PHOTONICS Research

Generation of quantum-certified random numbers using on-chip path-entangled single photons from an LED

Nicolò Leone,[1,*] Stefano Azzini,[1] Sonia Mazzucchi,[2] Valter Moretti,[2] Matteo Sanna,[1] Massimo Borghi,[3] Gioele Piccoli,[4] Martino Bernard,[4] Mher Ghulinyan,[4] and Lorenzo Pavesi[1]

[1]Department of Physics, University of Trento, 38122 Trento, Italy
[2]Department of Mathematics and TIFPA, University of Trento, 38122 Trento, Italy
[3]Department of Physics, University of Pavia, 27100 Pavia, Italy
[4]Centre for Sensors and Devices, Fondazione Bruno Kessler, 38123 Povo, Italy
*Corresponding author: nicolo.leone@unitn.it

Received 28 February 2023; revised 5 June 2023; accepted 20 June 2023; posted 21 June 2023 (Doc. ID 488875); published 9 August 2023

Single-photon entanglement is a peculiar type of entanglement in which two or more degrees of freedom of a single photon are correlated quantum-mechanically. Here, we demonstrate a photonic integrated chip able to generate and manipulate single-photon path-entangled states, using a commercial red LED as light source. A Bell test, in the Clauser, Horne, Shimony, and Holt (CHSH) form, is performed to confirm the presence of entanglement, resulting in a maximum value of the CHSH correlation parameter equal to 2.605 ± 0.004. This allows us to use it as an integrated semi-device independent quantum random number generator able to produce certified random numbers. The certification scheme is based on a Bell's inequality violation and on a partial characterization of the experimental setup, without the need of introducing any further assumptions either on the input state or on the particular form of the measurement observables. In the end a min-entropy of 33% is demonstrated.

https://doi.org/10.1364/PRJ.488875

1. INTRODUCTION

Entanglement is one of the most striking features of quantum physics. The non-classical correlations that entanglement induces in quantum states have been debated since 1935, when Einstein, Podolski, and Rosen pointed out what would have been named the EPR paradox after them [1]. It was only several years later that a way out of the impasse was proposed by John Bell. Its famous inequality [2] provides indeed a quantitative solution to effectively demonstrate that correlations induced by entanglement cannot be explained classically using any realistic local-hidden variable. Today entanglement represents a resource in many quantum applications, especially in quantum computing and communications [3–8]. However, its exploitation is mainly limited to research laboratories only, still far from being used in real-life devices. This is mainly due to technological complexities related to its generation and management.

In photonics, entangled photons pairs are typically obtained exploiting non-linear optical processes such as spontaneous parametric downconversion [9] or four-wave mixing [10], using suitable laser sources. On the contrary, single-photon entanglement (SPE) [11] can be more easily generated using only linear optical components and cheap light sources, such as LEDs [12]. SPE corresponds to quantum correlations between two or more degrees of freedom (DoFs) of a single photon. Examples of the possible DoFs used are momentum and polarization [12–15]. From the mathematical point of view, SPE is totally analogous to the entanglement of two photons, or inter-photon entanglement. In both cases, the Hilbert space is determined by the tensor product of two independent Hilbert spaces: in the case of SPE, these are the spaces associated with the two independent DoFs chosen, while, in the case of the inter-photon entanglement, the two spaces are each one associated with one of the two photons. Here, it is important to stress that there is a whole literature on the non-locality of a single photon [16,17] and on single-photon entanglement where the qubit is the occupation state of an optical mode [18,19]. This is a form of inter-photon entanglement. Therefore, it is physically different from what we name here as SPE [13,14]. In SPE, the qubit is not the state of a mode of the electromagnetic field (i.e., no use of photon number or Fock states) but a degree of freedom (i.e., momentum, polarization, path, or others) of a single photon [11]. And indeed, it is from the physical point of view that

the differences are more remarkable. Inter-photon entanglement exhibits a non-local phenomenology, while SPE concerns contextual, but local, observations. The meaning of the violation of the Bell inequality is also different in the two scenarios. In the case of inter-photon entanglement, it means that no realistic local hidden variable theory is able to explain the experiment's results, while, in the case of SPE, it means that no realistic non-contextual hidden variable theory is capable of predicting the results [11]. The fact that SPE is a local phenomenon implies that it cannot be used as a substitute for inter-photon entanglement in many quantum applications. However, there can be specific cases in which, thanks to the easier generation and management aspects, it can be exploited for developing entanglement-based applications with potentially larger diffusion. One of them concerns random number generation.

Random numbers are fundamental resources in many different applications, such as gambling and gaming, lotteries, computer simulation, and cryptography. In cryptography, in particular, the unpredictability of the random sequence ensures the reliability of the encryption protocols. To generate random numbers, random number generators (RNGs) are usually exploited. Among all RNGs, quantum random number generators (QRNGs) [20,21] are the only ones that can generate truly random numbers. Indeed, pseudo-random number generators [22] and true-random number generators [23,24] exploit algorithms and noisy/chaotic processes, respectively, to generate random sequences. While the first ones are not truly random by definition, the second ones involve complex physical processes making randomness certification quite hard to obtain. On the contrary, for QRNGs such a certification is usually easier and can be done even considering malicious and error-prone implementation or an eavesdropper that is attacking the generator. Considering the level of security, QRNGs can be divided into three categories: device-dependent QRNGs (DD-QRNGs), device-independent QRNGs (DI-QRNGs) [8], and semi-device-independent QRNGs (SDI-QRNGs) [20]. DD-QRNGs are less secure, as their randomness certification scheme is based on the perfect characterization of their physical implementation. In perfect conditions, these QRNGs work quite well, but they are unable to cope with any change in their performances, which can possibly alter the produced randomness. DI-QRNGs are instead the most secure QRNGs, since their *a priori* randomness certification is independent by the actual characterization of the physical system involved. However, their physical implementations are still particularly complex and challenging, strongly limiting so far their exploitation to research labs only. The SDI-QRNGs represent a trade-off between the easiness of implementation of the DD-QRNGs and the security of the DI-QRNGs: only limited parts of the physical implementation are characterized, treating the others as black boxes.

In this work we propose a photonic integrated circuit (PIC) able to generate and manipulate single-photon path-entangled states by using typical integrated photonic devices such as multi-mode interferometers (MMIs), thermal phase shifters (PSs), Mach–Zehnder interferometers (MZIs), and crossings (CRs) [25]. The qubit encoding is done using four waveguides: depending on which waveguide the photon is injected, a certain state is codified [26,27]. The presence of entanglement is validated by performing a Bell test [28]. SPE and Bell inequality violation are used to lower-bound the conditional min-entropy of the generated sequence of measurement outcomes. The min-entropy represents the figure of merit to quantify true quantum randomness [29], and its correct estimation is fundamental for each RNG to obtain, from the raw sequence of generated bits, a sequence of uniform random digits using the randomness extraction procedure [30]. In particular, conditional min-entropy can quantify the level of unpredictability, i.e., the security, of the produced sequence of raw bits independently of classical noise sources and of any information potentially accessible to an eavesdropper. In this context, statistical tests such as NIST or Diehard are of secondary importance since they can only check particular statistical properties of the produced random sequence but cannot assess its level of security. The reported PIC implements an SDI-QRNG. The necessary assumptions on which it is based are the use of trusted and characterized detectors and the not-maliciousness of the experimental setup used, which can be, however, considered error-prone. With respect to a previous work from a few of us [15], the SDI-QRNG here proposed is a PIC exploiting an external commercial red LED as a light source and achieving a high value of min-entropy in the most general and secure scenario one can envision, thus making a significant step toward real-world applications.

The paper is organized as follows. In Section 2, we introduce SPE in the case of path entanglement and we detail the structure of the PIC. Then, in Section 3, all the non-idealities of the experiment are considered and their effect on the Bell inequality is taken into account. In Section 5, we present the experimental data that certify the generation of path-entangled states. In Section 6, we present the experimental data demonstrating our SDI-QRNG based on SPE states of path. Finally, in Section 7 we draw the conclusion, and in Section 4 we report the experimental methods.

2. SINGLE-PHOTON PATH-ENTANGLED STATES ON A PIC

Single-photon entangled states are those states in which at least two DoFs of a single photon are quantum correlated. Here we generate single-photon path-entangled states by considering four waveguides and two effective DoFs, namely the absolute ($|U\rangle, |D\rangle$) and the relative ($|F\rangle, |N\rangle$) positions of each waveguide with respect to the symmetry axis of the system (dashed white line in Fig. 1). According to the scheme of Fig. 1, such a Hilbert space can be seen as $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$.

The four states of the Bell basis in such qubit encoding are

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|UF\rangle \pm |DN\rangle), \tag{1}$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|UN\rangle \pm |DF\rangle). \tag{2}$$

In this work, we focus on the state $|\phi^{+}\rangle$. To generate such state, we have designed and fabricated a PIC (a scheme is reported in Fig. 2) based on silicon oxynitride (SiO_xN_y) material, a low-index contrast photonic platform [31]. The structure of the PIC is simple and composed only of linear integrated

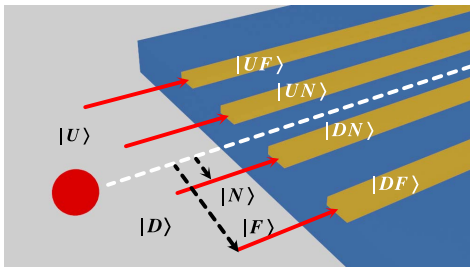

Fig. 1. Qubit encoding. Two qubits describe the system and are encoded according to the absolute and relative positions of the waveguide in which the photon is injected with respect to the dashed white line. The values of the two qubits are fixed using the following bases: absolute position (up $|U\rangle$ and down $|D\rangle$) and relative position (far $|F\rangle$ and near $|N\rangle$).

optical elements: MMIs, PSs, MZIs, and CRs [32,33]. The first part of the PIC (yellow box in Fig. 2) is responsible for generating the SPE state $|\phi^+\rangle$ by exploiting a 50:50 MMI and two PSs setting the relative phase ξ of the entangled state, that, apart from a global non-influent phase, can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|UF\rangle + ie^{i\xi}|DN\rangle), \tag{3}$$

with $\xi = \xi_1 - \xi_2$, where $\xi_{1(2)}$ is the phase induced by the phase shifter applied to $|UF\rangle(|DN\rangle)$ in the generation stage. By tuning ξ, it is eventually possible to precisely obtain the Bell state $|\phi^+\rangle$.

To demonstrate the presence of entanglement, a Bell test [34] in the Clauser, Horne, Shimony, and Holt (CHSH) form [35] is operated. Its aim is to quantify the presence of correlations between suitable measurements performed on the two qubits considered. To run a Bell test, it is necessary to define four measurement operations to be performed on the entangled state and connected to two observables, $\{A(x)\}_{x=0,1}$ and $\{B(y)\}_{y=0,1}$, each one dependent on a binary variable, x and y, respectively. Such measurements must have binary outputs, a and b, which can then assume values $\{\pm 1\}$. In particular, $A(x)$ is an observable that has to be measured only on one qubit, while $B(y)$ only on the other. By defining the correlation coefficient $\mathbb{E}(x,y)$ as

$$\mathbb{E}(x,y) = \mathbb{P}(a = b|x,y) - \mathbb{P}(a \neq b|x,y), \tag{4}$$

where $\mathbb{P}(a = b|x,y)$ is the conditional probability of observing $a = b$ and $\mathbb{P}(a \neq b|x,y)$ is the conditional probability of observing $a \neq b$, it is possible to define the correlation function χ as

$$\chi = \sum (-1)^{xy}\mathbb{E}(x,y). \tag{5}$$

If $|\chi| > 2$, then we are dealing with an entangled state. More precisely, entanglement is a necessary but non-sufficient condition for a state to satisfy such an inequality, while separable states always result in $|\chi| < 2$ [35]. In the PIC, the Bell test is performed by using the other two stages. The two measurement operations $\{A(x)\}_{x=0,1}$ and $\{B(y)\}_{y=0,1}$ are implemented by a combination of four MZIs with the help of two CRs and four single-photon avalanche diodes (SPADs) that are off-chip. In particular, two MZIs work in parallel to rotate the relative-position qubit by an angle ϕ (green box at the center of Fig. 2), while two cascaded MZIs, separated by a pair of CRs, rotate the absolute-position qubit by an angle θ (green box on the right side of Fig. 2), where ϕ and θ correspond to y and x in Eq. (4), respectively. A fair implementation of such rotations requires that the same rotation angle is set for both the MZIs relative to the same qubit. Then, the rotated SPE state is projected over the four states $|UF\rangle, |UN\rangle, |DF\rangle$, and $|DN\rangle$ composing the Hilbert space, by means of four waveguides coupled to four off-chip SPADs. According to this, the observable can be constructed in the following way:

$$A(\theta) = U_1^\dagger(\theta)\sigma_z U_1(\theta), \tag{6}$$

$$B(\phi) = U_2^\dagger(\phi)\sigma_z U_2(\phi), \tag{7}$$

where U_1 is the action of the MZIs that rotate the absolute-position qubit, U_2 represents the action of the MZIs that rotate the relative-position qubit, and σ_z is the z-Pauli matrix. In our PIC, σ_z is represented by the projection on the computational basis $|UF\rangle, |UN\rangle, |DF\rangle$, and $|DN\rangle$. In particular, we recall that the states $|U\rangle$ and $|F\rangle$ are eigenstates of the operator σ_z with eigenvalue $+1$, while $|D\rangle$ and $|N\rangle$ are eigenstates of the operator σ_z with eigenvalue -1. Consequently, the case $a = b$ is obtained every time the wave function collapses on the state $|UF\rangle(a = b = +1)$ or $|DN\rangle(a = b = -1)$. In contrast, the situation $a \neq b$ is obtained when the other states are detected, i.e., $|UN\rangle(a = +1, b = -1)$, $|DF\rangle(a = -1, b = +1)$. Thus,

