Quantum randomness generation via orbital angular momentum modes crosstalk in a ring-core fiber

Mujtaba Zahidy[1], Hamid Tebyanian[2], Daniele Cozzolino[1], Yaoxin Liu[1],
Yunhong Ding[1], Toshio Morioka[1], Leif K. Oxenløwe[1], and Davide Bacco[1]*
[1] *Center for Silicon Photonics for Optical Communications (SPOC),*
Department of Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark
[2] *Department of Mathematics, University of York, Heslington, York, YO10 5DD, United Kingdom*

Genuine random numbers can be produced beyond a shadow of doubt through the intrinsic randomness provided by quantum mechanics theory. While many degrees of freedom have been investigated for randomness generation, not adequate attention has been paid to the orbital angular momentum of light. In this work, we present a quantum random number generator based on the intrinsic randomness inherited from the superposition of orbital angular momentum modes caused by the crosstalk inside a ring-core fiber. We studied two possible cases: a first one, device-dependent, where the system is trusted, and a second one, semi-device-independent, where the adversary can control the measurements. We experimentally realized the former, extracted randomness, and, after privacy amplification, we achieved a generation rate higher than 10 Mbit/s. In addition, we presented a possible realization of the semi-device-independent protocol, using a newly introduced integrated silicon photonic chip. Our work can be considered as a starting point for novel investigations of quantum random number generators based on the orbital angular momentum of light.

I. INTRODUCTION

Quantum Mechanics has provided us with unique resources, many of which were not accessible through classical means. Secure communication empowered by quantum key distribution [1–3], quantum computing [4], quantum conference key agreement [5], and quantum electronic voting [6] are examples of emerging technologies thanks to quantum mechanics. Randomness is the critical ingredient of every secure communication protocol; besides, it has a wide range of applications in science and technology, e.g., simulation and gambling [7]. A random number generator (RNG) should, in general, be secure and practical, otherwise stated easy-to-implement, affordable, and high-rate. Classical RNGs, also known as pseudo-RNGs (PRNG), are quite practical, however the security of the generated random numbers can be compromised, as the randomness generation is based on deterministic phenomena that are predictable [8]. Thus PRNG cannot meet the high-security needs of highly confidential applications [9]. Conversely, quantum mechanics can provide genuine and unpredictable randomness based on its intrinsic probabilistic nature, thus allowing for the realization of a quantum RNG. Quantum random number generators (QRNG)'s protocols are classified into three main categories: device-dependent (DD) [10–12], device-independent (DI) [13–15], and semi-DI [16–18]. In the first category, namely DD protocols, the user trusts the performance of the generator and its experimental apparatus. QRNGs based on these kind of protocols could be very practical and relatively secure compared to the classical PRNGs [19]. On the other hand, in the DI scenarios, randomness can be generated needless of trusting the devices' performances, which also implies the violation of a Bell-type inequality to validate the protocols. Even though DI QRNGs offer the highest level of security, they are very slow and complicated, making them less practical [9]. Semi-DI protocols are an intermediate approach where, depending on the user's demands, some assumptions can be set on the devices. It should be noted that almost all of the commercial QRNGs are based on DD scenarios as they offer a good level of security with an uncomplicated high-rate device [20–23]. Different QRNGs can be devised on different degrees of freedom either in a discrete variable (DV) or continuous variable (CV) context with each having its benefits and disadvantages [24].

In this paper, we investigate the photons' spatial degree of freedom as a possible source of randomness [25]. In particular, we propose a QRNG based on the intrinsic crosstalk between orbital angular momentum (OAM) modes in a ring-core fiber (RCF) [26, 27], see Figure 1. Such crosstalk is caused by input modes whose wavefront is inclined with respect to the fiber coupler. Indeed, in an RCF, a certain input field would excite several guided modes, depending on its incident angle and field distribution, which can be determined by the overlap of the input field and fiber modes. Similarly, when a quantum state is coupled into the RCF with an angle, a state in superposition of modes is generated. Measuring such states lead to a probabilistic outcome which is theoretically unpredictable.

