

Four-qubit photonic system for publicly verifiable quantum random numbers and generation of public and private key

Mayalakshmi Kolangatt¹, Anirudh Verma¹, Sujai Matta¹, Kanad Sengupta¹, and C. M. Chandrashekar^{1,2,3,*}

¹*Quantum Optics & Quantum Information, Department of Instrumentation and Applied Physics, Indian Institute of Science, Bengaluru 560012, India*

²*The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India*

³*Homi Bhabha National Institute, Training School Complex, Anushakti Nagar, Mumbai 400094, India*



(Received 12 June 2024; accepted 26 August 2024; published 16 September 2024)

We theoretically propose and experimentally demonstrate the use of a configurable four-qubit photonic system to generate publicly verifiable quantum random numbers, to perform entanglement verification, and to generate a secure public and private key. Quantum circuits, to generate the desired four-qubit states and its experimental realization in the photonic architecture, are carried out using photon pairs entangled in polarization and path degrees of freedom. By performing measurements on the four-qubit system and accessing partial information of the four-qubit state for public verification, we generate publicly verified and purely secured random bits at the rate of 185 kbps from collective data of 370 kbps. When the system is used for generating public and private keys, an equal number of public and private keys are generated simultaneously. We also record about 97.9% of sampled bits from four-qubit states passing entanglement verification and demonstrate the use of public and private key generated for image encryption-decryption. The theoretical model of noise on the four-qubit state and its effect on the generation rate of verified and secured bits are in perfect agreement with the experimental results. This demonstrates the practical use of the small-scale multiqubit photonic system for quantum-safe applications by providing the option for real-time verification of the security feature of the quantum system.

DOI: [10.1103/PhysRevA.110.032615](https://doi.org/10.1103/PhysRevA.110.032615)

I. INTRODUCTION

Randomness generators are a very crucial resource and we employ them readily in our everyday computational and communication activities, including cryptography [1,2], scientific simulations, gaming, statistical sampling, and many others [3,4]. Most of the random number generators that are employed today for practical use are sourced from algorithms on a classical computer. With a knowledge of the algorithm and the initial input, the random sequence can be vulnerable to prediction and hence they are not true random number generators (TRNGs). They are better classified as pseudo-random number generators (PRNG) [5–7]. Ideally, the output of the random number generator should adhere to the principles of uniform distribution and independence. Several statistical tests exist that can verify the randomness of the observed sequence [8–10]. Despite passing all statistical tests, it is nearly impossible to distinguish between a random sequence from a PRNG and a genuinely random sequence, TRNGs. This is because true randomness cannot be generated and certified using classical methods. The inherent probabilistic nature of quantum physics enables the generation of true randomness from a quantum system [11,12]. Hence, a quantum system is becoming a new standard of being an optimal source for generating genuine random numbers [13–15]. Moreover, the principles of quantum mechanics can be applied to assess the quality of these random numbers. Quan-

tum technologies have progressed to the point where this can be achieved. Different schemes of quantum random number generators (QRNGs) have been demonstrated using various quantum sources as resources for randomness [13]. Entangled and single photons from the spontaneous parametric down-conversion (SPDC) process [16,17] and single-photon's entanglement states [18–21] have also been used to generate quantum random numbers. Depending on the method and characterization of the devices used for QRNG, the protocols are broadly classified into the following categories, namely, trusted device, semi-device-independent sources [13], and device-independent sources [22,23]. Current QRNGs are trusted devices, next-generation self-testing, and semi-self-testing QRNGs are under development, and selecting a QRNG method requires considering multiple factors based on user needs [24].

In addition to generating genuine random numbers, subjecting the random bit sequence to public verification is very important to ensure the trustworthiness of the device to the beneficiary. This would involve a third party accessing the bit string and performing a randomness test resulting in a compromise of the secrecy of the generated bit. Even though entangled photon pairs are used for generating certified quantum random numbers, using one of the entangled photons for public verification of randomness will make it vulnerable to the secrecy of the bit generated by the other photon due to the quantum correlation between the photons. Recently, the scheme for using a multiqubit entangled state which will allow public verification without compromising on the secrecy of the undisclosed bit has been proposed [25,26] and

*Contact author: chandracm@iisc.ac.in

its experimental demonstration using entangled photon pairs in three-qubit configuration has been reported [27].

In this work, we present a configurable four-qubit photonic system in the framework of a quantum circuit. A particular configuration of two photons entangled in polarization and path degrees of freedom is generated using polarization-entangled state [28] as the initial state is further configured to generate entanglement in path degree. We experimentally demonstrate the use of the four-qubit photonic system to generate publicly verifiable quantum random numbers without compromising on the secrecy of the undisclosed bits. The random numbers obtained from the scheme pass all the randomness tests in the NIST test suite [10]. We also show that different configurations of the four-qubit state can be prepared to demonstrate entanglement verification with access to sample space of all four strings generated and to two of the four strings of bits generated in real time, respectively. In addition, we also show that the four-qubit entangled state generated can serve as two entangled subsystems with access of one photon to each subsystem and use it to simultaneously generate private and public keys for secure communication between the two subsystem. Theoretical model of noise on the four-qubit state and its effect on the generation rate of verified and secured bits are numerically analyzed and shown to be in perfect agreement with the experimental results. This demonstrates the practical use of small-scale photonic quantum computers for multiple quantum-safe applications by providing the option for real-time verification of the genuine and verifiable security feature of the multiqubit quantum system.

II. THEORETICAL DESCRIPTION

A. Publicly verifiable quantum random numbers

A state from the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is said to be entangled if it is impossible to represent the state as a single product $|a\rangle \otimes |b\rangle$, where $|a\rangle \in \mathcal{H}_1$ and $|b\rangle \in \mathcal{H}_2$. Generalization of tensor product to n number of qubits leads to quantum entanglement of n qubits. In a mutually entangled state of $n > 2$ qubits, measurement in any one subsystem reduces partial entanglement, that is, the remaining qubits are entangled. The outcomes of local measurement in the next subsystem stay random with no correlation with the first subsystem [25]. A special class of entangled states that have two properties [(a) the state is in a superposition of all multiqubit states with the same parity and (b) the probability of each multiqubit state is equal] is used as a resource for publicly verifiable QRNG (PVQRNG). The most general four-qubit state satisfying the above two properties is given by

$$|\Phi_4^{\alpha_1 \dots \alpha_7}\rangle = \frac{1}{2\sqrt{2}}(|0000\rangle + e^{i\alpha_1}|0011\rangle + e^{i\alpha_2}|0101\rangle + e^{i\alpha_3}|0110\rangle + e^{i\alpha_4}|1001\rangle + e^{i\alpha_5}|1010\rangle + e^{i\alpha_6}|1100\rangle + e^{i\alpha_7}|1111\rangle), \quad (1)$$

where $\alpha_i \in R$ for parity 0.

One of the configurations of the quantum circuit to generate a four-qubit entangled state for generating the four-bit string from the measurement outcome is shown in Fig. 1. That is, a simple form of a four-qubit entangled state for PVQRNG

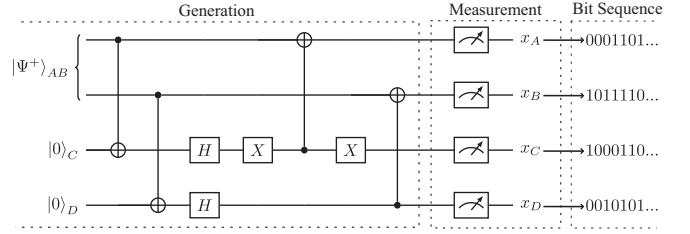


FIG. 1. Quantum circuit for generating four-qubit entangled state using two-qubit entangled state $|\Psi^+\rangle$. A general output quantum state for this setup is a four-qubit entangled state of the form given in Eq. (2).

can be prepared using the sequence of unitary operations on the initial state $|\Psi\rangle_0 = |\Psi^+\rangle|00\rangle$ with $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{12} + |10\rangle_{12})$.