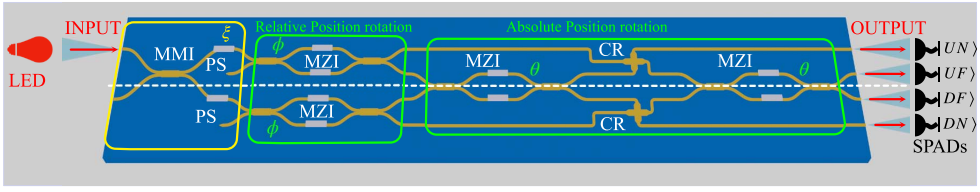

Fig. 2. Schematic representation of the PIC used for random number generation based on SPE. In cyan, the optical waveguides; in blue, the oxide cladding. A red LED is used as a light source. Light coupling in and out of the PIC is performed using tapered optical fibers (transparent cones in the drawing). The PIC can be divided into three parts: generation, relative-position rotation, and absolute-position rotation. The generation stage is enclosed by the yellow rectangle on the left side. Here, the entangled state is created. The relative-position rotation corresponds to the first green rectangle from the left: here two MZIs rotate the qubit of relative position by an angle ϕ. The absolute-position rotation stage is found in the large green rectangle on the right side: here two MZIs rotate the qubit of absolute position by an angle θ. At the output, the rotated state is projected onto one of the four states composing the basis of the four-dimensional Hilbert space: $|UF\rangle, |UN\rangle, |DF\rangle$, and $|DN\rangle$. List of abbreviations: MMI, multimode interferometer; PS, phase shifter; MZI, Mach–Zehnder interferometer; CR, crossing; SPADs, single-photon avalanche diodes.

$$\mathbb{P}(a = b|x, y) = \mathbb{P}(|UF\rangle|\phi, \theta) + \mathbb{P}(|DN\rangle|\phi, \theta), \quad (8)$$

$$\mathbb{P}(a \neq b|x, y) = \mathbb{P}(|UN\rangle|\phi, \theta) + \mathbb{P}(|DF\rangle|\phi, \theta), \quad (9)$$

where $\mathbb{P}(|\mu\nu\rangle|\phi, \theta)$ is the probability of observing the state $|\mu\nu\rangle$ given the pair of angles (ϕ, θ). Such probability can be written as

$$\mathbb{P}(|\mu\nu\rangle|\phi, \theta) = \mathrm{Tr}[U(\phi, \theta)\rho U(\phi, \theta)^\dagger P_\mu \otimes P_\nu], \quad (10)$$

where $U(\phi, \theta) = U_1(\theta) \otimes U_2(\phi)$ is the action of the MZIs in the PIC, $P_\mu \otimes P_\nu$ is the projection operation on the state, and ρ is the density matrix of the state written in the generation stage. Therefore, Eq. (4) becomes

$$\mathbb{E}(\phi, \theta) = \mathbb{P}(|UF\rangle|\phi, \theta) + \mathbb{P}(|DN\rangle|\phi, \theta) - \mathbb{P}(|UN\rangle|\phi, \theta) - \mathbb{P}(|DF\rangle|\phi, \theta). \quad (11)$$

The theoretical form of the correlation coefficient $\mathbb{E}$ and correlation function χ can be calculated introducing the matrix representation of the MZIs. In particular, an MZI is composed of two 50:50 beam splitters, implemented on-chip using MMI devices, separated by two optical waveguides, each one having a PS. In the ideal case, the 50:50 MMI and the PS matrix representations are

$$U_{\mathrm{MMI}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \quad U_{\mathrm{PS}(\zeta_1, \zeta_2)} = \begin{pmatrix} e^{2i\zeta_1} & 0 \\ 0 & e^{2i\zeta_2} \end{pmatrix}. \quad (12)$$

Consequently, according to standard transfer matrix formalism, the matrix representation of the MZI is

$$U_{\mathrm{MZI}}(\zeta_1, \zeta_2) = ie^{i(\zeta_1+\zeta_2)}\begin{pmatrix} \sin(\zeta_1 - \zeta_2) & \cos(\zeta_1 - \zeta_2) \\ \cos(\zeta_1 - \zeta_2) & -\sin(\zeta_1 - \zeta_2) \end{pmatrix} = ie^{iZ}\begin{pmatrix} \sin(\zeta) & \cos(\zeta) \\ \cos(\zeta) & -\sin(\zeta) \end{pmatrix}. \quad (13)$$

Essentially, each MZI implements a rotation of an angle $\zeta = \zeta_1 - \zeta_2$, with a global phase shift of $Z + \pi/2$, with $Z = \zeta_1 + \zeta_2$. Considering the four MZIs represented in Fig. 2, $\zeta_1 = \phi_1, \zeta_2 = \phi_2$ for the two MZIs that rotate the relative-position qubit (first green box from the left in Fig. 2), while $\zeta_1 = \theta_1, \zeta_2 = \theta_2$ for the two MZIs that rotate the absolute-position qubit (second green box from the left in Fig. 2). By implementing two rotations of angles ϕ and θ, respectively, for the relative- and absolute-position qubits, the theoretical form of the correlation coefficient $\mathbb{E}(\phi, \theta)$ becomes

$$\mathbb{E}(\phi, \theta) = \cos(2(\phi - \theta)), \quad (14)$$

and the correlation function $\chi(\phi, \phi', \theta, \theta')$ results to be

$$\chi(\phi, \phi', \theta, \theta') = \cos(2(\phi - \theta)) - \cos(2(\phi - \theta')) + \cos(2(\phi' - \theta)) + \cos(2(\phi' - \theta')). \quad (15)$$

By introducing the parameter α, such that $2(\phi - \theta) = 2(\phi' - \theta') = -2(\phi' - \theta) = \alpha$, the correlation function can be rewritten as

$$\chi(\alpha) = 3\cos(\alpha) - \cos(3\alpha). \quad (16)$$

As shown in Fig. 2, to generate SPE states we use an LED. As explained in detail in Ref. [12], the statistics of the photon source does not affect the estimate of the correlation function χ and the corresponding verification of Bell inequality violation since

- the photon flux is weak enough to yield a fairly low probability of having more than one photon in the time bin of observation;
- only linear optical operations are performed, i.e., any transformation is applied to single photons; and
- the observation is performed by single-photon detectors that are both trusted and can fairly sample the outcome probability distributions.

3. NON-IDEALITIES IN THE EXPERIMENTAL ESTIMATION OF $\chi(\phi, \phi', \theta, \theta')$

Our experimental implementation is affected by a few non-idealities, that in principle could result in a wrong estimation of $\chi(\phi, \phi', \theta, \theta')$. A first aspect to be considered is the broadband spectrum of emission of the LED. Indeed, the PIC has been designed for $\lambda = 730$ nm, so that its performances are optimized at that wavelength. However, the used LED source has a broadband spectrum ($\lambda = 730 \pm 10$ nm), so that the wavelength-dependent behavior of the integrated optical elements has to be taken into account. For example, the matrix representation of the MMIs becomes

$$U_{\mathrm{MMI}}(\lambda) = \begin{pmatrix} t(\lambda) & ir(\lambda) \\ ir(\lambda) & t(\lambda) \end{pmatrix}, \quad (17)$$

and consequently, the matrix representation of the MZIs is correctly described by

$$U_{\mathrm{MZI}}(\lambda, \zeta_1, \zeta_2) = \begin{pmatrix} t(\lambda)^2 e^{2i\zeta_1(\lambda)} - r(\lambda)^2 e^{2i\zeta_2(\lambda)} & ir(\lambda)t(\lambda)(e^{2i\zeta_1(\lambda)} + e^{2i\zeta_2(\lambda)}) \\ ir(\lambda)t(\lambda)(e^{2i\zeta_1(\lambda)} + e^{2i\zeta_2(\lambda)}) & t(\lambda)^2 e^{2i\zeta_2(\lambda)} - r(\lambda)^2 e^{2i\zeta_1(\lambda)} \end{pmatrix}. \quad (18)$$

A second aspect concerns losses. Waveguide propagation losses have to be considered. Moreover, MMIs can have insertion losses, meaning that $t^2(\lambda) + r^2(\lambda) \leq 1$. Finally, a third non-negligible aspect is represented by current instabilities of the electronics controlling the PSs of the PIC. Indeed, a key feature that must be ensured when a Bell test is performed is that each qubit must be rotated independently by the other [28]. More formally, the observables that are considered in a

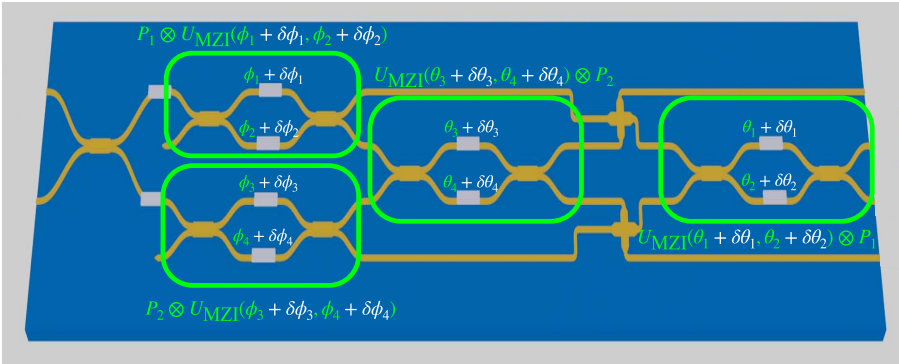

Fig. 3. Schematic representation of the different phases (green) associated with each MZI with the relative phase errors (white). Each green rectangle highlights the rotation operation performed by the considered MZI according to its phases.

Bell test must be written in product form $A(\theta) \otimes B(\phi)$. This is ensured by imposing the same rotation angle on the two MZIs rotating each qubit. To justify the above requirement, let us consider the situation in which all the MZIs are set with different rotation phases (see Fig. 3):

$$U(\phi_1,\phi_2,\phi_3,\phi_4) = P_1 \otimes U_{MZI}(\phi_1,\phi_2) + P_2 \otimes U_{MZI}(\phi_3,\phi_4);$$
$$U(\theta_1,\theta_2,\theta_3,\theta_4) = U_{MZI}(\theta_1,\theta_2) \otimes P_1 + U_{MZI}(\theta_3,\theta_4) \otimes P_2;$$
$$P_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{19}$$

The P_1 and P_2 matrices consider that each MZI rotates a particular part of the SPE state that is generated: considering the upper MZI in the first green box of Fig. 2, it rotates the far and near components of the up part of the state. Consequently, in order to have the equalities

$$U(\phi_1,\phi_2,\phi_3,\phi_4) = I \otimes U_{MZI}(\phi_1,\phi_2), \tag{20}$$

$$U(\theta_1,\theta_2,\theta_3,\theta_4) = U_{MZI}(\theta_1,\theta_2) \otimes I, \tag{21}$$

in such a way that the overall rotation operator takes the form $U(\phi,\theta) = U(\phi) \otimes U(\theta)$, with $\phi = \phi_1 - \phi_2$ and $\theta = \theta_1 - \theta_2$, the necessary requirements on the angles are $\phi_3 = \phi_1$, $\phi_4 = \phi_2$ and $\theta_3 = \theta_1$, $\theta_4 = \theta_2$. However, current instabilities cannot ensure such necessary product form to be implemented. Please note that even thermal cross talk between different PSs of the different MZIs could spoil the required product form. However, this phenomenon has not been observed, so it will be neglected in the following discussion (see Section 4 for further details).