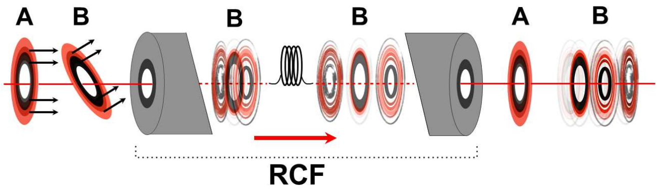

Figure 1. A superposition of OAM modes is generated by entering the RCF with a tilted input. Above, input mode 'A' will not experience distortion as its wavefront is aligned to the RCF, however, input mode 'B' is transformed to a superposition of different modes due to the coupling angle. Various modes are separated along the fiber due to their different group velocities.

[*] dabac@fotonik.dtu.dk

We leverage on this characteristic to present two QRNG implementations, following a DD and a semi-DI approach. The DD protocol is experimentally realized, and the extracted random numbers are tested for randomness. An experimental proposal for the studied semi-DI protocol is also given in the discussion. Our experiment enjoys simplicity and guarantees relatively high generation rate. In addition, it can be operated either as a no-input generator or as a randomness-expansion implementation.

II. PROTOCOL

A. Model

Crosstalk, which diligently is tried to be avoided in many applications [27, 28], can be considered as an intrinsic source of randomness. As simple as an ordinary beam-splitter, crosstalk happening within an RCF can be exploited to extract randomness as it transforms an OAM input state $|M\rangle$ into a superposition of various OAM modes denoted by $|N_j\rangle$,

$$|M\rangle = \sum_j \lambda_j |N_j\rangle, \tag{1}$$

where $|\lambda_j|^2$ is the probability of finding the output state in OAM mode $|N_j\rangle$. The superposition of OAM modes generated separates in time while propagating through the RCF due to a difference in group velocity for each mode. This mode-to-time mapping allow us to experimentally distinguish each OAM mode with a time of flight measurement from which, subsequently, is possible to extract randomness.

Crosstalk can be exploited to generate randomness both using a DD or semi-DI approach. In the former, which is experimentally realized in this study, a single OAM mode is prepared and coupled to the fiber, while in the latter scenario, an input state is selected from a set of possible modes, which amounts to an increase in randomness and privacy. In what follows, we explain each approach separately.

1. *Case I: Single Input QRNG*

The simplest QRNG that can be devised is by using a single input inducing a crosstalk such that multiple output modes are excited with probabilities close to $1/d$, with d being the number of modes excited in the RCF.

While this model has simplicity in the preparation stage, the protocol is fully trusted (DD scenario). Yet, we consider the devices' imperfections, e.g. optical devices loss, as the classical side-information known by the adversary. Denoting the set of output modes by $\{N_j\}$ with $|\{N_j\}| = d$, the probability of each outcome in its corresponding time-bin, b_j, reads

$$P(b_j) = P(N_j|M)\eta_{det}(1-\varepsilon)^{d-1}, \tag{2}$$

where η_{det} is the detector efficiency and ε is the probability of detection error in other time-bins due to dark counts or noise.

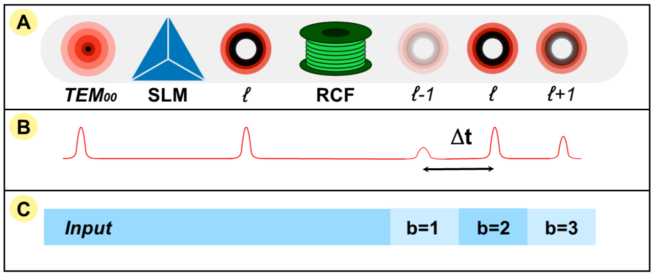

Figure 2. **A)** General model of the experiment: a spatial light modulator (SLM) converts a Gaussian beam to a particular OAM mode. Next, the superposition of OAM modes is generated in the RCF, and the modes are delayed depending on their OAM number. **B)** Mode-to-time mapping: the delay between the OAM modes allows us to distinguish them with a characterized time of flight measurement. Each of the pulses corresponding to an OAM mode is characterized by a specific amplitude. All of them, instead, are separated in time for $T = \Delta t$. **C)** The random bit, b, is extracted based on the time-bin at which the detection events occurred.

In low mean photon-number regime, equation (2) can be expressed as:

$$P(b_j) = (1-\xi_j-\xi_j\varepsilon)\eta_{det}(1-\varepsilon)^{d-1}, \tag{3}$$

where $\xi_j = |\langle 0|\alpha_j\rangle|^2 = e^{|\alpha_j|^2}$ is the probability of at least 1 photon in the signal and $|\alpha_j|^2 = \mu_j$ is the mean photon number at each mode. Ideally, if the initial superposition is balanced we have $\alpha_j = \alpha$ for all j.