The state generated before the measurement is performed will be

$$|\Psi\rangle_{ABCD} = \frac{1}{2\sqrt{2}}(|0000\rangle + |0101\rangle + |0110\rangle - |0011\rangle + |1100\rangle - |1001\rangle - |1010\rangle - |1111\rangle). \quad (2)$$

The above state can be rewritten as

$$|\Psi\rangle_{ABCD} = \frac{1}{2\sqrt{2}}(|0\rangle_A \otimes (|000\rangle + |101\rangle + |110\rangle - |011\rangle)_{BCD} + |1\rangle_A \otimes (|100\rangle - |001\rangle - |010\rangle - |111\rangle)_{BCD}). \quad (3)$$

This indicates that in a measurement of any single qubit from the entangled set of four, the remaining three qubits acquire an entangled state of a similar form as the four qubit. The obtained sequences of output from the measurement on each qubit, though unconditionally random, are correlated via XOR relation

$$X_A(i) \oplus X_B(i) \oplus X_C(i) \oplus X_D(i) = 0 \quad (4)$$

for all the permutations of the indices. The quantum entanglement distinguishes them for any set of four sequences, where three are produced by an independent random number generator and the fourth one by XOR operation. In this case, the randomness of the three generated sequences must be proved. This distinguishes our case, where the randomness in each string is intact. The precise statistical coupling in the sequences lies in the symmetry of the n -qubit entangled states (for $n > 3$). In simpler terms, when measurements are performed on these entangled states, the resulting binary sequences, while distinct, exhibit identical statistical properties (entropy) [26]. In the Appendix A, we have shown the quantum circuit for generation other configuration of four-qubit state for PVQRNG.

Public randomness verification. Standard QRNG produces a single sequence of bits which are inherently random, but there exists no method to verify it without accessing the information. However, when we use a four-qubit entangled state of the form given in Eq. (2), the measurement output gives the sequence of bits x_A , x_B , x_C , and x_D . Repeated measurement on identical four-qubit states gives four sequences of output on qubits A, B, C, and D given by X_A , X_B , X_C , and

X_D , respectively. These variables are mutually independent pairwise, $I(X_i, X_j) = 0$, for $i, j = A, B, C, D$. Therefore, randomness verification of X_i ensures the quality of randomness on the other sequences without explicitly analyzing them. However, the configuration of the four-qubit entanglement ensures that the projective measurement in the computational basis of each subsystem, the random variables for each subsystem will be either 0 or 1, which are denoted as x_A, x_B, x_C , and x_D and obey the relation

$$x_A \oplus x_B \oplus x_C \oplus x_D = 0, \quad (5)$$

where $\oplus$ represents the addition modulo 2 operator. This tells us that the knowledge of any three bits of information helps in the recovery of the fourth bit leaving it vulnerable to privacy of the random bits generated. To address this concern, one of the four sequences of bits generated can be made inaccessible by discarding them, the correlation between the sequences will then be lost and all the other three sequences will be independent of one another. From the three remaining sequences, public verification of randomness on one sequence ensures the randomness of the other two sequences in real time without being probed for any direct verification, thus securing the two sequences of random bits. The two sequences can be used as two independent publicly verified secured private random bits or the two can be combined and used as a single sequence of random bits. We can note that by subjecting n bits for public verification we can obtain $2n$ bit of verified random number.

Verification of entanglement. We should also note that the relation between the measurement outcome given in Eq. (5) is a resource for verification of entanglement in the four-qubit state used for QRNG, Eq. (2). For that we need to access all the four bits generated from the measurement outcome. However, instead of accessing all the bits generated, one can sample out some small fraction of measurement outputs validation of Eq. (5) can be verified to confirm the entanglement in the four-qubit state used for QRNG. Once the entanglement is verified, the sample output can be discarded and the remaining output can be used for PVQRNG. Following both procedures will ensure entanglement verification and public verification of the randomness in the bits generated without compromising the security of the bits.

There is also a possibility of defining a four-qubit entangled state which will enable us to perform real-time entanglement verification and randomness verification by accessing only two of the four random bit sequences. For that one has to generate a state with a direct correlation between the first two qubits. That state can be generated by removing the last two XOR and X-gates from Fig. 1 resulting in the circuit as shown in Fig. 9 in Appendix B. The output state will be in the following form,

$$|\Phi\rangle_{ABCD} = \frac{1}{2\sqrt{2}}(|1000\rangle + |0100\rangle - |1010\rangle + |0110\rangle + |1001\rangle - |0101\rangle - |1011\rangle - |0111\rangle) \quad (6)$$

and this can be rewritten as

$$|\Phi\rangle_{ABCD} = \frac{1}{2\sqrt{2}}[(|01\rangle + |10\rangle)_{AB} \otimes (|00\rangle - |11\rangle)_{CD} - (|10\rangle - |01\rangle)_{AB} \otimes (|10\rangle - |01\rangle)_{CD}]. \quad (7)$$

The outcomes from the measurement of the first two qubits will always satisfy

$$x_A \oplus x_B = 1 \quad (8)$$

and the condition given by Eq. (5) will not hold. Thus, the real-time entanglement and randomness verification involves generating four sequences of bits from n copies of the four-qubit entangled state $|\Phi_{ABCD}\rangle$. Each copy is measured in the computational basis, producing strings X_A, X_B, X_C , and X_D . The user sends X_A and X_B to a verifier, who performs an XOR continuity test, $X_A(i) \oplus X_B(i) = 1$, and keeps the other two, $X_C(i)$ and $X_D(i)$, hidden and secured. Once the XOR continuity test is verified, one set of the sequence is further sent for randomness verification. Randomness in one ensures randomness in the last two strings because of the mutual independence of the last two random variables.

B. Public and private key generation

Public and private key pairs are essential cryptographic tools for data encryption and decryption. While the public key can be freely distributed without concern, the private key must always be kept secure and never shared unprotected. Here, let us consider two spatially separated parties, Alice and Bob, who share the four-qubit entangled state, Eq. (1), between them. We present a method for Alice (Bob) to share an encrypted message with Bob (Alice), which can only be read by Bob (Alice) once Alice (Bob) shares her (his) public key. Let us say, Alice and Bob simultaneously generate the bits x_A, x_C (for Alice) and x_B, x_D (for Bob). Alice can access only x_A and x_C , while Bob can access only x_B and x_D . Alice needs to send a message $m \in \{0, 1\}$ to Bob. To encode this message, she performs an XOR operation between the message and her bit x_A resulting in $m \oplus x_A$. She then sends $m \oplus x_A$ along with x_C to Bob. Any third party intercepting $m \oplus x_A$ and x_C cannot deduce the original message m since they lack the necessary information about x_A . Bob, on the other hand, can determine x_A upon receiving x_C since Bob knows x_B and x_D . He can solve for x_A from the relation $x_A \oplus x_B \oplus x_C \oplus x_D = 0$. With x_A known, Bob can then decode the message m by computing $m = (m \oplus x_A) \oplus x_A$.

In this protocol, the receiver must keep both of his bits private, while the sender must keep one of her bits private and make the other one public to enable the receiver to read the message. Here, m is the message to be communicated, $m \oplus x_A$ is the encrypted message protected by Alice's private key x_A . Only Bob can decrypt the message once Alice shares her public key x_C using his private keys x_B and x_D . Generating a key from entanglement is a well-established concept [29,30]. However, in past scenarios, the key had to undergo various tests to confirm its randomness after being obtained. In our protocol, we can perform these randomness verification tests on one-bit strings while using other bit strings as keys. This method enables real-time verification and generation, ensuring that the keys we generate are never exposed to randomness testing.