A. Broadband Light Source

Here, we consider the wavelength dependence of the transmission and reflection coefficients of the MMIs (t, r), as well as of the rotation angles $\zeta_{1(2)}$ set via the MZIs. Without any loss of generality, we can represent the state ρ of the incoming photons as a convex superposition of the following form:

$$\rho = \int \rho_\omega \mathrm{d}\mu(\omega), \tag{22}$$

for a suitable probability measure μ over the set of possible frequencies ω, while ρ_ω represents the state of a monochromatic photon. Since the different elements of the PIC have a response which depends explicitly on the frequency ω of the incoming photons, the overall action of the rotation stage can be described by a family of unitary operators $U(\phi,\theta)_\omega$, in such a way that each component ρ_ω appearing in the decomposition Eq. (22) evolves under the action of the operator $U(\phi,\theta)_\omega$:

$$\rho_\omega \mapsto U(\phi,\theta)_\omega \rho_\omega U(\phi,\theta)_\omega^\dagger, \tag{23}$$

and by linearity, the transformation of the general state Eq. (22) is given by

$$\rho \mapsto \int U(\phi,\theta)_\omega \rho_\omega U(\phi,\theta)_\omega^\dagger \mathrm{d}\mu(\omega). \tag{24}$$

The corresponding quantum probabilities are a convex superposition of the following form:

$$\mathbb{P}(a,b|\phi,\theta) = \int \mathbb{P}(a,b|\phi,\theta)_\omega \mathrm{d}\mu(\omega), \tag{25}$$

where

$$\mathbb{P}(a,b|\phi,\theta)_\omega = \mathrm{Tr}[U(\phi,\theta)_\omega \rho_\omega U(\phi,\theta)_\omega^\dagger P_a \otimes P_b]. \tag{26}$$

This is equivalent to saying that each monochromatic component ρ_ω of the generic state Eq. (22) is subject to the measurement of a different pair of observables, $A(\phi)_\omega \otimes B(\theta)_\omega$, associated with specific projection-valued measures (PVMs) $\{P_a^{\theta,\omega} \otimes P_b^{\phi,\omega}\}_{a,b}$:

$$\begin{aligned}\mathbb{P}(a,b|\phi,\theta)_\omega &= \mathrm{Tr}[\rho_\omega P_a^{\theta,\omega} \otimes P_b^{\phi,\omega}] \\ &= \mathrm{Tr}[U(\phi,\theta)_\omega \rho_\omega U(\phi,\theta)_\omega^\dagger P_a \otimes P_b].\end{aligned} \tag{27}$$

Analogously, the Bell parameter χ is given by the convex superposition

$$\chi = \int \chi_\omega \mathrm{d}\mu(\omega), \tag{28}$$

with

$$\chi_\omega = \mathbb{E}_\omega(\phi,\theta) - \mathbb{E}_\omega(\phi,\theta') + \mathbb{E}_\omega(\phi',\theta) + \mathbb{E}_\omega(\phi',\theta'), \tag{29}$$

where

$$\mathbb{E}_\omega(\phi,\theta) = \mathbb{P}(a = b|\phi,\theta)_\omega - \mathbb{P}(a \neq b|\phi,\theta)_\omega. \tag{30}$$

This means that using a broadband light source results in a correlation function which is a spectrally weighted average. It is

important to point out that this fact does not affect the entropy certification protocol (see Section 6 and Appendix C).

Moreover, we want to stress that here the fact that our light source is non-monochromatic does not require the use of a narrowband optical filter for the actual integrated setup as it is the case for the bulk one reported in Ref. [12]. Indeed, thanks to the fact that the phase delay of MZIs is varied by slightly changing the refractive index of the waveguides all the rotation operations naturally occur within the coherence time.

B. Losses

We can consider two types of losses affecting the PIC:

- waveguide propagation losses, that can be viewed as a common factor $e^{-\alpha l}$, where α is the attenuation coefficient and l is the length of the path (waveguide) taken by photons; and
- optical losses specific of each device, due to its insertion in the PIC.

Thanks to the homogeneity of the discrete components and to the symmetry of the PIC, in particular to the nominally equal lengths of the paths corresponding to the four different outputs (detection channels), the overall impact of losses can be modeled by a diagonal operator of the form $L = \gamma I \otimes I$, with $\gamma \in (0,1]$, hence commuting with any operator acting on the 2-qubits Hilbert space. Therefore, the probability of photon detection per channel is given by

$$\mathbb{P}(a,b|\phi,\theta) = \frac{\mathrm{Tr}[U(\phi,\theta)L\rho L^\dagger U(\phi,\theta)^\dagger P_a \otimes P_b]}{\mathrm{Tr}[U(\phi,\theta)L\rho L^\dagger U(\phi,\theta)^\dagger]}, \tag{31}$$

which can be actually cast in the equivalent form

$$\mathbb{P}(a,b|\phi,\theta) = \mathrm{Tr}[U(\phi,\theta)\rho' U(\phi,\theta)^\dagger P_x \otimes P_y], \tag{32}$$

with a different density operator $\rho' := \frac{L\rho L^\dagger}{\mathrm{Tr}[L\rho L^\dagger]}$. In addition, it is even possible to consider the case in which the loss effect depends explicitly on the photons' frequency ω, according to the discussion of the previous subsection. However, as Eq. (32) is of the same form as Eq. (10), we can conclude that this issue does not directly affect the estimate of the correlation function χ.

C. Current Instabilities

In all cases in which electrical currents applied to PSs do not precisely correspond to the desired nominal values, an error ($\delta\zeta$) is introduced for each PS. As a general consequence, the matrices representing the rotation operators implemented by the MZIs are no longer in product form, but they have to be written as follows:

$$\begin{aligned}
&U_{\mathrm{real}}(\phi_1,\phi_2,\delta\phi_1,\delta\phi_2,\delta\phi_3,\delta\phi_4)\\
&= P_1 \otimes U_{\mathrm{MZI}}(\phi_1+\delta\phi_1,\phi_2+\delta\phi_2)\\
&\quad + P_2 \otimes U_{\mathrm{MZI}}(\phi_1+\delta\phi_3,\phi_2+\delta\phi_4);\\
&U_{\mathrm{real}}(\theta_1,\theta_2,\delta\theta_1,\delta\theta_2,\delta\theta_3,\delta\theta_4)\\
&= U_{\mathrm{MZI}}(\theta_1+\delta\theta_1,\theta_2+\delta\theta_2)\otimes P_1\\
&\quad + U_{\mathrm{MZI}}(\theta_1+\delta\theta_3,\theta_2+\delta\theta_4)\otimes P_2.
\end{aligned} \tag{33}$$

Note that, with respect to Fig. 3, we have already introduced the conditions $\phi_3 = \phi_1$, $\phi_4 = \phi_2$ and $\theta_3 = \theta_1$, $\theta_4 = \theta_2$. The terms $\delta\phi_1, \delta\phi_2, \delta\phi_3, \delta\phi_4, \delta\theta_1, \delta\theta_2, \delta\theta_3, \delta\theta_4$ are all different and appear both in the rotation angles $\phi = \phi_1 - \phi_2$ and $\theta = \theta_1 - \theta_2$, as well as in the global phase terms imposed by the MZIs $\Phi = \phi_1 + \phi_2$ and $\Theta = \theta_1 + \theta_2$. P_1 and P_2 are defined in Eq. (19). In this situation the matrix U_{PS} is influenced by the experimental error as

$$U^{\mathrm{real}}_{\mathrm{PS}(\zeta_1,\zeta_2)} = \begin{pmatrix} e^{2i(\zeta_1+\delta\zeta_1)} & 0 \\ 0 & e^{2i(\zeta_2+\delta\zeta_2)} \end{pmatrix}. \tag{34}$$

In general, due to these current instabilities, the effective angle of rotation is different for each PS of each MZI. For clarity, we focus our discussion on the rotation angle ϕ, for which $\delta\zeta_1 = \delta\phi_1, \delta\zeta_2 = \delta\phi_2, \delta\zeta_3 = \delta\phi_3, \delta\zeta_4 = \delta\phi_4$. Then, the same arguments can be applied to current-related non-idealities affecting the other rotation angle θ. We start by representing the real operator describing the rotation of the related qubit in the following form:

$$\begin{aligned}
&U^{\mathrm{real}}(\phi_1,\phi_2,\delta\phi_1,\delta\phi_2,\delta\phi_3,\delta\phi_4)\\
&= P_1 \otimes U_{\mathrm{MMI}} U^{\mathrm{real}}_{\mathrm{PS}(\phi_1,\phi_2,\delta\phi_1,\delta\phi_2)} U_{\mathrm{MMI}}\\
&\quad + P_2 \otimes U_{\mathrm{MMI}} U^{\mathrm{real}}_{\mathrm{PS}(\phi_1,\phi_2,\delta\phi_3,\delta\phi_4)} U_{\mathrm{MMI}}.
\end{aligned} \tag{35}$$

This problem is addressed by using the same techniques reported in [15,36]: we look for an ideal operator that can be written as $I \otimes U^{\mathrm{ideal}}$ whose distance from U^{real} is the smallest possible, i.e., an operator minimizing the distance from $U^{\mathrm{real}}(\phi_1,\phi_2,\delta\phi_1,\delta\phi_2,\delta\phi_3,\delta\phi_4)$ according to the Hilbert–Schmidt norm. Without loss of generality, we can represent U^{ideal} as the product $U^{\mathrm{ideal}} = U_{\mathrm{MMI}} W^{\mathrm{ideal}} U_{\mathrm{MMI}}$, for a suitable unitary operator W^{ideal}. In the general case, the real operator describing the rotation of one qubit by an angle ϕ can be represented as

$$\begin{aligned}
&U^{\mathrm{real}}(\phi_1,\phi_2,\delta\phi_1,\delta\phi_2,\delta\phi_3,\delta\phi_4) = (I \otimes U_{\mathrm{MMI}})\\
&\times (I \otimes U^{\mathrm{ideal}}_{\mathrm{PS}}(\phi_1,\phi_2)) D(\delta\phi_1,\delta\phi_2,\delta\phi_3,\delta\phi_4)(I \otimes U_{\mathrm{MMI}}),
\end{aligned} \tag{36}$$

where

$$D(\delta\phi_1,\delta\phi_2,\delta\phi_3,\delta\phi_4) = \begin{pmatrix} e^{2i\delta\phi_1} & 0 & 0 & 0 \\ 0 & e^{2i\delta\phi_2} & 0 & 0 \\ 0 & 0 & e^{2i\delta\phi_3} & 0 \\ 0 & 0 & 0 & e^{2i\delta\phi_4} \end{pmatrix}. \tag{37}$$

Similarly, we can rewrite the factorized unitary operator U^{ideal}, which minimizes the Hilbert–Schmidt distance from U^{real}, as

$$U^{\mathrm{ideal}} = I \otimes (U_{\mathrm{MMI}} U_{\mathrm{PS}}(\phi_1,\phi_2) V^{\mathrm{ideal}} U_{\mathrm{MMI}}) \tag{38}$$

for a suitable unitary operator V^{ideal}, where $W^{\mathrm{ideal}} = U_{\mathrm{PS}}(\phi_1,\phi_2) V^{\mathrm{ideal}}$. By exploiting the representation of a generic element of SU(2) as the exponential of a Pauli vector, the generic unitary operator V^{ideal} will be written in the form

$$V^{\mathrm{ideal}} = e^{i\varphi} e^{i\vartheta \hat{n}\cdot\sigma} = e^{i\varphi}(\cos\vartheta I + i \sin\vartheta \hat{n}\cdot\sigma), \tag{39}$$

for some $\varphi, \vartheta \in [0,2\pi)$, and $\hat{n} \in \mathbb{R}^3$, $\|\hat{n}\| = 1$. It can be proven (see Appendix B) that for

$$\hat{n} = (0,0,1), \quad \varphi = \frac{\delta\phi_1 + \delta\phi_3 + \delta\phi_2 + \delta\phi_4}{2},$$
$$\vartheta = \frac{\delta\phi_1 + \delta\phi_3 - \delta\phi_2 - \delta\phi_4}{2}, \tag{40}$$

the Hilbert–Schmidt distance from U^{real} is minimum. We remark that the same reasoning can be applied also for current instabilities affecting the angle θ.

Consequently, it is necessary to evaluate

$$e_\chi = \max_{\{\phi,\phi',\theta,\theta',\rho\}} |\chi^{\text{ideal}}(\phi,\phi',\theta,\theta') - \chi^{\text{real}}(\phi,\phi',\theta,\theta')|, \tag{41}$$

which represents a correction term that has to be applied to the experimental correlation function χ^{real}. It takes into account the fact that with U^{real} we are not exactly applying a factorized operator to the state ρ and so we are making the error e_χ. To estimate such a correction term, we use the numerical approach detailed in Ref. [15]. Note that in the construction of $\chi(\phi,\phi',\theta,\theta')$ four correlation coefficients $\{\mathbb{E}_i\}_{i=1,\ldots,4}$ are considered, each of them having different values of the errors $\{\{\delta\phi_{i,j},\delta\theta_{i,k}\}_{j,k=1,\ldots,4}\}_{i=1,\ldots,4}$. To simplify the evaluation, we evaluate $\{e_{\chi,\xi}\}_{\xi=1,\ldots,4}$ considering that the four $\{\mathbb{E}_i\}_{i=1,\ldots,4}$ in χ have the same errors $\{\delta\phi_{\xi,j},\delta\theta_{\xi,k}\}_{j,k=1,\ldots,4}$ of the correlation coefficient $\mathbb{E}_{xi}$.

