quantum information processing with space-division multiplexing optical fibres, Commun. Phys. **3**, 9 (2020).

[32] L. M. Procopio, F. Delgado, M. Enríquez, N. Belabas, and J. A. Levenson, Communication enhancement through quantum coherent control of N channels in an indefinite causal-order scenario, Entropy **21**, 1012 (2019).

[33] L. M. Procopio, F. Delgado, M. Enríquez, N. Belabas, and J. A. Levenson, Sending classical information via three noisy channels in superposition of causal orders, Phys. Rev. A **101**, 012346 (2020).

[34] M. Araújo, A. Feix, M. Navascués, and Č. Brukner, A purification postulate for quantum mechanics with indefinite causal order, Quantum **1**, 10 (2017).

[35] M. M. Taddei, R. V. Nery, and L. Aolita, Quantum superpositions of causal orders as an operational resource, Phys. Rev. Res. **1**, 033174 (2019).

[36] K. J. Horadam, *Hadamard Matrices and Their Applications* (Princeton University Press, Princeton, 2007).

[37] A. Y. Kitaev, Quantum measurements and the Abelian Stabilizer Problem, arXiv:9511026 [quant-ph] (1995).

[38] 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).

[39] J. Cariñe, G. Cañas, P. Skrzypczyk, I. Šupić, N. Guerrero, T. Garcia, L. Pereira, M. A. S. Prosser, G. B. Xavier, A. Delgado, S. P. Walborn, D. Cavalcanti, and G. Lima, Multi-port beamsplitters based on multi-core optical fibers for high-dimensional quantum information, arXiv:2001.11056 (2020).

[40] K. Watanabe, T. Saito, K. Imamura, and M. Shiino, in *IEEE 17th Opto-Electronics and Communications Conference* (2012), p. 5C1.

[41] Y. Tottori, T. Kobayashi, and M. Watanabe, Low loss optical connection module for seven-core multicore fiber and seven single-mode fibers, IEEE Photonics Technol. Lett. **24**, 1926 (2012).

[42] S. P. Walborn, M. O. Terra Cunha, S. Pádua, and C. H. Monken, Double-slit quantum eraser, Phys. Rev. A **65**, 33818 (2002).

[43] F. A. Torres-Ruiz, G. Lima, A. Delgado, S. Pádua, and C. Saavedra, Decoherence in a double-slit quantum eraser, Phys. Rev. A **81**, 42104 (2010).

[44] C. Branciard, Witnesses of causal nonseparability: An introduction and a few case studies, Sci. Rep. **6**, 26018 (2016).

[45] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[46] P. Bhatnagar and R. K. Nema, Maximum power point tracking control techniques: State-of-the-art in photovoltaic applications, Renewable Sustainable Energy Rev. **23**, 224 (2013).

[47] M. Araújo, A. Feix, F. Costa, and Č. Brukner, Quantum circuits cannot control unknown operations, New J. Phys. **16**, 93026 (2014).

[48] J. Thompson, K. Modi, V. Vedral, and M. Gu, Quantum plug 'n' play: Modular computation in the quantum regime, New J. Phys. **20**, 013004 (2018).

[49] A. A. Abbott, J. Wechs, D. Horsman, M. Mhalla, and C. Branciard, Communication through coherent control of quantum channels, Quantum **4**, 333 (2020).

[50] G. Chiribella and H. Kristjánsson, Quantum Shannon theory with superpositions of trajectories, Proc. R. Soc. A: Math., Phys. Eng. Sci. **475**, 20180903 (2019).

[51] H. Kristjánsson, G. Chiribella, S. Salek, D. Ebler, and M. Wilson, Resource theories of communication, New J. Phys. **22**, 073014 (2020).

[52] P. Koutas and T. Hu, Shortest string containing all permutations, Discrete Math. **11**, 125 (1975).

[53] M.-D. Choi, Completely positive linear maps on complex matrices, Linear Algebra Appl. **10**, 285 (1975).

[54] J. Wechs, H. Dourdent, A. A. Abbott, and C. Branciard, Quantum circuits with classical versus quantum control of causal orders (to be published).

[55] J. Wechs, A. A. Abbott, and C. Branciard, On the definition and characterisation of multipartite causal (non)separability, New J. Phys. **21**, 013027 (2019).

[56] B. O'Donoghue, E. Chu, N. Parikh, and S. Boyd, Conic optimization via operator splitting and homogeneous self-dual embedding, J. Optim. Theory Appl. **169**, 1042 (2016).

[57] B. O'Donoghue, E. Chu, N. Parikh, and S. Boyd, SCS: Splitting conic solver, version 2.1.2 (2019).

[58] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, Measurement-based quantum computation beyond the one-way model, Phys. Rev. A **76**, 052315 (2007).

[59] Aidan Roy and A. J. Scott, Unitary designs and codes, Designs, Codes Cryptography **53**, 13 (2009).

Correction: The previously published Figure 1(b) was processed improperly during the final production cycle and its rendition has been corrected.

Bibliography

[1] C. H. Bennett y G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (1984).

[2] A. K. Ekert, Physical Review Letters (1991).