C. QBER analysis

The generated state ρ'_{ABCD} may not match the expected state $\rho_{ABCD} = |\Psi\rangle_{ABCD}\langle\Psi|_{ABCD}$ from our experimental setup.

It is possible that

$$F(\rho'_{ABCD}, \rho_{ABCD}) < 1 - \epsilon, \quad (9)$$

where F is the fidelity and $\epsilon > 0$. The state $|\Psi\rangle_{ABCD}$ in Eq. (2) can also be written as

$$|\Psi\rangle_{ABCD} = \frac{1}{2\sqrt{2}}(|0\rangle \otimes |\Theta_3^{\pi 00}\rangle + |1\rangle \otimes |\Theta_3^{\pi \pi \pi}\rangle), \quad (10)$$

where $|\Theta_3^{\pi 00}\rangle = \frac{1}{2}(|000\rangle + e^{i0}|110\rangle + e^{i0}|101\rangle + e^{i\pi}|011\rangle)$ and $|\Theta_3^{\pi \pi \pi}\rangle = \frac{1}{2}(|100\rangle + e^{i\pi}|001\rangle + e^{i\pi}|010\rangle + e^{i\pi}|111\rangle)$. Decrease in fidelity results in a deviation from the ideal state. Suppose we perform projective measurement on subsystem A , keeping everything untouched. The projective operators can be defined as $K_A^x = |x\rangle\langle x| \otimes I_{BCD}$ for $x \in \{0, 1\}$. The state postmeasurement for system BCD is given by

$$\rho_{BCD}^x = \frac{\text{tr}_A(K_A^x \rho_{ABCD} K_A^{x\dagger})}{\text{tr}(K_A^{x\dagger} K_A^x \rho_{ABCD})}. \quad (11)$$

The privacy of the state ρ_{BCD}^0 can be analyzed as follows.

The state ρ_{BCD}^0 can be written as

$$\rho_{BCD}^0 = (1 - p)|\Theta_3^{\pi 00}\rangle\langle\Theta_3^{\pi 00}| + \frac{p}{8}I_{BCD}, \quad (12)$$

where p is the probability of getting a maximally mixed state in place of a maximally entangled state. On measuring the system B , C , and D in the computational basis, then there is a probability $p/2$ with which the outcome does not match the outcome from $|\Theta_3^{\pi 00}\rangle$. Thus, quantum bit error rate (QBER) = $p/2$ for this case. The privacy of other states like ρ_{CD}^0 can also be calculated in a similar way.

The state ρ_{CD}^{00} can be written as

$$\rho_{CD}^{00} = (1 - p)|\Theta_2^{0\pi}\rangle\langle\Theta_2^{0\pi}| + \frac{p}{4}I_{CD}, \quad (13)$$

where $|\Theta_2^{0\pi}\rangle$ is the Bell state $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. On measuring the systems C and D on the computational basis QBER comes out as $p/2$ for this case as well. It can be readily checked that the QBER remains the same for all other cases ($|\Phi\rangle_{ABCD}$) as well.

III. EXPERIMENTAL REALIZATION ON A FOUR-QUBIT PHOTONIC SYSTEM

Multiple-qubit quantum state preparation and computation based on these internal degrees of freedom of photons have already been demonstrated [31–33]. A comparable schematic representation of the experimental setup generating a four-qubit state given in Eq. (2) using photons entangled in polarization and path degree of freedom is illustrated in Fig. 2. The experimental realization of the circuit diagram given in Fig. 1 is shown in Fig. 3.

To generate a four-qubit state, entangled photon pairs in polarization degree of freedom are used as source. Entangled photons are generated through the type-II SPDC process using a periodically poled KTP crystal. The schematic of the source is illustrated in Fig. 3. A 10 mm long PPKTP crystal was pumped by a continuous-wave diode laser (Surelock, Coherent), having a center wavelength of 405 nm. The astigmatism of the laser output pump beam is corrected by coupling with a single-mode optical fiber (SMF). The collimated circular

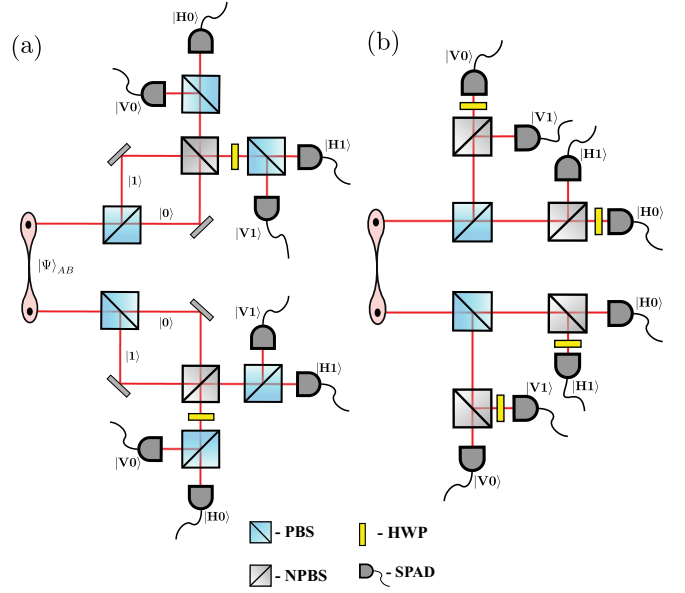


FIG. 2. The optical scheme for four-qubit state preparation equivalent to quantum circuit given in Fig. 1 using photon pairs entangled in polarization and path degree of freedom. (a) The scheme involves single-photon interference. (b) The schematic achieves the same quantum state without interference.

pump beam is allowed to pass through a polarizing beam splitter (PBS1) to set the pump polarization to horizontal. A plano-convex lens ($L1$, $f = 17.5$ cm) is used for focusing the beam at the center of the PPKTP crystal. The crystal temperature is maintained at 32.3°C for the two down converted photons to have a degenerate wavelength of 810 nm. We have selected the SPDC cone angle of approximately 0.83° relative to the pump beam to ensure a comparable counting rate in each spatial mode and to gather roughly twice the number of photon pairs compared to the collinear configuration. The down-converted photons from PPKTP are collimated using a plano-convex lens ($L2$, $f = 10$ cm). A prism mirror has been placed for the ease of collecting the signal and idler photons in two separate arms. A half-wave plate (HWP) at 45° (between the lens and prism mirror), followed by 5 mm long KTP crystals is placed as timing compensators in both arms. Bandpass interference filters (IF) of the center wavelength of 810 nm (± 10 nm) are used to filter out the residual pump beam and to only allow the down-converted photons. To maintain the polarization, the photons are coupled through the fiber polarization controllers (FPCs) [28,34–36]. We have generated a bright source of polarization-entangled photons at a rate of ~ 16400 pairs/s/mW. The density matrix of the generated entangled state is determined through quantum state tomography (QST), and the resulting real and imaginary parts are illustrated in the inset of Fig. 3. The generated state exhibits a fidelity of 98.12% with the Bell state given by

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B). \quad (14)$$

The fitted visibility curves along with the raw data points are also shown in the inset of Fig. 3. Data were taken at a lower pump power of 0.15 mW so that the accidental counts were minimal (16 counts/s). We have obtained visibility of