D. Other Sources of Non-Idealities

Other non-idealities in our experimental setup come from the detectors (dead-time, after-pulsing, and dark counts), especially because no randomization of the input sequence of measurement operations necessary to estimate the probabilities $\{\mathbb{P}(a,b|\phi,\theta)\}_{\phi,\theta,a,b}$ is performed. In this particular implementation we neglect such non-idealities because in Ref. [15] it has been observed that, for a photon flux of $\simeq$200 kHz, the corrections to the probabilities are negligible. As a lower flux of photons $\simeq$120 kHz is here used (mainly because of LED-to-fiber low coupling efficiency), we can safely neglect such a correction factor.

4. METHODS

The PIC has been fabricated in the cleanroom of Fondazione Bruno Kessler. The waveguide core (300 nm thick and 700 nm wide) is made of silicon oxynitride (SiO_xN_y) and the bottom and top claddings are made, respectively, of thermally grown silicon oxide (SiO_2) and borophosphosilicate glass. The design wavelength of the integrated components is 730 nm and the mode polarization is transverse electric (TE). The linear characterization of the building-blocks of the PIC, namely MMIs and CRs, has been carried out using a spectrally filtered supercontinuum laser emitting from 300 to 2000 nm, and details about their performances can be found in Appendix A. The measured insertion loss of a 1 cm long straight waveguide is 27 dB for TE polarization.

Our experiment is performed using an attenuated commercial LED at 730 ± 10 nm. The light coming from the LED is collimated using an objective and polarized using a Glan–Thompson polarizer. A fiber port is used to couple light inside an optical fiber, where light is attenuated by means of a variable optical attenuator and polarization is controlled and set to be TE at the output. The input–output coupling is performed using a standard fiber array. A power supply is used to control the different phase shifters present on the PIC.

Prior to our measurements, a mandatory calibration of integrated MZIs has been performed using a Ti:sapphire laser tuned at 730 nm. In particular, the phase-power relation $\phi = \phi(W)$ of the different MZIs is retrieved by fitting operations of the transmitted optical power using the following equations:

$$I_{\text{out1}} = a\cos(bW + d)^2 + c, \tag{42}$$
$$I_{\text{out2}} = a\sin(bW + d)^2 + c, \tag{43}$$

corresponding to the two output ports of an MZI, where a, b, c, d are fitting parameters. This allows reconstruction of the relation $\phi = \phi(W)$ for each MZI by means of the linear function $\phi(W) = bW + d$. Please note that, to eliminate the thermal cross talk between different MZIs, each PS is encapsulated between trenches (areas in which the core and cladding materials are removed) to limit the heat propagation inside the PIC. This and the low thermal conductivity of the silicon oxide strongly limit the thermal cross talk, making it negligible during the experiment.

The phase $\xi = \xi_1 - \xi_2$ of the generation stage is obtained by another fitting operation, applying the correct calibration to each MZI. Here an issue is due to the absence of additional compensation phase shifters after the MZIs rotating the relative-position qubit. In this situation, the value of ξ to fix the phase difference between the $|N\rangle$ components of the state basis is different with respect to the one for the $|F\rangle$ components. For this reason, the following strategy is introduced. First, we set the value of ξ necessary to have the expected phase relation between the $|F\rangle$ components, and only counts from channels $|UF\rangle$ and $|DF\rangle$ are acquired. Second, the experiment is repeated acquiring only counts from channels $|UN\rangle$ and $|DN\rangle$, by changing ξ to the value that adjusts the phase relation of the $|N\rangle$ components too.

Finally, the measurements to demonstrate our certified QRNG integrated device are performed using four SPADs (Excelitas), whose efficiencies have been equalized using fiber-coupled variable optical attenuators, and whose electrical outputs are sent to a time-tagging electronics (Swabian Instruments) connected to a PC in order to count single-photon detection events for each channel over time. The following procedure has been followed. First, an angle of rotation θ of the absolute-position qubit is fixed and a sweep over ϕ angles of relative position is performed. For each pair (θ,ϕ) of angles, a 1 s time window is acquired with a time bin set at 1 μs for the time tagger. Then, the angle θ is changed and a sweep of the other angle ϕ is again performed. Time bins with no detection events are discarded, while whenever multiple photon detection events are registered at different SPADs within the same time bin, one single event is randomly assigned to one of the four two-qubit states by means of a pseudo-random number generator.

5. EXPERIMENTAL DEMONSTRATION OF THE PRESENCE OF ENTANGLEMENT

The experimental demonstration of the presence of entanglement is performed by fixing the angle $\theta \in [-2,0]$ rad and

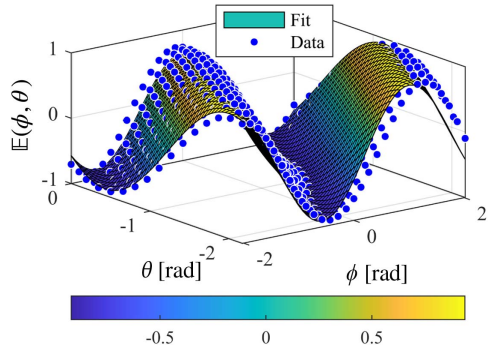

Fig. 4. Experimental correlation coefficients $\mathbb{E}(\phi,\theta)$) (blue dots) with the related fit (colored surface), according to Eq. (45). ϕ is the rotation angle of the relative-position qubit, while θ is the rotation angle of the absolute-position qubit. Color bar refers to the value of $\mathbb{E}$.

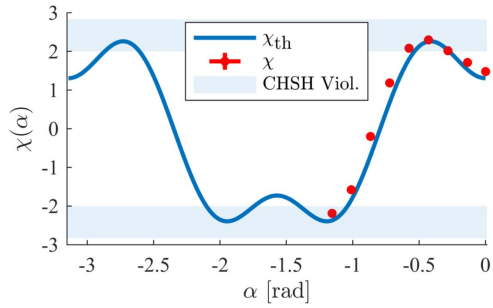

Fig. 5. Experimental demonstration of the violation of the Bell inequality. Data points (red dots) with their error bars (smaller than the size of the data points) and the theoretical curve (blue line) of the χ correlation function, both with respect to the parameter α. In cyan, the areas corresponding to violation of the Bell inequality. Due to a failure of the wire bonding of one PS of one MZI, it was possible to acquire only data points in a limited range of α.

performing a sweep of the rotation angle $\phi \in [-2,2]$ rad. An acquisition 1 s long with a time bin of 1 μs is performed for each (ϕ,θ). The average photons flux is ≃120 kHZ. In this way, we estimate the conditional probabilities $\mathbb{P}(|\mu\nu\rangle|\phi,\theta)$ as the empirical frequencies of the counts:

$$\mathbb{P}(|\mu\nu\rangle|\phi,\theta) = \frac{N_{|\mu\nu\rangle}}{\sum N_{|\mu\nu\rangle}}, \tag{44}$$

where $N_{|\mu\nu\rangle}$ is the number of detected photons in the state $|\mu\nu\rangle$ and $\sum N_{|\mu\nu\rangle}$ is the total number of detected photons. Note that no-detection events are eliminated from the detection sequence, while multiple-detection events are randomly assigned to only one of the detection channels using a pseudo-random number generator. The experimental correlation coefficients $\mathbb{E}(\phi,\theta)$ are reported in Fig. 4 as data points. The colored surface reported in Fig. 4 represents the theoretical correlation coefficient $\mathbb{E}(\phi,\theta)$ in the case of non-ideal 50:50 beam splitters with transmission and reflection power coefficients of $T = 40\%$ and $R = 60\%$, respectively (see Appendix A for the results of our experimental characterization). This results in

$$\begin{aligned}\mathbb{E}(\phi,\theta) = \eta(&5 + (-48)\sqrt{6} + (-24)(5+2\sqrt{6})\cos(2\phi)\\ &+ (-24)(5+2\sqrt{6})\cos(2\theta)\\ &+ 48(30+(-13)\sqrt{6})\cos(2(\phi+\theta))\\ &+ 288(5+2\sqrt{6})\cos(2(\phi-\theta)),\end{aligned} \tag{45}$$

where $\eta = \frac{1}{3125} \simeq 3.2\times10^{-4}$. Instead, by a fit of the experimental data, we obtain $\eta = (3.01 \pm 0.04)\times10^{-4}$. The difference between the theoretical and the fitted η values could be explained by the broadband spectrum of the LED source, since for $\lambda \neq 730$ nm the parameters of the MMI are slightly different.

Using these correlation coefficients, it is possible to construct the correlation function $\chi(\phi,\phi',\theta,\theta')$. By making the choice $\phi = -\alpha, \phi' = \alpha, \theta = 0, \theta' = 2\alpha$, the correlation function can be plotted as a function of the parameter α. The resulting $\chi(\alpha)$ function is reported in Fig. 5 as a blue curve [obtained starting from Eq. (45) with the fitted value of η], while measured data are plotted as red dots. A good agreement

Table 1. Errors on the Rotation Angles ϕ and θ in the Estimation of $\chi^{\pm}$[a]

	$\delta\phi_1$	$\delta\phi_2$	$\delta\phi_3$	$\delta\phi_4$	$\delta\theta_1$	$\delta\theta_2$	$\delta\theta_3$	$\delta\theta_4$
χ^+	0.000	0.011	−0.004	−0.006	0.068	0.216	0.036	0.215
χ^-	0.002	0.004	0.007	−0.006	0.068	0.187	0.036	0.180

[a]The standard error for each value is $\delta = 0.003$ and it is obtained through repeated measurements. Note that the errors on θ are greater than the errors on ϕ. This is due to the fact that one of the heaters enabling the θ rotation was not working.

can be observed. It can also be noticed that the theoretical form of the correlation function does not reach the maximum attainable value of $2\sqrt{2}$: this is caused by the non-ideal transmission and reflection coefficients of the MMIs. However, a clear violation of the CHSH inequality can be observed, reaching a maximum value $\chi^+ = 2.297 \pm 0.004$ and a minimum $\chi^- = -2.181 \pm 0.004$, meaning that single-photon entangled states have been generated. Moreover, it is important to underline that the choice $\phi = -\alpha, \phi' = \alpha, \theta = 0, \theta' = 2\alpha$ gives the maximum achievable Bell inequality violation only if the considered entangled state is exactly $|\phi^+\rangle$. However, due to the fact that the MMI-based beam splitters do not have a 50:50 branching ratio, in our experimental implementation the generated state is actually different. For this reason, it is a better strategy to consider every possible combination of $(\phi,\phi',\theta,\theta')$ between the measured $\mathbb{E}(\phi,\theta)$ to look for a better violation of the inequality. Using this approach, we obtain respectively $\chi^+ = 2.697 \pm 0.004$ for $(\phi_0 = -0.576 \pm 0.002, \phi_1 = -1.445 \pm 0.002, \theta_0 = -1.11 \pm 0.02, \theta_1 = -1.87 \pm 0.02)$ and $\chi^- = -2.668 \pm 0.004$ for $(\phi_0 = -1.589 \pm 0.002, \phi_1 = 0.863 \pm 0.002, \theta_0 = -0.35 \pm 0.02, \theta_1 = -1.27 \pm 0.02)$. Error bars on χ data points are obtained by dividing each 1 s time sequence in intervals of 0.2 s. For each interval, the correlation function is evaluated, and the final uncertainty is obtained as the standard error related to the number of intervals. Lastly, it is necessary to correct the values $\chi^{\pm}$ with the terms $e_{\chi^{\pm}}$ [Eq. (41)]. Using the values of current instabilities-related errors reported in Table 1, we obtain $e_{\chi^+} = 0.092$ for χ^+ and $e_{\chi^-} = 0.077$ for

χ^-. As a result, the corrected values of the correlation functions are $\chi^+ = 2.605 \pm 0.004$ and $\chi^- = -2.591 \pm 0.004$.

6. FROM ENTANGLEMENT TO QUANTUM-CERTIFIED RANDOM NUMBERS

Recently, a few of us demonstrated that it is possible to obtain a semi-device-independent randomness certification scheme starting from SPE states of momentum and polarization using a bulky experimental implementation [15,36]. Therefore, here we use the PIC reported in Fig. 2 as an SDI-QRNG, certified by the evaluation of the correlation function χ.