2. *Case II: seeded QRNG*

The security of the DD protocol, presented in II A 1, can be improved to a seeded QRNG that increases the privacy of final random numbers generated. To each input mode, there corresponds a different crosstalk profile, hence, varying the input mode will enlarge the expected outcome space.

Similar to II A 1, denoting the set of OAM input states $\{M_i\}$ and corresponding outputs $\{N_j^i\}$ with probabilities $\{P(N_j^i|M_i)\}$ and $\{N\}$ be the set of all the outcomes regardless of input mode, one can define the probability of any outcome as:

$$P(b_j|M_i) = \sum_i P(M_i)P(N_j|M_i)\eta_{det}(1-\varepsilon)^{d-1}, \tag{4}$$

where $P(M_i)$ is the probability of selecting the OAM input mode M_i according to a classical input, seed. Defining multiple inputs provides the ground for introducing a security circumstance in which randomness can be generated without trusting the measurement apparatus, provided the preparation section is trusted and the measurement outcome meets the criteria. In general, distinguishing two (or more) neighboring OAM input modes from the measurement result comes with ambiguity. Indeed, the superposition created by each of the input modes has overlaps with the rest, thus one cannot uniquely

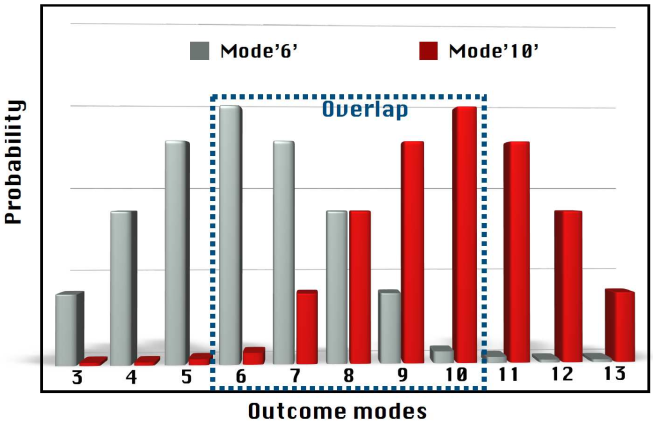

Figure 3. Schematic representation of Case II with binary inputs (OAM mode '6' and OAM mode '10'). The gray and red bars show the probability of a click triggered by binary input 0 (mode '6') or 1 (mode '10'), respectively. The dotted area is where the outcomes overlap significantly and the input mode cannot be distinguished unambiguously by the detection events.

determine the input mode from the measurement results. This uncertainty in the detection limits the adversary's (Eve) power to tamper with the measurement device's output. Eve's presence is detectable in post-processing through a mismatch of the sent and received clicks statistics. Figure 3 represents a simple example of Case II, with binary input. A click registered in modes $6,8,9,10$, the dotted rectangle, reveals no information about the input OAM mode, as it could be the result of either mode 6 or 10.

B. Security Estimation

Although an intuitive comprehension of the randomness concept exists, there are alternative ways of defining and understanding it. Fundamentally, the components of a random string should be uniformly distributed, and its elements necessitate to be modeled independently of one another. Otherwise stated, it should be unpredictable; this unpredictability or uncertainty in information can be formulated by information theoretic entropy in a mathematical concept. The most-known method for measuring the informativity of a random variable is defined by Shannon entropy [29, 30]. On the other hand, min-entropy provides a tighter measure to quantify randomness and is the most conservative means of estimating the unpredictability of a set of outcomes [31] and is defined as

$$H_{min}(X) = -\log_2[P_{guess}(X)], \tag{5}$$

where the guessing probability (P_{guess}), defined on the set of possible outcomes, is the maximum probability that an eavesdropper can correctly guess the output of an RNG. Since the worst-case scenario is considered in the min-entropy calculation, it is a more reliable estimate of a system's randomness.

In this protocol, we assume superposition of OAM modes in the RCF is a non-deterministic phenomenon imposed by the quantum theory. As shown in Figure 2 (B), we consider multiple temporal windows of width Δt, each corresponding to the arrival time of an OAM mode. Depending on the detected time-bin, the measurement device outputs $b \in \{1,2,3,\dots\}$, e.g., in the case of Figure 2 (B), the measurement device returns $b = 1$. Therefore, the measurement output (b) is resulting from a probabilistic random phenomenon and forms our probability distribution.