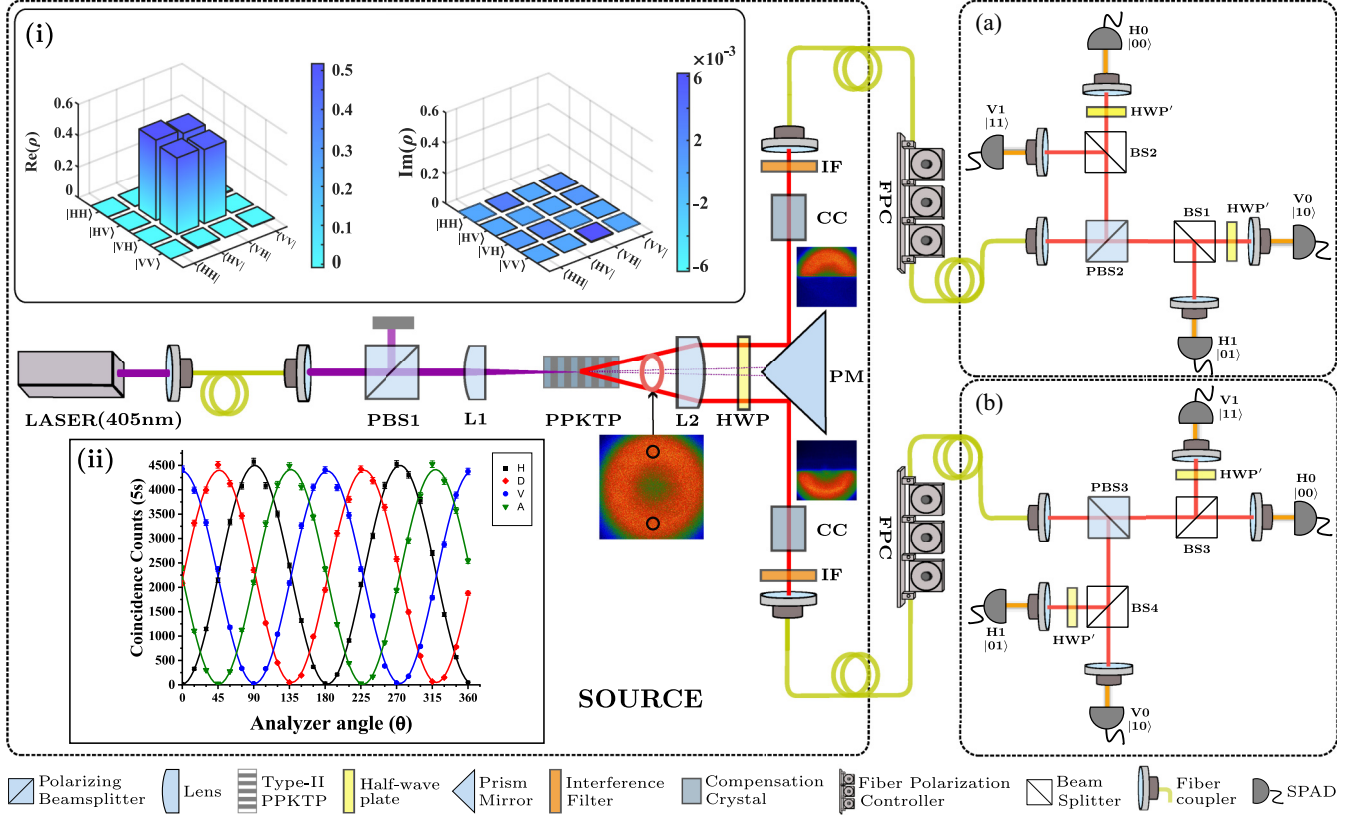


FIG. 3. Experimental setup: The source part represents the generation of polarized entangled photons through SPDC in a type-II PPKTP crystal; the generated entangled photons are separated via a prism mirror (PM) and coupled with a fiber. (i) Shows the real and imaginary parts of the reconstructed density matrix of the entangled photons with fidelity 98.12%, and (ii) visibility plot in H/V (98.6%) and A/D (98.1%) basis. Fiber polarization controllers (FPC) are used to guarantee that the polarization will remain after going through the fiber. (a) The measurement setup at Alice's side for generating random number sequence X_A and X_C . (b) The measurement setup at Bob's side for generating random number sequence X_B and X_D .

98.6% and 98.1% in the H/V and A/D basis, respectively, and achieved a maximum B-CHSH value(S) violation of $2.77(\pm 0.001)$.

Both the entangled photons are directed to the QRNG units (a) and (b) as illustrated in the schematic of the experimental setup. Both the photons entering the QRNG unit have an equal likelihood of being in either the horizontal ($|H\rangle$) or vertical ($|V\rangle$) state. Both the (a) and (b) units consist of a polarizing beam splitter (PBS2, PBS3), followed by 50:50 nonpolarizing beam splitters (BS) in both output paths as illustrated in Fig. 3. The PBS separates the polarization information while preserving the entanglement and creating two additional path degrees of freedom, and the resultant state would be

$$\begin{aligned} |\Psi\rangle_{ABCD}^I &= (\text{PBS}_{AC} \otimes \text{PBS}_{BD})(|\Psi\rangle_{AB} \otimes |0\rangle_C \otimes |0\rangle_D) \\ &\equiv (\text{CNOT}_{AC} \otimes \text{CNOT}_{BD})(|\Psi\rangle_{AB} \otimes |0\rangle_C \otimes |0\rangle_D) \\ &= \frac{|H0\rangle_{AC}|V1\rangle_{BD} + |V1\rangle_{AC}|H0\rangle_{BD}}{\sqrt{2}}. \end{aligned} \quad (15)$$

Here suffixes A and B represent the polarization information, and C and D represent the path information of the first and second photon, respectively. Both the outputs from the PBS of the signal photon are guided through nonpolarizing beam splitters (BS). When a single photon enters a 50:50 beam splitter, it has an equal probability of being transmitted

or reflected. The BS functions similarly to a Hadamard gate, acting on path degrees of freedom to generate the following state:

$$\begin{aligned} |\Psi\rangle_{ABCD}^{II} &= (\text{BS}_C \otimes \text{BS}_D)|\Psi\rangle_{ABCD}^I \equiv (H_C \otimes H_D)|\Psi\rangle_{ABCD}^I \\ &= \frac{1}{\sqrt{2}} \left(|H\rangle_A \frac{|0\rangle_C + |1\rangle_C}{\sqrt{2}} \right) \left(|V\rangle_B \frac{|0\rangle_D - |1\rangle_D}{\sqrt{2}} \right) \\ &\quad + \frac{1}{\sqrt{2}} \left(|V\rangle_A \frac{|0\rangle_C - |1\rangle_C}{\sqrt{2}} \right) \left(|H\rangle_B \frac{|0\rangle_D + |1\rangle_D}{\sqrt{2}} \right). \end{aligned} \quad (16)$$