Using SPE states, the methods of generating quantum-certified random numbers can be schematized in the following way [Fig. 6(a)]: first, a set of angles $\{(\phi_i, \theta_j)\}_{i,j=0,1}$ is selected to evaluate the Bell correlation function $\chi(\phi_0, \phi_1, \theta_0, \theta_1)$. Then, the actual protocol starts. A single-photon path-entangled state is generated. The two qubits that compose the state are rotated by the operation $U(\phi_i, \theta_j)$. The rotated state is projected over the four states $|UF\rangle, |UN\rangle, |DF\rangle$, and $|DN\rangle$. Depending on the outcome of the measurement operation, or equivalently, on the collapsed state, a random digit is obtained according to the following encoding: $|UF\rangle \to 00, |UN\rangle \to 01$, $|DF\rangle \to 10, |DN\rangle \to 11$. Then, the raw random sequence is generated by repeating this procedure many times for each pair of angles. An example of the raw sequence obtained is reported in Fig. 6(b). Note that the pair of angles (ϕ_i, θ_j) can be kept fixed during a long acquisition of detection events. Then the angles could be changed, and a new acquisition would start. This methodology does not require any input randomness and enables the application of an entropy certification protocol similar to the one reported in Refs. [15,36].

First of all, we recall the hypotheses over which our certification scheme is based:

1. SPADs are characterized.
2. A characterization of all the MZIs present on the PIC is available.
3. The power supply that drives the currents to the PSs is error-prone and it is not controlled by an adversary.
4. The generation and measurement parameters must be stable during the acquisition time.

Hypothesis 1 means that the used SPADs are trustworthy and not controlled by an adversary. Moreover, their non-idealities, such as the limited efficiency, the probability of after-pulsing, and the dead time, are known. Such a hypothesis is necessary to fairly reconstruct the probabilities $\mathbb{P}(a, b|\phi_i, \theta_j)$. Indeed, as soon as the pair of angles (ϕ_i, θ_j) is not randomized for every round of the experiment, an adversary could induce detector clicks in a deterministic way to mimic the violation of a Bell inequality. Hypotheses 2 and 3, instead, are necessary to set the same angles ϕ and θ on the different MZIs pairs. In particular, hypothesis 2 is required to take into account the fact that the starting phase of each MZI is not exactly 0, while hypothesis 3 is necessary to set the correct currents at the phase shifters. These hypotheses mean that for each MZI in the PIC, the relation between the rotation angle ξ and the applied power W, $\xi(W) = bW + d$ is known. Moreover, the power supply used is trustworthy and not maliciously controlled by an adversary. However, it can be error-prone, so it can set a power W', slightly different from the selected one, W. Hypothesis 4 is necessary to rule out any possible measurement basis-dependent change of the input state [15]. In practice, this means that when the pair of angles (ϕ_i, θ_j) is fixed and the measurement is performed, the entangled state and the rotations do not change with time, i.e., the phases set by the different PSs do not change. Such a requirement is ensured by selecting a total measurement time short enough that no

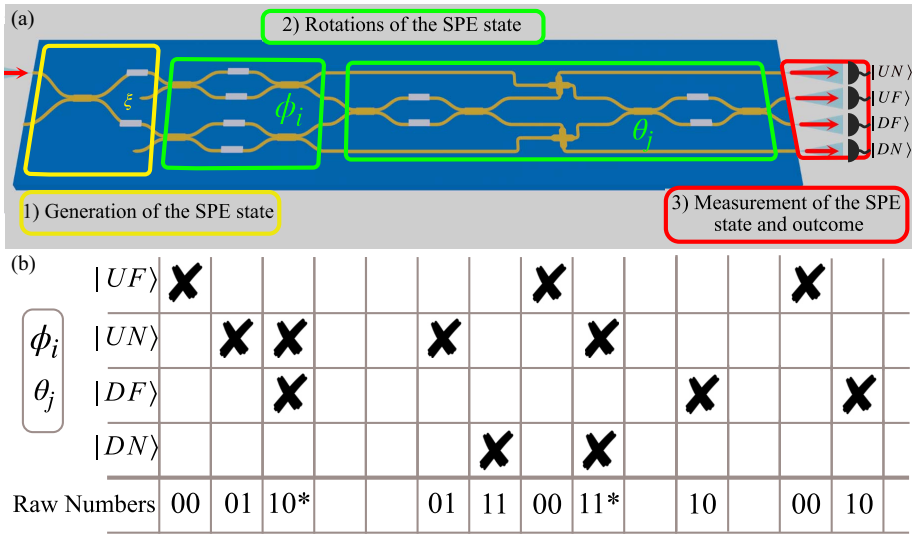

Fig. 6. (a) Method to generate a random number: (1) an SPE state is generated (yellow box); (2) the relative- and absolute-position qubits of the SPE state are rotated respectively by the angles ϕ_i (first green box) and θ_j (second green box) by the different MZIs; (3) the rotated SPE state is measured by state projection on one of the four basis states ($|UF\rangle, |UN\rangle, |DF\rangle, |DN\rangle$) and the clicking SPAD determines the raw number. These steps are repeated many times to generate a raw sequence of random numbers. (b) Example of the random number sequence obtained using the encoding $|UF\rangle \to 00, |UN\rangle \to 01, |DF\rangle \to 10, |DN\rangle \to 11$ given a certain pair (ϕ_i, θ_j). The outcome of multiple detection events is randomized (slots with $*$ in the figure), while time bins with no detection are discarded.

instabilities are observed and by letting the PIC thermalize between different measurements to eliminate any thermal cross talk. Our certification protocol is independent of the particular form of the input state ρ. In particular, for the four sequences of detection events corresponding to the angles $\{(\phi_i, \theta_j)\}_{i,j=0,1}$, the related conditional guessing probability can be bounded by using [15,36]

$$\mathbb{P}_{\text{guess}}(a, b|\phi_i, \theta_j) \leq \frac{1}{2} + \frac{1}{2}\sqrt{2 - (|\chi_{\text{real}}| - e_\chi)^2/4} + e_P, \quad \textbf{(46)}$$

where χ_{real} is the correlation function in the CHSH form estimated from the experimental data. e_χ represents the correction term previously introduced in Section 3. We stress that the maximization procedure for e_χ is run over every possible combination of angles $\{\phi, \phi', \theta, \theta'\}$, in such a way to map every possible operator U^{real}, and over every possible state ρ. e_P is another numerical correction term, which has the same meaning as e_χ but for probabilities instead: it represents an upper bound for the difference between the ideal probabilities obtained by measuring factorized observables and the estimated probabilities obtained in the presence of the non-idealities here considered. e_P is estimated in the same way as e_χ by using the numerical methods described in Ref. [15]. We remind the reader that, with respect to the result reported in Ref. [15], here we are neglecting the Markovian correction to the guessing probability $\mathbb{P}_{\text{guess}}$, introduced to take into account memory effects due to detectors non-idealities, such as after-pulsing and dead time. Indeed, as this work is interested by a lower flux compared to the one reported in that work, the effect of that correction is actually negligible. Note that Eq. (46) is valid even considering the broadband spectrum of our LED source (see the demonstration in Appendix C).

To experimentally demonstrate the generation of certified random numbers we select the time trace of the detection events giving the maximum and minimum violations of the Bell inequality, as reported in Section 5. These are $\chi^+ = 2.697 \pm 0.004$ for $(\phi_0 = -0.576 \pm 0.002, \phi_1 = -1.445 \pm 0.002, \theta_0 = -1.11 \pm 0.02, \theta_1 = -1.87 \pm 0.02)$ and $\chi^- = -2.668 \pm 0.004$ for $(\phi_0 = -1.589 \pm 0.002, \phi_1 = 0.863 \pm 0.002, \theta_0 = -0.35 \pm 0.02, \theta_1 = -1.27 \pm 0.02)$. The time traces of the estimated probabilities used for computing the correlation functions χ^+ and χ^- are reported in Figs. 7(a) and 8(a). These are obtained as 50 ms long averages. As can be observed, the probabilities are quite stable during the entire acquisition time. The values of χ corresponding to these time intervals are then reported in Fig. 7(b) for χ^+ and Fig. 8(b) for χ^-, together with their mean value and related 99% confidence interval (blue shaded region).

Considering these values of violation of Bell inequality and the corresponding values of e_χ, e_P $[e_{\chi^+} = 0.092, e_P(\chi^+) = 0.02$ and $e_{\chi^-} = 0.077, e_P(\chi^-) = 0.014]$, we obtain the following guessing probabilities:

$$\mathbb{P}_{\text{guess}}(a, b|\phi_x, \theta_y) = 0.796 \pm 0.002 \quad \text{for } \chi^+,$$
$$\mathbb{P}_{\text{guess}}(a, b|\phi_x, \theta_y) = 0.798 \pm 0.002 \quad \text{for } \chi^-.$$

Note that the upper bound to $\mathbb{P}_{\text{guess}}(a, b|\phi_x, \theta_y)$ given by Eq. (46) represents the best estimate for the marginal guessing probability, e.g., $\mathbb{P}_{\text{guess}}(b|\theta_y) = \max \sum_a \mathbb{P}_{\text{guess}}(a, b|\phi_x, \theta_y)$,

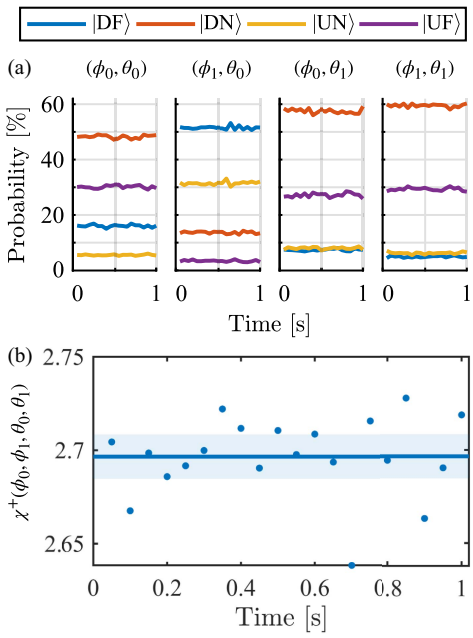

Fig. 7. (a) Probabilities of each measurement outcome as a function of time (blue $|DF\rangle$, red $|DN\rangle$, yellow $|UN\rangle$, and purple $|UF\rangle$) for the four pairs of angles (ϕ_0, θ_0), (ϕ_1, θ_0), (ϕ_0, θ_1), (ϕ_1, θ_1) of χ^+. The estimates have been done considering time intervals of 50 ms. (b) Dots: corresponding values of χ^+ as a function of time. Solid line: mean value of χ^+. Dashed region: 99% confidence interval.

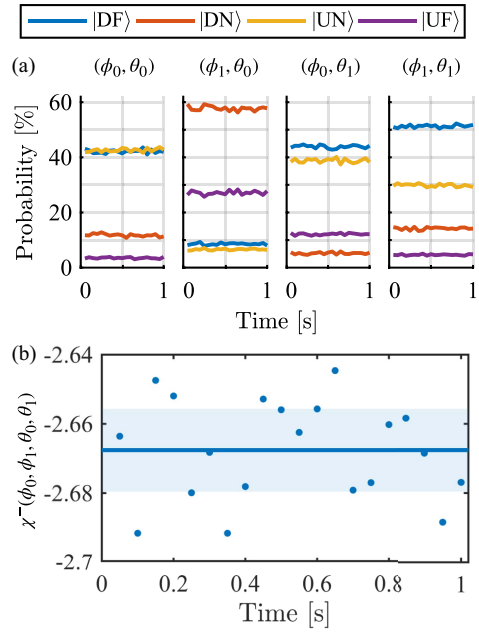

Fig. 8. (a) Probabilities of each measurement outcome as a function of time (blue $|DF\rangle$, red $|DN\rangle$, yellow $|UN\rangle$, and purple $|UF\rangle$) for the four pairs of angles (ϕ_0, θ_0), (ϕ_1, θ_0), (ϕ_0, θ_1), (ϕ_1, θ_1) of χ^-. The estimates have been done considering time intervals of 50 ms. (b) Dots: corresponding values of χ^- as a function of time. Solid line: mean value of χ^-. Dashed region: 99% confidence interval.

where the marginal refers to a single qubit. Therefore, from an operative point of view, in order to refer $H_{\min}$ to a single qubit, we write as bit 0 each photon detected as $|F\rangle$ state independently of its absolute position, and as bit 1 each photon detected as $|N\rangle$ state independently of its absolute position (i.e., 00,10 → 0; 01,11 → 1). By applying the formula [29]

$$H_{\min} = -\log_2(\mathbb{P}_{\text{guess}}(a, b|\phi_x, \theta_y)), \tag{47}$$

we get

$$H_{\min} = (33.0 \pm 0.4)\% \quad \text{for } \chi^+,$$
$$H_{\min} = (32.6 \pm 0.4)\% \quad \text{for } \chi^-.$$

Having used an average rate of 120 kHz for each acquisition, the final rate of our quantum-certified SDI-QRNG is given by $(120 \times H_{\min})$ kHz which, in the best case (namely χ^+), gives a generation rate of ≃40 kHz. This rate does not consider the randomness extraction procedure [30]. We remind the reader that, in this work, we focus on the estimation of $H_{\min}$ and the extraction procedure is not performed. However, by applying a quantum-safe randomness extractor, e.g., Toeplitz-hashing extractor [37] or Trevisan's extractor [38,39], it is mathematically proven that it is possible to obtain a final sequence of independent and uniformly distributed bits up to a given level of accuracy.