However, the string b is partially deterministic due to classical noises and losses stemming from the experimental apparatus' imperfections. Therefore, to ensure that the extracted random numbers have a quantum origin rather than a classical one, we should exclude all the possible noises introduced by devices imperfections. To account for all these imperfections, conditional min-entropy [32] as a measure to estimate the amount of extractable randomness in the presence of side-information is employed [33]. Note that, since the single-input model is the protocol implemented in this article, we assume full control over the device, and no quantum side-information is present. Hence, we limit ourselves to classical side-information, such as laser power fluctuation or losses in the preparation and detection. In this case, the conditional min-entropy on the variable b conditioned on classical side-information (E) reads [34]

$$H_{min}(b|E) = -\log_2 P_{guess}(b|E), \tag{6}$$

where

$$P_{guess}(b|E) = \sum_e P_E(e)\ \max[P(b|E=e)]. \tag{7}$$

The above maximization problem can be optimized numerically. The classical side-information probability is experimentally measured by characterizing the experimental devices. Note that these side-information can only be known to the eavesdropper and can not be controlled or manipulated by her.

III. EXPERIMENT

The QRNG protocol discussed in section II is experimentally implemented following Case I, (II A 1) and leveraging on the OAM degree of freedom. Photons owning an OAM different from zero are characterized by a helical phase factor $e^{i\ell\varphi}$, where φ is the azimuthal angle and ℓ is an unbounded integer value representing the quanta of OAM each photon possesses [35]. Different values of ℓ represent different discrete states on which superposition states can be devised. The experimental setup consists of a continuous laser at 1550 nm, which is carved to form train of pulses at a repetition rate of 12.5 MHz with approximately 2 ns width, see Figure 4 (A). Two cascaded intensity modulator, shown as one in Figure 4, guarantee high extinction ratio. The electrical signal is generated by an arbitrary waveform generator (AWG) that also provided the signal for clock synchronization.

The pulses are then collimated and further expanded with a beam expander and modulated by means of a spatial light

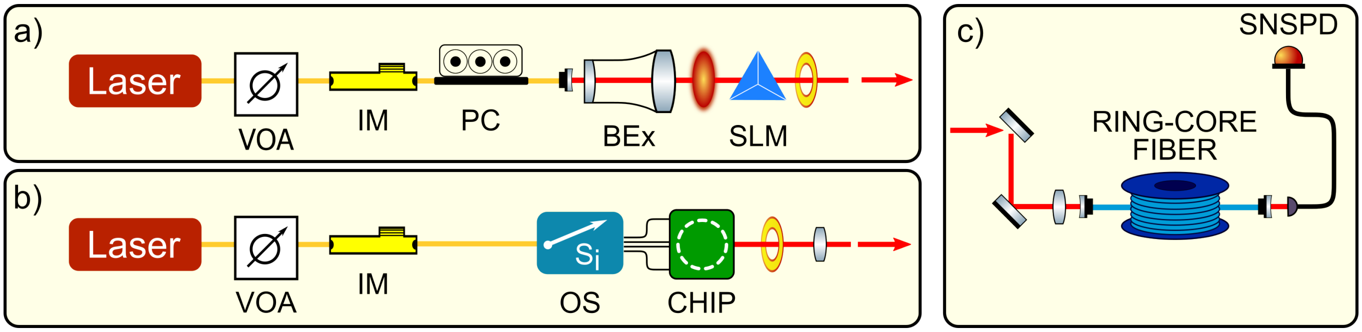

Figure 4. **a)** Experimental setup. VOA: variable optical attenuator; IM: intensity modulator; PC: polarization controller; BEx: beam expander; SLM: spatial light modulator. **b)** Proposal to implement Case II, II A 2. Chip: integrated silicon photonic chip able to excite OAM modes in the ring-core fiber; OS: optical switch. **c)** SNSPD: superconducting nano-wire single photon detector.