Now let us introduce half-wave plates at 45° in the transmitted path ($|0\rangle_C$) of the beam splitters in unit (a) and the reflected path ($|1\rangle_D$) of the beam splitters in unit (b) as shown in Fig. 3 to get the final state:

$$\begin{aligned} |\Psi\rangle_{ABCD} &= \frac{1}{\sqrt{2}} \left(\frac{|V\rangle_A|0\rangle_C + |H\rangle_A|1\rangle_C}{\sqrt{2}} \right) \left(\frac{|V\rangle_B|0\rangle_D - |H\rangle_B|1\rangle_D}{\sqrt{2}} \right) \\ &\quad + \frac{1}{\sqrt{2}} \left(\frac{|H\rangle_A|0\rangle_C - |V\rangle_A|1\rangle_C}{\sqrt{2}} \right) \left(\frac{|H\rangle_B|0\rangle_D + |V\rangle_B|1\rangle_D}{\sqrt{2}} \right) \\ &= \frac{|\Phi^+\rangle_{AB}|\Phi^-\rangle_{CD} + |\Phi^-\rangle_{AB}|\Phi^+\rangle_{CD}}{\sqrt{2}}, \end{aligned} \quad (17)$$

where $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$ are the four Bell states. This state can also be written as

$$\begin{aligned} |\Psi\rangle_{ABCD} &= |0\rangle_A \left(\frac{|000\rangle + |101\rangle + |110\rangle - |011\rangle}{2\sqrt{2}} \right)_{BCD} \\ &\quad + |1\rangle_A \left(\frac{|100\rangle - |001\rangle - |010\rangle - |111\rangle}{2\sqrt{2}} \right)_{BCD} \\ &\equiv \frac{1}{2\sqrt{2}} (|0000\rangle + |0101\rangle + |0110\rangle - |0011\rangle \\ &\quad + |1100\rangle - |1001\rangle - |1010\rangle - |1111\rangle)_{ABCD}, \end{aligned} \quad (18)$$

which is identical to the state given in Eq. (2). The outputs from the four BS are coupled to multimode optical fibers (MMF), which are connected to eight single-photon counting modules (SPCMs). These are connected to a time tagger to record the arrival times of the photons.

Ideally, after the entangled photon passes through a PBS on both units (a) and (b), it becomes entangled in the path as well, generating a four-qubit polarization-path entangled state. Applying a Hadamard gate to the path qubit involves interference between the path states. However, we know that interference occurs for photons only if both paths have the same polarization. After passing through the PBS, the polarizations are separated. Therefore, we do not necessarily need a single BS for the paths. Instead, we can use two separate BSs for the two paths and label them accordingly. But in our scheme, on the Alice and Bob sides, at any given time, only horizontal polarization (H-pol) and vertical polarization (V-pol) exist. Consequently, the result is unaffected by single-photon interferometer presence or absence. In the end, full polarization and path information can only be obtained with a polarizing beam splitter (PBS), which creates four different paths. To create these four outputs, we employed two beam splitters (BS) in two different paths. We then performed two polarization-dependent actions on these particular labeled pathways. As a result of this labeling, two of the paths are designated as $|0\rangle$ and the remaining two as $|1\rangle$. Finally, we apply the controlled-NOT (CNOT) operation based on our convention. In Fig. 2(a), we show the exact optical setup for that state preparation. In Fig. 2(b), we show the setup used for our experimental purposes. Both setups lead to the same state preparation.

The state exists in an equal superposition of eight possible output states and satisfies the conditions required for being an entanglement-certified QRNG. Each output from the four beam splitters corresponds to one of these eight states, and their specific outcomes remain entirely uncertain until measurement. Employing a measurement at this stage allows for the generation of four-bit quantum random numbers. Whenever there is a coincidence between one of the detectors from unit (a) and from (b), we record it as a four-bit number. The first and third bits correspond to detection in unit (a) and the second and fourth correspond to detection in unit (b).

To generate the state given by Eq. (6), we can remove the last four half-wave plates in the experimental setup given in Fig. 3. Thus, in the given experimental setup we can gen-

erate both the four-qubit state described in the theoretical description to generate real-time publicly verifiable QRNG, for real-time entanglement verification, and to use it as a public and private key generation unit.

A. Quantum random number generation and public verification

If we only have access to the strings X_A , X_B , X_C , and X_D , then while Eq. (5) is a necessary condition, it is not sufficient by itself to prove the faithfulness of the device. In this setup, we generate a source of polarization-entangled photons, which we verify using quantum state tomography, visibility measurements, and CHSH-value measurements. These photons are then passed through beam splitters as described, resulting in the generation of a four-qubit entangled state, as given by Eq. (2). Given the polarization entanglement of the photons, the condition in Eq. (5), together with the randomness of the sequences, should ensure that the output state conforms to Eq. (2). We generated random numbers across a range of pump powers from 0.1 mW to 6 mW, achieving a collective bit rate of ~ 60 kbps/mW. At a pump power of 6 mW, we reached a bit rate of ~ 370 kbps, which can be further increased by boosting the pump power. All the strings were subjected to randomness testing. The sequences are correlated in such a way that they have the same entropy but remain mutually independent [25]. We verified that a successful randomness test on one sequence ensures the randomness of the other sequences, as expected. This randomness test can be conducted by an external party without compromising the secrecy of the other random strings. All the strings X_A , X_B , X_C , and X_D of the generated random numbers passed all 15 NIST tests without any need for postprocessing. Each bit x_i is generated at a rate of ~ 15 kbps/mW. Among the four-bit strings, one (e.g., X_A) can be used for public randomness testing, while another (e.g., X_D) can be discarded for security purposes. The remaining two strings (X_B and X_C) can either be used separately or merged to achieve a higher bit rate of 30 kbps/mW for verified and secure random numbers.

The results of the 15 NIST tests for the data taken at 6 mW are shown in Fig. 4. The dashed line ($p = 0.01$) indicates the critical p value above which the sequence is considered random. Results indicate that the statistical patterns are not found in the tested samples of the random bits.

B. Private and public key generation

Using the setup shown in Fig. 3, we can achieve a secure communication between two parties as described in Sec. II. For this setup, part (a) is assigned to Alice, and part (b) is assigned to Bob. Alice and Bob can locally and simultaneously generate their respective keys from the coincidence measurement between them and generate keys x_A and x_C for Alice, and x_B and x_D for Bob. To obtain the coincidence measurement and generate keys Alice and Bob have to classically exchange the timing information of photon detection and postselect coinciding events. An eavesdropper cannot find any keys from this timing information since they are not giving out any keys generated corresponding to each detection. The sender can keep one as a private key and announce the other as a public

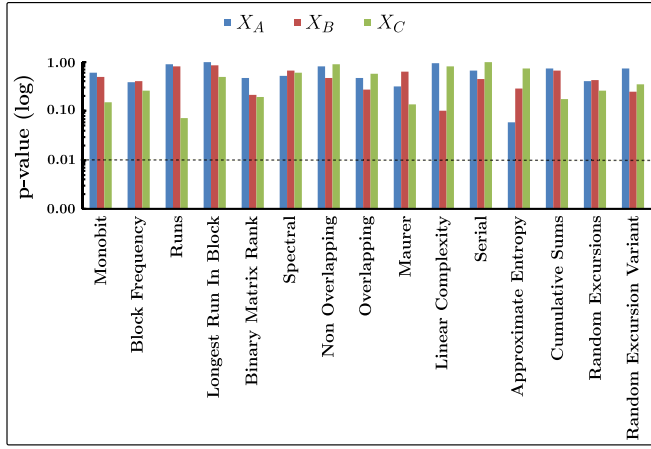


FIG. 4. NIST randomness test results for the streams of data X_A , X_B , and X_C . We can note that the data obtained from measurement outcome passes all the NIST tests with a value above 0.01 without the need for any postprocessing.

key. Using the information of the public key, the receiver can recover the fourth key described in Sec. II B.

In Fig. 5, we demonstrate the encryption and decryption of two images using the keys generated from the data we collected. The images used are of bit length 42 818 and 306 916, respectively. For the successful encryption and decryption of these images, the number of four-bit strings (X_A , X_B , X_C , X_D) should be of the same length as that of the image. So, we have generated keys from the four-qubit entangled state of the same length. This corresponds to a total key length of 171 272 for image (a) and 1 227 664 for image (b) given in Fig. 5. The string X_A (Alice's private key) is used for encrypting the image. For image decryption, the strings X_B , X_C (Bob's private keys), X_C (Alice's public key), and the relation (5) are used. Original, encrypted, and decrypted images are shown in Fig. 5.