7. CONCLUSION

Single-photon path entanglement has been demonstrated in a PIC by measuring the Bell inequality violation in the CHSH formulation. Photons are generated in an off-chip LED, are manipulated in a PIC fabricated in a silicon foundry, and are detected by using off-chip silicon SPADs. The PIC is based on simple and well-known optical components, i.e., MMIs, PSs based on the thermo-optic effect, MZIs, and CRs. Experimental data are well fitted by a theoretical model which considers the non-idealities of our setup, mainly related to unbalanced beam splitters (MMIs). A large violation of the CHSH inequality is reported (2.605 ± 0.004) by recursively trying each possible combination of the acquired correlation coefficients.

These SPE states are used to demonstrate a certified QRNG working accordingly to a semi-device-independent certification protocol similar to the one in Refs. [15,36]. Since in Refs. [15,36] discrete optical components and different degrees of freedom were used, a few assumptions are here different. Specifically, our present approach is based on the knowledge of the single-photon detectors as well as of the integrated MZIs. In addition, the power supply controlling the heaters in the MZIs must be trusted, even if error-prone, as well as the set phase delays must be stable during the acquisition time. No hypothesis is needed on the input state. Under these assumptions, we are able to certify a maximum value of the quantum min-entropy $H_{\min} = (33.0 \pm 0.4)\%$, which is 1 order of magnitude larger than that obtained with a bulk setup [15]. This large improvement is due to the smaller correction terms e_χ and e_P of the integrated QRNG because of the smaller non-idealities in the integrated photonic components with respect to the discrete optical components. To compare the proposed SDI-QRNG to the existing literature, three parameters will be discussed: security, speed, and integration. Concerning security, the proposed QRNG can be compared to source-independent QRNGs, in which the source is left uncharacterized while the measurement operations are fully characterized. Our system is more secure because the performed measurements are only partially characterized. The only requirements are that the measured observables must be in product form, i.e., the measurement performed on one qubit does not influence the other, and they do not change during the experiment. Apart from these assumptions, the particular form of the chosen operator is unimportant. Concerning speed, the achieved generation rate is low compared to the ones reported in the literature. However, this work has focused on demonstrating the generation of certified quantum random numbers using an integrated PIC without optimizing the generation rate. The measured QRNG generation rate (≃40 kHz) is strongly limited by the actual coupling efficiency of the LED to the optical fiber and to the PIC, decreasing the photon flux in the PIC. In future experiments, a better coupling scheme based on, e.g., optimized grating couplers or direct LED bonding could significantly improve the coupling efficiency. Then, the saturation rate of the SPAD detectors will give the other limit. Considering working at the linearity limit of SPADs, i.e., 1 MHz rate, the achievable certified random bit rate is of the order of 330 kHz. To further increase such a value, it is necessary to use engineered detectors, e.g., multiplexing more SPADs in a single detector. The use of silicon photomultipliers (SiPMs), which are arrays of SPADs, could be a viable solution. For example, having four SiPMs composed by 16 SPADs with a linearity limit of 1 MHz, as the one reported in Ref. [40], it is possible to reach a generation rate of ≃5 MHz. By using SiPMs with bigger arrays of SPADs, it is possible to increase the rate further. Another solution relies on the multiplexing of N circuits in the same PIC, using the same light source and dividing it by using an initial $1 \times N$ MMI. Such a solution will require less attenuation of the LED. Moreover, all the circuits act as independent SDI-QRNGs, improving the rate by a factor of N. Last but not least, integration. The proposed QRNG is particularly interesting concerning potential applications. Many works in the literature are based on laser sources which can be fully integrated as well. However, our QRNG uses an LED, which is potentially cheaper to integrate than a laser. This, together with the possibility of co-integration of the SPADs [41,42], enables its use for applications that necessitate low production costs, such as Internet of Things devices.

To conclude, a PIC able to generate quantum certified random numbers using single-photon path-entangled states represents a further step to move semi-device-independent QRNGs from the lab to real-world applications.

APPENDIX A: CHARACTERIZATION OF THE INTEGRATED OPTICAL DEVICES

The characterization of CRs and MMIs has been performed by means of a supercontinuum laser and two tapered optical fibers for in and out coupling to the PIC. Input laser light is TE-polarized using two half-wave plates and one quarter-wave plate. Spectrally resolved detection is done with an optical

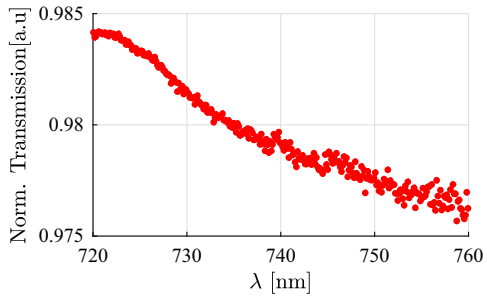

Fig. 9. Measured transmission spectrum of a single crossing in SiON.

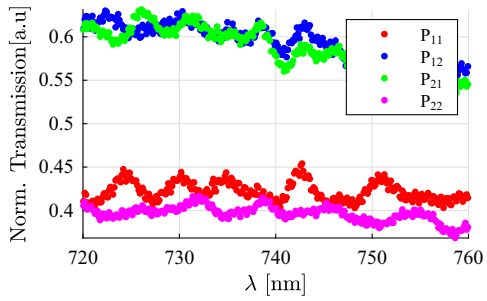

Fig. 10. Measured transmission spectra of an MMI-based integrated beam splitter made of SiON.

spectrum analyzer. The test structure for CR is a sequence of 150 CRs not-equidistant to avoid any Fabry–Perot effect. The transmission spectrum of a single CR normalized to a reference straight waveguide is shown in Fig. 9: a measured power transmission coefficient of ≃98% is reported at 730 nm.

For MMIs, optical power at the two output ports is collected for light entering at both inputs. The experimental data in Fig. 10 are again normalized with respect to a straight waveguide transmission spectrum: P_{ij} indicates the normalized power coefficient of output i with respect to input j. At 730 nm, the transmission coefficients P_{11} and P_{22} are measured to be ≃40%, while the transmission coefficients P_{12} and P_{21} are ≃60%. These are the characterized values entering into hypothesis 2 of our certification protocol.

APPENDIX B: EXPLICIT COMPUTATION OF THE VALUES OF $\hat{n}, \phi, \theta$ THAT MINIMIZE THE HILBERT–SCHMIDT DISTANCE

The square of the Hilbert–Schmidt distance (HS-distance) between U^{ideal} and U^{real} is given by

$$\mathrm{Tr}[(U^{\text{real}} - U^{\text{ideal}})(U^{\text{real}} - U^{\text{ideal}})^\dagger] \tag{B1}$$

$$= 8 - \mathrm{Tr}[D(\delta\phi_1, \delta\phi_2, \delta\phi_3, \delta\phi_4)(I \otimes V^{\text{ideal}})^\dagger + \text{h.c.}]. \tag{B2}$$

Hence, one has to find the optimal parameters $\phi, \vartheta, \hat{n}$ maximizing the term $\mathrm{Tr}[D(\delta\phi_1, \delta\phi_2, \delta\phi_3, \delta\phi_4)(I \otimes e^{i\varphi} e^{i\vartheta \hat{n}\cdot\sigma})^\dagger + \text{h.c.}]$. By direct computation this term is given by

$$\mathrm{Tr}[V^{\text{ideal}} U_1^\dagger + U_1 (V^{\text{ideal}})^\dagger] + \mathrm{Tr}[V^{\text{ideal}} U_2^\dagger + U_2 (V^{\text{ideal}})^\dagger], \tag{B3}$$

with

$$U_1 = \begin{pmatrix} e^{2i\delta\phi_1} & 0 \\ 0 & e^{2i\delta\phi_2} \end{pmatrix}, \tag{B4}$$

$$U_2 = \begin{pmatrix} e^{2i\delta\phi_3} & 0 \\ 0 & e^{2i\delta\phi_4} \end{pmatrix}. \tag{B5}$$

For a particular phase shifter operator of the form

$$U(\alpha, \beta) = \begin{pmatrix} e^{2i\alpha} & 0 \\ 0 & e^{2i\beta} \end{pmatrix} = e^{i(\alpha+\beta)} e^{i(\alpha-\beta)\sigma_z} \tag{B6}$$

and a generic unitary operator $V = e^{i\varphi} e^{i\vartheta \hat{n}\cdot\sigma}$, by using the composition rule in SU(2) one can easily obtain the following formula:

$$\mathrm{Tr}[U(\alpha, \beta) V^\dagger + V U^\dagger(\alpha, \beta)] = 4\cos(\varphi - \alpha - \beta) \times (\cos\vartheta \cos(\alpha - \beta) + n_z \sin\vartheta \sin(\alpha - \beta)). \tag{B7}$$

In particular, we have

$$\begin{aligned} &\mathrm{Tr}\left[V^{\text{ideal}} U_1^\dagger + U_1 (V^{\text{ideal}})^\dagger\right] + \mathrm{Tr}\left[V^{\text{ideal}} U_2^\dagger + U_2 (V^{\text{ideal}})^\dagger\right] \\ &= 4\cos(\varphi - \delta\phi_1 - \delta\phi_2) \\ &\quad \times (\cos\vartheta \cos(\delta\phi_1 - \delta\phi_2) + n_z \sin\vartheta \sin(\delta\phi_1 - \delta\phi_2)) \\ &\quad + 4\cos(\varphi - \delta\phi_3 - \delta\phi_4)(\cos\vartheta \cos(\delta\phi_3 - \delta\phi_4) \\ &\quad + n_z \sin\vartheta \sin(\delta\phi_3 - \delta\phi_4)), \end{aligned} \tag{B8}$$

and we are now concerned with the computation of the triple $(\varphi, \vartheta, n_z)$ maximizing the right-hand side of Eq. (B8). By direct computation, it is possible to prove that the maximum is attained for

$$n_z = 1, \qquad \varphi = \frac{\delta\phi_1 + \delta\phi_3 + \delta\phi_2 + \delta\phi_4}{2}, \qquad \vartheta = \frac{\delta\phi_1 + \delta\phi_3 - \delta\phi_2 - \delta\phi_4}{2},$$

and it is equal to

$$8\cos\left(\frac{\delta\phi_1 - \delta\phi_3}{2} + \frac{\delta\phi_2 - \delta\phi_4}{2}\right)\cos\left(\frac{\delta\phi_1 - \delta\phi_3}{2} - \frac{\delta\phi_2 - \delta\phi_4}{2}\right),$$

while the minimum square HS-distance between U^{real} and U^{ideal} is given by

$$\min_{\varphi, \vartheta, \hat{n}} \| U^{\text{ideal}} - U^{\text{real}} \|_{\text{HS}} = \left(8 - 8\cos\left(\frac{\delta\phi_1 - \delta\phi_3}{2} + \frac{\delta\phi_2 - \delta\phi_4}{2}\right) \times \cos\left(\frac{\delta\phi_1 - \delta\phi_3}{2} - \frac{\delta\phi_2 - \delta\phi_4}{2}\right)\right)^{1/2}, \tag{B9}$$

while the operator U^{ideal} is given by

$$U^{\text{ideal}} = I \otimes (U_{\text{MMI}} U_{\text{Ph}(\phi_1, \phi_2)} V^{\text{ideal}} U_{\text{MMI}}) \tag{B10}$$

with $V^{\text{ideal}} = e^{i\varphi} e^{i\vartheta \hat{n}\cdot\sigma}$ and with $\hat{n} = (0,0,1)$, $\varphi = \frac{\delta\phi_1 + \delta\phi_3 + \delta\phi_2 + \delta\phi_4}{2}$, $\vartheta = \frac{\delta\phi_1 + \delta\phi_3 - \delta\phi_2 - \delta\phi_4}{2}$. The detailed computation can be performed by considering the map $F{:}[0,2\pi) \times [0,2\pi) \times [-1,1] \to \mathbb{R}$ defined as

$$F(\varphi,\vartheta,n_z) := 4\cos(\varphi-\delta\phi_1-\delta\phi_2)(\cos\vartheta\cos(\delta\phi_1-\delta\phi_2) + n_z\sin\vartheta\sin(\delta\phi_1-\delta\phi_2)) + 4\cos(\varphi-\delta\phi_3-\delta\phi_4)(\cos\vartheta\cos(\delta\phi_3-\delta\phi_4) + n_z\sin\vartheta\sin(\delta\phi_3-\delta\phi_4)), \tag{B11}$$

and computing the triple (φ,ϑ,n_z) for which F attains its maximum. To this end, it is convenient to represent F in the equivalent form:

$$F(\varphi,\vartheta,n_z) = f(\varphi)\cos\vartheta + n_z g(\varphi)\sin\vartheta, \tag{B12}$$

where $f:\mathbb{R}\to\mathbb{R}$ and $g:\mathbb{R}\to\mathbb{R}$ are given by

$$f(\varphi) = 4(\cos(\varphi-\delta\phi_1-\delta\phi_2)\cos(\delta\phi_1-\delta\phi_2) + \cos(\varphi-\delta\phi_3-\delta\phi_4)\cos(\delta\phi_3-\delta\phi_4)), \tag{B13}$$

$$g(\varphi) = 4(\cos(\varphi-\delta\phi_1-\delta\phi_2)\sin(\delta\phi_1-\delta\phi_2) + \cos(\varphi-\delta\phi_3-\delta\phi_4)\sin(\delta\phi_3-\delta\phi_4)). \tag{B14}$$

1. First Family of Local Maxima

First of all, we observe that the partial derivative $\frac{\partial F}{\partial n_z}$ is given by

$$\frac{\partial F}{\partial n_z}(\varphi,\vartheta,n_z) = g(\varphi)\sin\vartheta. \tag{B15}$$

Hence, if $(\tilde\varphi,\tilde\vartheta,\tilde n_z)$ is a point where $\frac{\partial F}{\partial n_z}=0$, then

(i) either $\sin\vartheta = 0$,
(ii) or $g(\varphi)=0$.