[3] Č. Brukner, M. Żukowski y A. Zeilinger, Phys. Rev. Lett. **89**, 19 (2002).

[4] G. M. Nikolopoulos, K. S. Ranade y G. Alber, Phys. Rev. A **73**, 3 (2006).

[5] N. J. Cerf, M. Bourennane, A. Karlsson y N. Gisin, Phys. Rev. Lett. **88**, 12 (2001).

[6] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski y A. Zeilinger, Physical Review Letters (2000).

[7] M. Araújo, F. Costa y Č. Brukner, Physical Review Letters (2014).

[8] D. Martínez, A. Tavakoli, M. Casanova, G. Cañas, B. Marques y G. Lima, Physical Review Letters (2018).

[9] J. Cariñe, G. Cañas, P. Skrzypczyk, I. Šupić, N. Guerrero, T. Garcia, L. Pereira, M. A. S. Prosser, G. B. Xavier, A. Delgado, S. P. Walborn, D. Cavalcanti y G. Lima, Optica **7**, 5 (may 2020).

[10] M. A. Nielsen y I. L. Chuang, *Quantum Computation and Quantum Information* (2010).

[11] 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 y C. Monroe, Nature **464**, 7291 (2010).

[12] A. Acín y L. Masanes, Certified randomness in quantum physics (2016).

[13] A. Rukhin, J. Soto y J. Nechvatal, Nist Special Publication (2010).

[14] H. K. Lo, M. Curty y B. Qi, Physical Review Letters **108**, 13 (2012).

[15] S. Pironio, V. Scarani y T. Vidick, New Journal of Physics **18**, 10 (oct 2016).

[16] 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 y J. W. Pan, Physical Review Letters (2018).

[17] M. Pawłowski y N. Brunner, Physical Review A - Atomic, Molecular, and Optical Physics (2011).

[18] G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima y M. Pawłowski, Experimental quantum randomness generation invulnerable to the detection loophole (2014).

[19] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden y N. Brunner, Physical Review Letters (2015).

[20] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden y N. Brunner, Physical Review Applied (2017).

[21] I. Supić, P. Skrzypczyk y D. Cavalcanti, Phys. Rev. A **95**, 4 (apr 2017).

[22] C. E. Shannon, The Bell System Technical Journal **27**, 3 (July 1948).

[23] M. Herrero-Collantes y J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (Feb 2017).

[24] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset y N. Brunner, Physical Review A (2018).

[25] N. Gisin, G. Ribordy, W. Tittel y H. Zbinden, Reviews of Modern Physics (2002).

[26] H. K. Lo, M. Curty y K. Tamaki, Secure quantum key distribution (2014).

[27] D. J. Richardson, J. M. Fini y L. E. Nelson, Space-division multiplexing in optical fibres (2013).

[28] S. Inao, T. Sato, S. Sentsui, T. Kuroha y Y. Nishimura (2014).

[29] K. Saitoh y S. Matsuo, Journal of Lightwave Technology (2016).

[30] P. Sillard, M. Bigot-Astruc y D. Molin, Journal of Lightwave Technology **32**, 16 (2014).

[31] G. B. Xavier y G. Lima, Quantum information processing with space-division multiplexing optical fibres (2020).

[32] M. Reck, A. Zeilinger, H. J. Bernstein y P. Bertani, Physical Review Letters (1994).

[33] L. Gan, R. Wang, D. Liu, L. Duan, S. Liu, S. Fu, B. Li, Z. Feng, H. Wei, W. Tong, P. Shum y M. Tang, IEEE Photonics Journal **8**, 1 (2016).

[34] G. Weihs, M. Reck, H. Weinfurter y A. Zeilinger, Optics Letters (1996).

[35] S. Rahimi-Keshari, M. A. Broome, R. Fickler, A. Fedrizzi, T. C. Ralph y A. G. White, Opt. Express **21**, 11 (jun 2013).

[36] K. Watanabe, T. Saito, K. Imamura y M. Shiino, en *Technical Digest - 2012 17th Opto-Electronics and Communications Conference, OECC 2012* (2012).

[37] S. P. Walborn, M. O. Terra Cunha, S. Pádua y C. H. Monken, Physical Review A - Atomic, Molecular, and Optical Physics (2002).

[38] F. A. Torres-Ruiz, G. Lima, A. Delgado, S. Pádua y C. Saavedra, Physical Review A - Atomic, Molecular, and Optical Physics (2010).

[39] P. Bhatnagar y R. K. Nema, Maximum power point tracking control techniques: State-of-the-art in photovoltaic applications (2013).

[40] S. Boyd y L. Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).

[41] M. Farkas, N. Guerrero, J. Cariñe, G. Cañas y G. Lima, Phys. Rev. Appl. **15**, 1 (jan 2021).

[42] 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 y G. Lima, PRX Quantum **2**, 1 (feb 2021).

[43] M. N. Bera, A. Acín, M. Kus, M. W. Mitchell y M. Lewenstein, Randomness in quantum mechanics: Philosophy, physics and technology (2017).

[44] Vlatko Vedral, *Introduction to Quantum Information Science* (Oxford Graduate Texts, 2006).