C. Verification of entanglement

To verify the polarization entanglement between the two photons from the outputs of the device, the photons

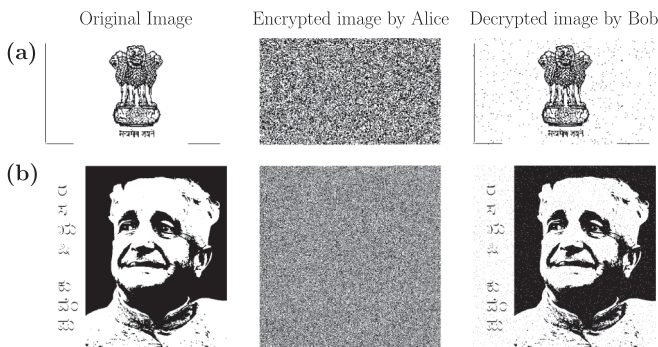


FIG. 5. Encryption and decryption of image using the private and public key generated from the four-qubit entangled state. (a) Image bit length is 42 818 and total key length is 171 272. (b) Image bit length is 306 916 and total key length is 1 227 664.

from Alice's and Bob's outputs, which exhibit orthogonal polarization, can be separately subjected to visibility or S-value measurements. We ensure that the two photons are polarization-entangled before generating the four-qubit entangled state, and the detailed process is discussed above. Given the polarization entanglement between the two photons, Eq. (5) along with the successful randomness tests will guarantee the generation of the four-qubit entangled state given in Eq. (2). We used 10% of the recorded strings, consisting of 3 330 856 bits, to verify if the outputs satisfy the condition in Eq. (5). Of the sample data, 97.9% met the condition. The sample used for verification can be discarded, allowing the remaining data to be used.

D. Influence of entanglement variation and depolarizing noise on four-qubit QRNG system

Variation in the probability amplitudes of the basis state of the four-qubit system will result in the variation of entanglement and alter the quality and rate of the verified random number generation. To study the effect of entanglement variation and depolarizing noise on the bitrate of the four-qubit system, we will introduce entanglement control parameters and noise effect only on the first two qubits. The effect on the first two qubits will reflect on the full four-qubit system. This can be experimentally realized by using the two-photon polarization entangled state

$$|\psi\rangle_{\alpha\beta} = (\alpha|HV\rangle + \beta|VH\rangle), \quad (19)$$

where $|\alpha|^2 + |\beta|^2 = 1$ as the initial state. The effective four-qubit state will be

$$\begin{aligned} |\Psi\rangle_{ABCD} = & \frac{\alpha}{2} (|VV00\rangle + |HV10\rangle - |VH01\rangle - |HH11\rangle) \\ & \times \frac{\beta}{2} (|HH00\rangle - |VH10\rangle + |HV01\rangle - |VV11\rangle). \end{aligned} \quad (20)$$

When Eq. (19) is the input state, the probabilities of the $|0\rangle$ and $|1\rangle$ outputs from PBS1 would be α^2 and β^2 , respectively. That is, the probabilities of the generation of the bits 00 and 01 would be $\frac{|\alpha|^2}{2}$ each and that of 10 and 11 would be $\frac{|\beta|^2}{2}$ each, leading to the generation of an unequal number of 0's and 1's in the generated random numbers, depending upon the value of α and β . As α decreases from $\frac{1}{\sqrt{2}}$ to 0, the state will become less entangled, the difference between the number of 0's and 1's in the generated data increases, and the sequence will become less random. To experimentally demonstrate this effect, we postselect the photons just before detection by using a polarizer in the transmitted arm of PBS3, varying the number of horizontal photons detected. This manipulation affects the coincidence counts and thus the random numbers generated, mirroring the effects as if the input state is of the form described by Eq. (19), depending on the polarizer angles. Here, $\alpha^2 = \frac{\cos^2 \theta}{2}$, where θ is the polarizer angle. As θ increases from 0 to 90 (equivalent to α decreasing from $\frac{1}{\sqrt{2}}$ to 0), the generation rate of the sequence and the number of NIST tests the bit string taken for verification passes decrease, as illustrated in Fig. 6.

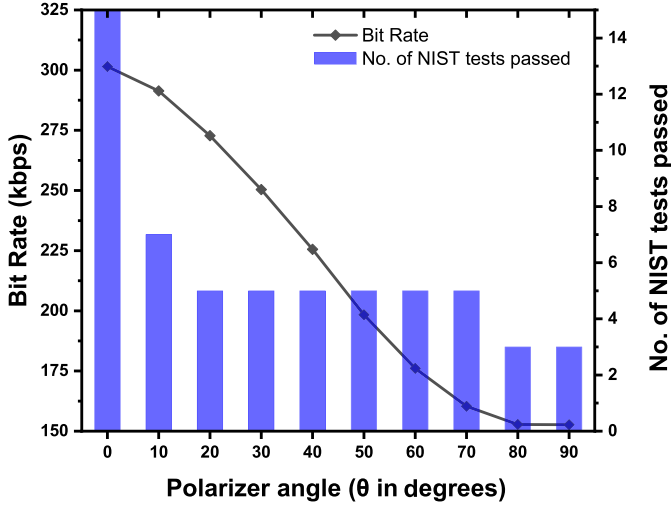


FIG. 6. Effect of varying degree of entanglement on the bit rate and the randomness of the bit string used for randomness verification using NISTtest (at pump power = 6 mW). We can note that with a decrease in entanglement, the number of bits generated decreases and the number of NIST tests it passes also significantly goes down.

We also reduced the entanglement quality by decreasing the visibilities, achieved through adjustments to the timing compensator. We measured Bell's Clauser-Horne-Shimony-Holt (CHSH) value (S value) for the corresponding state and observed its impact on random number generation. The data are depicted in Fig. 7(a).

We can analyze the quantum state using a noisy treatment to theoretically model our experimental data. The noisy state is given by

$$\rho_{\text{Noisy}} = (1 - p)|\Psi_{AB}\rangle\langle\Psi_{AB}| + \frac{p}{4}\mathbb{I}_4, \quad (21)$$

where $p = 0$ corresponds to the pure quantum state, and $p = 1$ represents a completely mixed state. To define the visibility, we use the following projection operator:

$$|\theta_1\rangle \otimes |\theta_2\rangle = (\cos\theta_1|H\rangle_A + \sin\theta_1|V\rangle_A) \otimes (\cos\theta_2|H\rangle_B + \sin\theta_2|V\rangle_B), \quad (22)$$

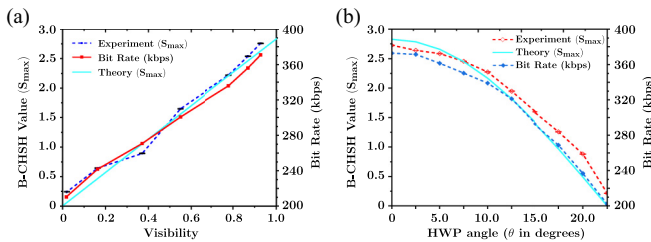


FIG. 7. Measured bit rate of the generated random numbers and CHSH parameter (S value) for the corresponding state for different entanglement visibilities (pump power = 6 mW). With the decrease in entanglement visibility, we can see a corresponding decrease in S value and secured bit rate generated. The experimental output is in complete agreement with the theoretically expected value.

where θ_1 can be fixed to define the basis. For SPDC entangled photons, the A/D ($\theta_1 = \pi/4$ or $3\pi/4$) basis visibility is crucial for certifying the quality of entanglement. By varying θ_2 and calculating $\text{Tr}(\rho_{\text{Noisy}}M)$, where

$$M = |\theta_1\rangle \otimes |\theta_2\rangle \langle\theta_1| \otimes \langle\theta_2|, \quad (23)$$

we obtain a series of values for each θ_2 .