(i) In the first case, $\cos\vartheta=\pm1$ and the map F reduces to

$$F(\varphi,\vartheta,n_z) = \pm f(\varphi), \tag{B16}$$

where f is given by Eq. (B13).

Actually, it is sufficient to find the value of φ maximizing $f(\varphi)$. Indeed, by the elementary identity $\cos(\varphi+\pi) = -\cos\varphi$, it is trivial to check that both functions f and $-f$ attain the same set of values. By denoting $\varphi_1^* := \arg\max f$, a first local maximum is attained for $\vartheta=0$ and $\varphi=\varphi_1^*$.

The precise value φ_1^* can be obtained by solving the equation $f'(\varphi)=0$, with

$$f'(\varphi) = -4\sin(\varphi-\delta\phi_1-\delta\phi_2)\cos(\delta\phi_1-\delta\phi_2) - 4\sin(\varphi-\delta\phi_3-\delta\phi_4)\cos(\delta\phi_3-\delta\phi_4) = 0. \tag{B17}$$

By direct computation it is easy to find all the solutions of Eq. (B17), which have the form $\varphi_1^*+k\pi$, $k\in\mathbb{Z}$, with

$$\varphi_1^* = \arctan\left(\frac{\sin(\delta\phi_1+\delta\phi_2)\cos(\delta\phi_1-\delta\phi_2)+\sin(\delta\phi_3+\delta\phi_4)\cos(\delta\phi_3-\delta\phi_4)}{\cos(\delta\phi_1+\delta\phi_2)\cos(\delta\phi_1-\delta\phi_2)+\cos(\delta\phi_3+\delta\phi_4)\cos(\delta\phi_3-\delta\phi_4)}\right).$$

Actually, thanks to the small values of the parameters $\delta\phi_1,\delta\phi_2,\delta\phi_3,\delta\phi_4$, the angle φ_1^* satisfies the inequality $|\varphi_1^*|<\pi/2$ and gives a maximum of the function f equal to

$$f(\varphi_1^*) = 4(\cos^2(\delta\phi_1-\delta\phi_2)+\cos^2(\delta\phi_3-\delta\phi_4) + 2\cos(\delta\phi_1-\delta\phi_2)\cos(\delta\phi_3-\delta\phi_4) \times\cos(\delta\phi_1+\delta\phi_2-\delta\phi_3-\delta\phi_4))^{1/2}, \tag{B18}$$

while the angle $\varphi_1^*+\pi$ gives a minimum.

(ii) In the second case, restricting ourselves to those values of the variable φ such that $g(\varphi)=0$, the function F reduces to

$$F(\varphi,\vartheta,n_z) = f|_{g=0}(\varphi)\cos\vartheta. \tag{B19}$$

Since trivially $\max_{g=0}|f|\le\max|f|$ and $|\cos\vartheta|\le1$, the possible local maxima belonging to this set of solutions do not exceed those found in step (i).

2. Second Family of Local Maxima

Another set of points (φ,ϑ,n_z) maximizing locally the function Eq. (B11) can be searched among those for which $n_z=\pm1$. In this case we are concerned with the maximization of the functions

$$G_\pm(\varphi,\vartheta) = f(\varphi)\cos\vartheta \pm g(\varphi)\sin\vartheta, \tag{B20}$$

with f and g defined in Eqs. (B13) and (B14), respectively. Since $G_+(\varphi,2\pi-\vartheta) = G_-(\varphi,\vartheta)$, without loss of generality we can restrict ourselves to the maximization of the function G_+, which can be equivalently written as

$$G_+(\varphi,\vartheta) = 4(\cos(\varphi-\delta\phi_1-\delta\phi_2)\cos(\delta\phi_1-\delta\phi_2-\vartheta) + \cos(\varphi-\delta\phi_3-\delta\phi_4)\cos(\delta\phi_3-\delta\phi_4-\vartheta)). \tag{B21}$$

The local maxima are to be searched among the stationary points of G_+, i.e., among the solutions of the system

$$\begin{cases}\frac{\partial G_+}{\partial\varphi}=0\\ \frac{\partial G_+}{\partial\vartheta}=0\end{cases}. \tag{B22}$$

More specifically,

$$\begin{cases}-\sin(\varphi-\delta\phi_1-\delta\phi_2)\cos(\delta\phi_1-\delta\phi_2-\vartheta)\\ -\sin(\varphi\delta\phi_3-\delta\phi_4)\cos(\delta\phi_3-\delta\phi_4-\vartheta)=0,\\ \cos(\varphi-\delta\phi_1-\delta\phi_2)\sin(\delta\phi_1-\delta\phi_2-\vartheta)\\ +\cos(\varphi-\delta\phi_3-\delta\phi_4)\sin(\delta\phi_3-\delta\phi_4-\vartheta)=0.\end{cases} \tag{B23}$$

By summing and subtracting the two equations above, we get the equivalent system

$$\begin{cases}-\sin(\varphi-2\delta\phi_1+\vartheta)-\sin(\varphi-2\delta\phi_3+\vartheta)=0,\\ \sin(\varphi-2\delta\phi_2-\vartheta)+\sin(\varphi-2\delta\phi_4-\vartheta)=0,\end{cases} \tag{B24}$$

which yields the family of linear systems, labeled by two integers $k, h \in \mathbb{Z}$:

$$\begin{cases} \varphi + \vartheta = \delta\phi_1 + \delta\phi_3 + k\pi, \\ \varphi - \vartheta = \delta\phi_2 + \delta\phi_4 + h\pi, \end{cases} \tag{B25}$$

with solutions

$$\begin{cases} \varphi = \frac{\delta\phi_1+\delta\phi_3+\delta\phi_2+\delta\phi_4}{2} + \frac{k+h}{2}\pi, \\ \vartheta = \frac{\delta\phi_1+\delta\phi_3-\delta\phi_2-\delta\phi_4}{2} + \frac{k-h}{2}\pi. \end{cases} \tag{B26}$$

Under the assumption that the fluctuations $\delta\phi_1, \delta\phi_3$, $\delta\phi_2, \delta\phi_4$ are small, the maximum of the map G_+ is attained at $\varphi = \frac{\delta\phi_1+\delta\phi_3+\delta\phi_2+\delta\phi_4}{2}$, $\vartheta = \frac{\delta\phi_1+\delta\phi_3-\delta\phi_2-\delta\phi_4}{2}$ and it equals to

$$\begin{aligned} &G_+\left(\frac{\delta\phi_1 + \delta\phi_3 + \delta\phi_2 + \delta\phi_4}{2}, \frac{\delta\phi_1 + \delta\phi_3 - \delta\phi_2 - \delta\phi_4}{2}\right) \\ &= 8\cos\left(\frac{\delta\phi_1 - \delta\phi_3}{2} + \frac{\delta\phi_2 - \delta\phi_4}{2}\right) \\ &\quad \times \cos\left(\frac{\delta\phi_1 - \delta\phi_3}{2} - \frac{\delta\phi_2 - \delta\phi_4}{2}\right). \end{aligned} \tag{B27}$$

If the fluctuations $\delta\phi_1, \delta\phi_3, \delta\phi_2, \delta\phi_4$ are small, one can verify that the local maximum Eq. (B27) is greater than the local maximum Eq. (B18). Hence, the absolute maximum is attained for

$$\begin{aligned} n_z = 1, \qquad \varphi &= \frac{\delta\phi_1 + \delta\phi_3 + \delta\phi_2 + \delta\phi_4}{2}, \\ \vartheta &= \frac{\delta\phi_1 + \delta\phi_3 - \delta\phi_2 - \delta\phi_4}{2}. \end{aligned}$$

3. Analytical Bound on the HS Norm

We can now introduce a rather conservative bound by computing the maximum of Eq. (B9) over the admissible range of the phase fluctuations. In particular, by assuming that

$$|\delta\zeta_1| \le \epsilon, |\delta\zeta_2| \le \epsilon, |\delta\zeta_3| \le \epsilon, |\delta\zeta_4| \le \epsilon, \tag{B28}$$

for a suitable constant $\epsilon > 0$, then

$$\max_{\delta\zeta_1, \delta\zeta_2, \delta\zeta_3, \delta\zeta_4} \min_{\varphi, \vartheta, \hat{n}} \|U^{\text{ideal}} - U^{\text{real}}\|_{\text{HS}} \le 2\sqrt{2}(1 - \cos(2\epsilon))^{1/2}. \tag{B29}$$

In particular, by expanding the r.h.s of Eq. (B29) in powers of ϵ and by neglecting the terms ϵ^k of order $k \ge 2$, we eventually get

$$\max_{\delta\zeta_1, \delta\zeta_2, \delta\zeta_3, \delta\zeta_4} \min_{\varphi, \vartheta, \hat{n}} \|U^{\text{ideal}} - U^{\text{real}}\|_{\text{HS}} \le 4\epsilon. \tag{B30}$$

Consider now the two operators

$$U_{\text{real}}(\phi_1, \phi_2, \delta\phi_1, \delta\phi_2, \delta\phi_3, \delta\phi_4) = U_\phi^{\text{real}} \tag{B31}$$

and

$$U_{\text{real}}(\theta_1, \theta_2, \delta\theta_1, \delta\theta_2, \delta\theta_3, \delta\theta_4) = U_\theta^{\text{real}}. \tag{B32}$$

Similarly, the factorized operator minimizing the distance from the U_ϕ^{real} (resp. U_θ^{real}) will be denoted U_ϕ^{ideal} (resp. U_θ^{ideal}). The unitary operator describing the overall action of the rotation stage is given by the product $U_\phi^{\text{real}} U_\theta^{\text{real}}$ and its HS-distance from the product of the two ideal (factorized) operators $U_\phi^{\text{ideal}} U_\theta^{\text{ideal}}$ can be estimated as

$$\begin{aligned} \|U_\phi^{\text{real}} U_\theta^{\text{real}} - U_\phi^{\text{ideal}} U_\theta^{\text{ideal}}\|_{\text{HS}} &\le \|(U_\phi^{\text{real}} - U_\phi^{\text{ideal}})(U_\varphi^{\text{real}} - U_\varphi^{\text{ideal}})\|_{\text{HS}} \\ &+ \|U_\theta^{\text{ideal}}(U_\phi^{\text{real}} - U_\phi^{\text{ideal}})\|_{\text{HS}} + \|(U_\varphi^{\text{real}} - U_\varphi^{\text{ideal}})U_\phi^{\text{ideal}}\|_{\text{HS}} \\ &\le \|(U_\phi^{\text{real}} - U_\phi^{\text{ideal}})\|\|(U_\varphi^{\text{real}} - U_\varphi^{\text{ideal}})\|_{\text{HS}} \\ &+ \|U_\theta^{\text{ideal}}\|\|(U_\phi^{\text{real}} - U_\phi^{\text{ideal}})\|_{\text{HS}} + \|(U_\varphi^{\text{real}} - U_\varphi^{\text{ideal}})\|_{\text{HS}}\|U_\phi^{\text{ideal}}\| \\ &\le \|(U_\phi^{\text{real}} - U_\phi^{\text{ideal}})\|_{\text{HS}}\|(U_\varphi^{\text{real}} - U_\varphi^{\text{ideal}})\|_{\text{HS}} \\ &+ \|(U_\phi^{\text{real}} - U_\phi^{\text{ideal}})\|_{\text{HS}} + \|(U_\varphi^{\text{real}} - U_\varphi^{\text{ideal}})\|_{\text{HS}}. \end{aligned} \tag{B33}$$

In particular, by assuming that the phase fluctuations have maximum amplitude ϵ and by neglecting the terms ϵ^k of order $k \ge 2$, we get the final estimate:

$$\max_{\delta\phi_i, \delta\theta_j} \min_{\varphi, \vartheta, \hat{n}} \|U^{\text{ideal}} - U^{\text{real}}\|_{\text{HS}} \le 8\sqrt{2}\epsilon. \tag{B34}$$

APPENDIX C: ENTROPY CERTIFICATION BASED ON BELL INEQUALITY VIOLATION

For clarity, in the following discussion we identify the guessing probability of the main text $\mathbb{P}_{\text{guess}}$ with G to better distinguish it from the probabilities indicated as $\mathbb{P}$. The relevant figure of merit of a device-independent certification protocol based on CHSH violation is the (realization-independent) quantum guessing probability $G(\mathbb{P})$ associated with a (quantum) probability distribution $\{\mathbb{P}(x,y)\}_{x,y=\pm1}$ defined as

$$G(\mathbb{P}) := \sup_{\{\tilde{\rho}, A, B\} \in R(\mathbb{P})} G(\tilde{\rho}, A, B), \tag{C1}$$

where the family $R(\mathbb{P})$ contains all possible realizations $\{\tilde{\rho}, A, B\}$ compatible with $\mathbb{P}$, i.e., all pairs of quantum states $\tilde{\rho}$ and product observables $A \otimes B$, each with two possible outcomes $x, y \in \{\pm 1\}$, such that

$$\mathbb{P}(x,y) = \text{Tr}[\tilde{\rho} P_x^A \otimes P_y^B], \quad x, y = \pm 1, \tag{C2}$$

$\{P_x^A\}_{x=\pm1}$ and $\{P_y^B\}_{y=\pm1}$ being the PVMs associated with A and B, respectively. The corresponding min-entropy is defined as $H_{\min} := -\log_2(G(\mathbb{P}))$.