From these values, visibility can be calculated using the formula

$$V = \frac{v_{\text{max}} - v_{\text{min}}}{v_{\text{max}} + v_{\text{min}}}, \quad (24)$$

where v_{max} and v_{min} are the maximum and minimum values obtained, respectively. This procedure is repeated for all p values. Finally, we will plot visibility versus S value according to our experimental results.

Implementing depolarizing noise in experiments poses significant challenges. Therefore, we present a mathematical model of depolarizing noise and demonstrate its impact on the generated random numbers. If we keep a half-wave plate at an angle θ before PBS3 in the unit (b), state Eq. (14) becomes

$$|\Psi\rangle_\theta = \frac{1}{\sqrt{2}} \{ [\cos(2\theta)|H\rangle + \sin 2\theta|V\rangle] |V\rangle + [\sin(2\theta)|H\rangle - \cos 2\theta|V\rangle] |H\rangle \}$$

which can also be written as

$$\begin{aligned} |\Psi\rangle_\theta &= \frac{1}{\sqrt{2}} \cos 2\theta \{ |HV\rangle - |VH\rangle \} \\ &+ \frac{1}{\sqrt{2}} \sin 2\theta \{ |HH\rangle + |VV\rangle \} \\ &= \cos 2\theta |\Psi^-\rangle + \sin 2\theta |\Phi^+\rangle, \end{aligned} \quad (25)$$

where $|\Psi^+\rangle$ and $|\Phi^+\rangle$ are the Bell states. $|\Psi\rangle_\theta$ is not maximally entangled in the H/V basis for $\cos 2\theta, \sin 2\theta \neq 0$. As θ increases from 0 to $\frac{\pi}{8}$, uncertainty in the polarization of the reference photon increases, and at $\frac{\pi}{8}$, it is maximum.

The measured Bell's CHSH value (for a measurement choice, which gives maximal violation for a maximally entangled state on the H/V basis) is depicted against the half-wave-plate angles $\theta \in [0, \frac{\pi}{8}]$ in Fig. 7(b), along with the corresponding reduction in bit rate.

Ideally, measurements of the state $|\Psi\rangle_{ABCD}$ yield uniformly distributed bits x_A, x_B, x_C , and x_D , satisfying Eq. (5) with maximal Shannon entropy of 1 for each bit. Sampling out a small fraction of measurement output can be used to calculate QBER. For n copies of the entangled state $|\Psi\rangle_{ABCD}$ measured in the computational basis, producing strings X_A, X_B, X_C , and X_D . Assign $L = \{i : \text{st } X_A(i) \oplus X_B(i) \oplus X_C(i) \oplus X_D(i) \neq 0\}$, the quantum bit error rate (QBER) is calculated as $\delta = \frac{|L|}{n}$. Similar analysis for $|\Phi\rangle_{ABCD}$ can be done where $L = \{i : \text{st } X_A(i) \oplus X_B(i) \neq 1\}$. Imperfections due to nonideal entanglement or measurements can be mitigated using entanglement purification [37] and error correction [38] techniques.

IV. CONCLUSION

In this study, we have demonstrated the practical use of a configurable four-qubit photonic system for quantum-safe

applications. Utilizing photon pairs entangled in polarization and path degrees of freedom, our four-qubit system achieves several significant outcomes. We have reported the generation of publicly verified and secure random bits at a rate of 165 kbps by performing measurements on the four-qubit system and accessing partial information for public verification. The entangled source photon pairs used for the generation of four-qubit state and randomness generation gives a Bell's CHSH value of 2.77, and the system maintains a high entanglement verification success rate of 97.9% for the sampled bits from the four-qubit states. This ensures the secrecy of undisclosed bits and the trustworthiness of the four-qubit system to the beneficiary. The system simultaneously generates equal numbers of public and private keys, indicating its efficiency in producing secure cryptographic keys essential for quantum communication protocols. This dual-key generation capability enhances the applicability of the system for secure communication infrastructures. This has been demonstrated by encrypting and decrypting images.

The theoretical model of noise on the four-qubit state and its effect on the generation rate of verified and secure bits aligns with the experimental results. This alignment validates our approach and demonstrates the practical viability of our small-scale multiqubit photonic system for quantum-safe applications. We also provide a way to verify the security features of the quantum system in real time, making it easier to integrate into secure communication networks and other applications needing strong quantum security.

ACKNOWLEDGMENTS

We would like to thank Dr. K. Muhammed Shafi for his input on the design of experimental setup and M. Joshi for his contribution to build the entangled photon source. We acknowledge the support from the Office of Principal Scientific Advisor to the Government of India, Project No. Prn.SA/QSim/2020.

APPENDIX A

The four-qubit entangled state for PVQRNG can be prepared using the sequence of unitary operations on the initial state $|\Psi\rangle_0 = |0000\rangle = |q\rangle_A |q\rangle_B |q\rangle_C |q\rangle_D$. In Fig. 8 we have show the operations in in circuit form.

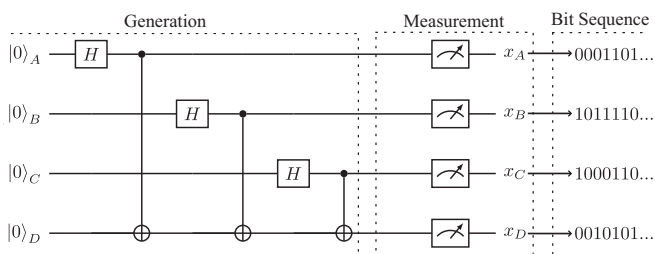


FIG. 8. Circuit diagram for generation of alternate four qubit entangled state given in Eq. (A1) for generation of random bit sequence.

The resulting state after applying the gates as shown in Fig. 8 is

$$\begin{aligned} |\Psi\rangle_{ABCD} &= \text{CNOT}_{CD} \cdot H_C \cdot \text{CNOT}_{BD} \cdot H_B \\ &\quad \cdot \text{CNOT}_{AD} \cdot H_A |0000\rangle \\ &= \frac{1}{2\sqrt{2}}(|0000\rangle + |0011\rangle + |0101\rangle + |0110\rangle \\ &\quad + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle). \end{aligned} \quad (\text{A1})$$

The above state can be rewritten as

$$\begin{aligned} |\Psi\rangle_{ABCD} &= \frac{1}{2\sqrt{2}}(|0\rangle \otimes (|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\ &\quad + |1\rangle \otimes (|001\rangle + |010\rangle + |100\rangle + |111\rangle)). \end{aligned} \quad (\text{A2})$$

A single copy of the state $|\Psi\rangle_{ABCD}$ is used to make projective measurements in the computational basis of each subsystem. The random variable for each subsystem is a bit i.e. either 0 or 1 and can be denoted as x_A , x_B , x_C , and x_D , as mentioned in the Table I below.

APPENDIX B

The real time entanglement verification state satisfying Eq. (6) and given by Eq. (8) is generated from the circuit, as shown in Fig. 9.

$$\begin{aligned} |\Phi\rangle_{ABCD} &= H_C \cdot H_D \cdot \text{CNOT}_{BD} \cdot \text{CNOT}_{AC} |\Psi^+\rangle |00\rangle \\ &= \frac{1}{2\sqrt{2}}(|1000\rangle + |0100\rangle - |1010\rangle + |0110\rangle \\ &\quad + |1001\rangle - |0101\rangle - |1011\rangle - |0111\rangle) \end{aligned} \quad (\text{B1})$$

with $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)_{AB}$.

Similarly, a single copy of the state $|\Phi\rangle_{ABCD}$ is used to make projective measurements in the computational basis of each subsystem. The random variable for each subsystem is a bit i.e. either 0 or 1 and can be denoted as x_A , x_B , x_C , and x_D , as mentioned in the Table II below.

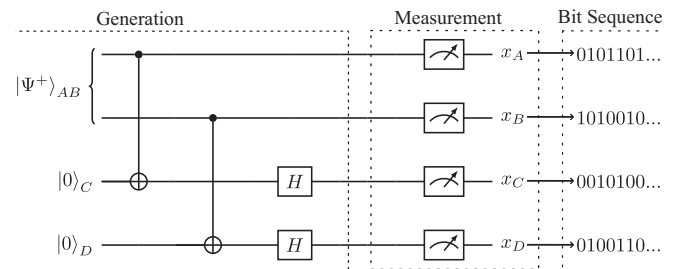


FIG. 9. Circuit diagram for real-time entanglement verification for the state $|\Phi\rangle_{ABCD}$.

TABLE I. Projection probabilities in the computational basis of subsystems for the output entangled state $|\Psi\rangle_{ABCD}$ given by Eq. (A1). Outcomes with probability zero are not mentioned.

$p(x_A, x_B, x_C, x_D)$	x_A	x_B	x_C	x_D
1/8	0	0	0	0
1/8	0	0	1	1
1/8	0	1	0	1
1/8	0	1	1	0
1/8	1	0	0	1
1/8	1	0	1	0
1/8	1	1	0	0
1/8	1	1	1	1

TABLE II. Projection probabilities in the computational basis of subsystems for the output state $|\Phi\rangle_{ABCD}$ given by Eq. (B1).

$p(x_A, x_B, x_C, x_D)$	x_A	x_B	x_C	x_D
1/8	0	1	0	0
1/8	0	1	0	1
1/8	0	1	1	0
1/8	0	1	1	1
1/8	1	0	0	0
1/8	1	0	0	1
1/8	1	0	1	0
1/8	1	0	1	1

- [1] W. Schindler, Random number generators for cryptographic applications, *Cryptographic Engineering* (Springer, Boston, 2009).
- [2] R. Gennaro, Randomness in cryptography, *IEEE Security Privacy* **4**, 64 (2006).
- [3] H. Bauke and S. Mertens, Random numbers for large-scale distributed Monte Carlo simulations, *Phys. Rev. E* **75**, 066701 (2007).
- [4] M. Du, Q. Chen, L. Liu, and X. Ma, A blockchain-based random number generation algorithm and the application in blockchain games, in *IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy* (IEEE, Piscataway, NJ, 2019), pp. 3498–3503.
- [5] F. James, A review of pseudorandom number generators, *Comput. Phys. Commun.* **60**, 329 (1990).
- [6] W. Hörmann, J. Leydold, and G. Derflinger, *Automatic Nonuniform Random Variate Generation* (Springer, Berlin, 2004).
- [7] T. E. Hull and A. R. Dobell, Random number generators, *SIAM Rev.* **4**, 230 (1962).
- [8] U. M. Maurer, A universal statistical test for random bit generators, *J. Cryptology* **5**, 89 (1992).
- [9] A. N. Kolmogorov, On tables of random numbers, *Theor. Comput. Sci.* **207**, 387 (1998).
- [10] A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, Jr., and S. C. Vo, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication (NIST SP), Report No. 800-22 (National Institute of Standards and Technology, Gaithersburg, MD, 2001).
- [11] H. Schmidt, Quantum mechanical random number generator, *J. Appl. Phys.* **41**, 462 (1970).
- [12] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, Randomness in quantum mechanics: Philosophy, physics and technology, *Rep. Prog. Phys.* **80**, 124001 (2017).
- [13] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
- [14] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, *npj Quantum Inf.* **2**, 16021 (2016).
- [15] M. M. Jacak, P. Józwiak, J. Niemczuk, and J. E. Jacak, Quantum generators of random numbers, *Sci. Rep.* **11**, 16108 (2021).
- [16] M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and W. Ling-An, A random number generator based on quantum entangled photon pairs, *Chin. Phys. Lett.* **21**, 1961 (2004).
- [17] D. Branning and M. Bermudez, Testing quantum randomness in single-photon polarization measurements with the NIST test suite, *J. Opt. Soc. Am. B* **27**, 1594 (2010).
- [18] K. M. Shafi, P. Chawla, A. S. Hegde, R. S. Gayatri, A. Padhye, and C. M. Chandrashekar, Multi-bit quantum random number generator from path-entangled single photons, *EPJ Quantum Technol.* **10**, 43 (2023).
- [19] O. Kwon, Y.-W. Cho, and Y.-H. Kim, Quantum random number generator using photon-number path entanglement, *Appl. Opt.* **48**, 1774 (2009).
- [20] 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).
- [21] 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).
- [22] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, *Nat. Commun.* **9**, 5365 (2018).
- [23] C. Foreman, S. Wright, A. Edgington, M. Berta, and F. J. Curchod, Practical randomness amplification and privatisation with implementations on quantum computers, *Quantum* **7**, 969 (2023).
- [24] V. Mannalatha, S. Mishra, and A. Pathak, A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness, *Quantum Inf. Proc.* **22**, 439 (2023).
- [25] P. Józwiak, J. E. Jacak, and W. A. Jacak, New concepts and construction of quantum random number generators, *Quantum Inf. Proc.* **23**, 132 (2024).
- [26] J. E. Jacak, W. A. Jacak, W. A. Donderowicz, and L. Jacak, Quantum random number generators with entanglement for public randomness testing, *Sci. Rep.* **10**, 164 (2020).
- [27] T. Islam, A. Banerji, C. J. Boon, W. Rui, A. Reezwana, J. A. Grieve, R. Piera, and A. Ling, A privacy-preserving publicly verifiable quantum random number generator, *Sci. Rep.* **14**, 11337 (2024).

- [28] S. M. Lee, H. Kim, M. Cha, and H. S. Moon, Polarization-entangled photon-pair source obtained via type-II non-collinear SPDC process with PPKTP crystal, *Opt. Express* **24**, 2941 (2016).
- [29] K. Shannon, E. Towe, O. K. Tonguz, On the use of quantum entanglement in secure communications: A survey, [arXiv:2003.07907](#).
- [30] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. Lond. A* **461**, 207 (2005).
- [31] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, X. Jiang *et al.*, 18-Qubit entanglement with six photons' three degrees of freedom, *Phys. Rev. Lett.* **120**, 260502 (2018).
- [32] R. C. Souza, W. F. Balthazar, and J. A. O. Huguenin, Universal quantum gates for path photonic qubit, *Quantum Inf. Proc.* **21**, 68 (2022).
- [33] K. Sengupta, K. M. Shafi, S. P. Dinesh, S. Asokan, and C. M. Chandrashekar, Experimental realization of universal quantum gates and six-qubit state using photonic quantum walk, [arXiv:2403.06665](#).
- [34] M. Fiorentino, C. E. Kuklewicz, and F. N. C. Wong, Source of polarization entanglement in a single periodically poled KTiOPO4 crystal with overlapping emission cones, *Optics Express* **13**, 127 (2005).
- [35] S. Guo and K. Shang, High-flux, high-visibility entangled photon source obtained with a non-collinear type-II PPKTP crystal pumped by a broadband continuous-wave diode laser, *Opt. Commun.* **545**, 129586 (2023).
- [36] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, Entangled photon-pair sources based on three-wave mixing in bulk crystals, *Rev. Sci. Instrum.* **92**, 041101 (2021).
- [37] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Experimental entanglement purification of arbitrary unknown states, *Nature (London)* **423**, 417 (2003).
- [38] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, *Phys. Rev. A* **54**, 3824 (1996).