For a generic mixed state ρ the average guessing probability $G(\tilde{\rho}, A, B)$ appearing on the r.h.s of Eq. (C1) is defined as

$$G(\tilde{\rho}, A, B) = \sup \int G(\psi_\lambda, A, B) \mathrm{d}\nu(\lambda), \tag{C3}$$

where the supremum is taken over all decompositions $\rho = \int |\psi_\lambda\rangle\langle\psi_\lambda| \mathrm{d}\nu(\lambda)$ of ρ into an incoherent superposition of pure states $|\psi_\lambda\rangle$ (ν being a probability measure), while

$$G(\psi_\lambda, A, B) := \max_{(x,y)} \text{Tr}[|\psi_\lambda\rangle\langle\psi_\lambda| P_x^A \otimes P_y^B]. \tag{C4}$$

Giving a pure state $|\psi\rangle$ and two pairs of observables A_1, A_2, and B_1, B_2 yielding a value χ for the correlation function

$$\chi = \langle A_1 \otimes B_1\rangle_\psi + \langle A_1 \otimes B_2\rangle_\psi + \langle A_2 \otimes B_1\rangle_\psi - \langle A_2 \otimes B_2\rangle_\psi, \tag{C5}$$

the inequality $G(\psi_\lambda, A_i, B_j) \le f(\chi)$, with $f(x) = \frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{x^2}{4}}$, holds true for any $i,j = 1,2$ [8,43]. By the concavity of the function f, this inequality can be generalized to the case of convex superpositions of pure states of the form $\rho = \int |\psi_\lambda\rangle\langle\psi_\lambda| \mathrm{d}\nu(\lambda)$, even considering the case of two pairs of

observables $A(\lambda)_1, A(\lambda)_2$ and $B(\lambda)_1, B(\lambda)_2$ explicitly depending on the parameter λ and yielding a CHSH parameter χ_λ:

$$\chi_\lambda = \langle A_1^\lambda \otimes B_1^\lambda \rangle_{\psi_\lambda} + \langle A_1^\lambda \otimes B_2^\lambda \rangle_{\psi_\lambda} + \langle A_2^\lambda \otimes B_1^\lambda \rangle_{\psi_\lambda} - \langle A_2^\lambda \otimes B_2^\lambda \rangle_{\psi_\lambda}. \tag{C6}$$

In particular,

$$\max_{(x,y)} \int \mathrm{Tr}[|\psi_\lambda\rangle\langle\psi_\lambda| P_x^{A(\lambda)_i} \otimes P_y^{B(\lambda)_j}] \mathrm{d}\nu(\lambda) \tag{C7}$$

$$\leq \int \max_{(x,y)} \mathrm{Tr}[|\psi_\lambda\rangle\langle\psi_\lambda| P_x^{A(\lambda)_i} \otimes P_y^{B(\lambda)_j}] \mathrm{d}\nu(\lambda) \tag{C8}$$

$$\leq \int f(\chi_\lambda) \mathrm{d}\nu(\lambda) \leq f\left(\int \chi_\lambda \mathrm{d}\nu(\lambda)\right) = f(\chi). \tag{C9}$$

The chain of inequalities above, the concavity of the function f, and the explicit dependence of the final term in Eq. (C9) only on the parameter χ, i.e., a function of the probability distributions $\{\mathbb{P}^{i,j}(x,y)\}_{x,y=\pm 1}$ independent of their particular quantum realizations, allow one to prove the final bound for the quantum guessing probability of each of the four distributions $\{\mathbb{P}^{i,j}(x,y)\}_{x,y=\pm 1}$:

$$G(\mathbb{P}^{i,j}) \leq f(\chi), \qquad \forall\ i,j = 1,2. \tag{C10}$$

Inequality (C10) is actually robust under a generalization of definition Eq. (C3). Indeed, thanks to the discussion leading to Eq. (C9), for each quantum probability distribution $\{\mathbb{P}(x,y)\}_{x,y=\pm 1}$ one can consider a larger set of realizations allowing one, at least in principle, to change observables according to the different components of a mixed state. More precisely, given a quantum state ρ and any decomposition $\rho = \int |\psi_\lambda\rangle\langle\psi_\lambda| \mathrm{d}\nu(\lambda)$, one can consider corresponding product observables $A(\lambda) \otimes B(\lambda)$ such that

$$\mathbb{P}(x,y) = \int \mathrm{Tr}[|\psi_\lambda\rangle\langle\psi_\lambda| P_x^{A(\lambda)} \otimes P_y^{B(\lambda)}]. \tag{C11}$$

Funding. Horizon 2020 Framework Programme (899368, 820405).

Acknowledgment. This project has been supported by PAT via Q@TN, the joint lab between University of Trento, FBK-Fondazione Bruno Kessler, INFN-National Institute for Nuclear Physics and CNR-National Research Council.

Disclosures. L. P., V. M., and S. M. declare the following competing interests: a patent has been filed on single-photon entanglement.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Phys. Rev. **47**, 777–780 (1935).
2. J. Bell, "On the Einstein-Rosen-Podolsky paradox," Physica **1**, 195–200 (1964).
3. M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2002).
4. C. Macchiavello, "On the role of entanglement in quantum information," Physica A **338**, 68–75 (2004).
5. C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," Phys. Rev. Lett. **69**, 2881–2884 (1992).
6. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
7. A. Ekert, R. Jozsa, and P. Marcer, "Quantum algorithms: entanglement-enhanced information processing and discussion," Philos. Trans. R. Soc. London A **356**, 1769–1782 (1998).
8. S. Pironio, A. Acn, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).
9. S. Magnitskiy, D. Frolovtsev, V. Firsov, P. Gostev, I. Protsenko, and M. Saygin, "A SPDC-based source of entangled photons and its characterization," J. Russ. Laser Res. **36**, 618–629 (2015).
10. H. Takesue and K. Inoue, "Generation of polarization-entangled photon pairs and violation of Bell's inequality using spontaneous four-wave mixing in a fiber loop," Phys. Rev. A **70**, 031802 (2004).
11. S. Azzini, S. Mazzucchi, V. Moretti, D. Pastorello, and L. Pavesi, "Single-particle entanglement," Adv. Quantum Technol. **3**, 2000014 (2020).
12. M. Pasini, N. Leone, S. Mazzucchi, V. Moretti, D. Pastorello, and L. Pavesi, "Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp," Phys. Rev. A **102**, 063708 (2020).
13. M. Michler, H. Weinfurter, and M. Z. Żukowski, "Experiments towards falsification of noncontextual hidden variable theories," Phys. Rev. Lett. **84**, 5457–5461 (2000).
14. B. R. Gadway, E. J. Galvez, and F. De Zela, "Bell-inequality violations with single photons entangled in momentum and polarization," J. Phys. B **42**, 015503 (2009).
15. N. Leone, S. Azzini, S. Mazzucchi, V. Moretti, and L. Pavesi, "Certified quantum random-number generator based on single-photon entanglement," Phys. Rev. Appl. **17**, 034011 (2022).
16. S. M. Tan, D. F. Walls, and M. J. Collett, "Nonlocality of a single photon," Phys. Rev. Lett. **66**, 252–255 (1991).
17. S. Van Enk, "Single-particle entanglement," Phys. Rev. A **72**, 064306 (2005).
18. H.-W. Lee and J. Kim, "Quantum teleportation and Bell's inequality using single-particle entanglement," Phys. Rev. A **63**, 012305 (2000).
19. P. Caspar, E. Oudot, P. Sekatski, N. Maring, A. Martin, N. Sangouard, H. Zbinden, and R. Thew, "Local and scalable detection of genuine multipartite single-photon path entanglement," Quantum **6**, 671 (2022).
20. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).
21. X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Inf. **2**, 16021 (2016).
22. F. James and L. Moneta, "Review of high-quality random number generators," Comput. Softw. Big Sci. **4**, 2 (2020).
23. H. Zhun and C. Hongyi, "A truly random number generator based on thermal noise," in *4th International Conference on ASIC Proceedings* (IEEE, 2001), pp. 862–864.
24. Y. Hu, X. Liao, K.-W. Wong, and Q. Zhou, "A true random number generator based on mouse movement and chaotic cryptography," Chaos Solitons Fractals **40**, 2286–2293 (2009).
25. L. Vivien and L. Pavesi, *Handbook of Silicon Photonics* (Taylor & Francis, 2016).
26. J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, V. Zwiller, G. D. Marshall, J. G. Rarity, J. L. O'Brien, and M. G. Thompson, "On-chip quantum interference between silicon photon-pair sources," Nat. Photonics **8**, 104–108 (2014).
27. J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acn, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, "Multidimensional quantum entanglement with large-scale integrated optics," Science **360**, 285–291 (2018).

28. V. Scarani, *Bell Nonlocality*, Oxford Graduate Texts (Oxford University, 2019).
29. R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Trans. Inf. Theory **55**, 4337–4347 (2009).
30. N. Nisan and A. Ta-Shma, "Extracting randomness: a survey and new constructions," J. Comput. Syst. Sci. **58**, 148–173 (1999).
31. G. Piccoli, M. Sanna, M. Borghi, L. Pavesi, and M. Ghulinyan, "Silicon oxynitride platform for linear and nonlinear photonics at NIR wavelengths," Opt. Mater. Express **12**, 3551–3562 (2022).
32. L. B. Soldano and E. C. Pennings, "Optical multi-mode interference devices based on self-imaging: principles and applications," J. Lightwave Technol. **13**, 615–627 (1995).
33. B. E. Saleh and M. C. Teich, *Fundamentals of Photonics* (Wiley, 2019).
34. J. Bell, *The Theory of Local Beables. Speakable and Unspeakable in Quantum Mechanics* (Springer, 1974).
35. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," Phys. Rev. Lett. **23**, 880–884 (1969).
36. S. Mazzucchi, N. Leone, S. Azzini, L. Pavesi, and V. Moretti, "Entropy certification of a realistic quantum random-number generator based on single-particle entanglement," Phys. Rev. A **104**, 022416 (2021).
37. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics **2**, 728–732 (2008).
38. L. Trevisan, "Extractors and pseudorandom generators," J. ACM **48**, 860–879 (2001).
39. A. De, C. Portmann, T. Vidick, and R. Renner, "Trevisan's extractor in the presence of quantum side information," SIAM J. Comput. **41**, 915–940 (2012).
40. N. Leone, D. Rusca, S. Azzini, G. Fontana, F. Acerbi, A. Gola, A. Tontini, N. Massari, H. Zbinden, and L. Pavesi, "An optical chip for self-testing quantum random number generation," APL Photonics **5**, 101301 (2020).
41. N. J. Martinez, M. Gehl, C. T. Derose, A. L. Starbuck, A. T. Pomerene, A. L. Lentine, D. C. Trotter, and P. S. Davids, "Single photon detection in a waveguide-coupled Ge-on-Si lateral avalanche photodiode," Opt. Express **25**, 16130–16139 (2017).
42. M. Bernard, F. Acerbi, G. Paternoster, G. Piccoli, L. Gemma, D. Brunelli, A. Gola, G. Pucker, L. Pancheri, and M. Ghulinyan, "Top-down convergence of near-infrared photonics with silicon substrate-integrated electronics," Optica **8**, 1363–1364 (2021).
43. A. Acn, S. Massar, and S. Pironio, "Randomness versus nonlocality and entanglement," Phys. Rev. Lett. **108**, 100402 (2012).