modulator (SLM) to a definite OAM mode, $\ell = -5$. The resulting signal is then coupled into the ring-core fiber which is capable of carrying up to 12 different OAM modes [26]. The fiber crosstalk stems from two main sources, misalignment of the mode to the RCF and bends and twists along the fiber, with the former being the most dominant factor. The intended superposition is created by exploiting the mode misalignment at the RCF facet. With the help of 2 adjustable mirrors, misalignment is introduced such that an expected crosstalk is observed at the output. For the purpose of this experiment, we achieved a 4-mode crosstalk state where the probability distribution in multiple trials of the experiment is presented in Figure 5. Different OAM modes exhibit different group velocities in a medium. Hence, it is possible to distinguish them by a time-of-flight measurement and furthermore, estimate the crosstalk. This estimation can be achieved if the RCF length is long enough to give a noticeable time delay between different modes. If such a condition is satisfied, it is straightforward to allocate different outcomes to distinctive detection time-bin that should be synced with the prepared states a priori. For this experiment, we used an 800 meter long RCF which amounts to 10 ns temporal separation of adjacent OAM modes. Provided that the optical pulses are short enough, such fiber length gives enough separation to uniquely distinguish the modes. At the output of the RCF, the pulses are then collimated and coupled into a standard single-mode fiber where they are redirected to a superconducting nano-wire single photon detector (SNSPD) with 83% detection efficiency and ≈ 50 dark counts per second. A time to digital converter (TDC) registers the detection events with temporal resolution of 1 ps.

IV. RESULT

In this section, we present the results of a test carried out following the Case 1 (II A 1), and performed to certify the protocol as a source of randomness. The Gaussian mode is first converted to OAM $\ell = -5$ and then coupled to the RCF while misalignment is introduced to create the intended crosstalk. We excite 4 dominant modes with close probabilities and several minor modes. Achieving crosstalk to higher number of modes is possible, however, the coupling loss will also increase. In case the input power is limited, this can lead to lower detection rate and a reduction of the rate of the random number generator. The total probability of finding the photon in the 4 dominant modes is more than 98% in each case, rendering the other excited modes impractical for randomness generation. The 4 dominant excited modes have comparable extinction ratios as also shown by the probability distribution presented in Figure 5.

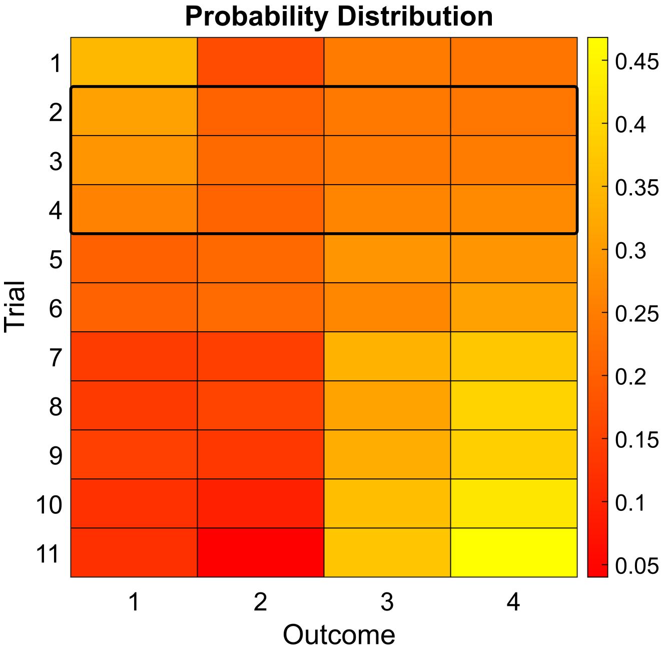

Figure 5. Probability distribution of the 4 outcomes obtained in 11 trials. Trials 2 to 4 (see the rectangle) were taken close to the balanced outputs condition, and they give almost uniform distribution.

We further applied a privacy amplification stage through a Toeplitz randomness extractor with proper parameter chosen based on $H_{min}(b|E)$ [36, 37] and security parameter $\varepsilon = 10^{-200}$ to remove any non-uniformities. To form the Toeplitz-hashing extractor, PRNG generated by a computer is used. With this stage applied to the random numbers, we achieved a generation rate of 10.5 MBit/sec. It is worth noting that the test performed here was not aimed to exploit the full potential of the proposal but a proof of principle and demonstration.

Finally, we performed a set of conventional statistical checks from Diehard to certify the randomness of extracted bits.As shown in Figure 6, the extracted random numbers passed successfully all the Diehard tests executed as the p-Values obtained are higher than the lower threshold 0.01. As such, the possibility to extract quantum randomness from OAM modes crosstalk in a RCF has been demonstrated.

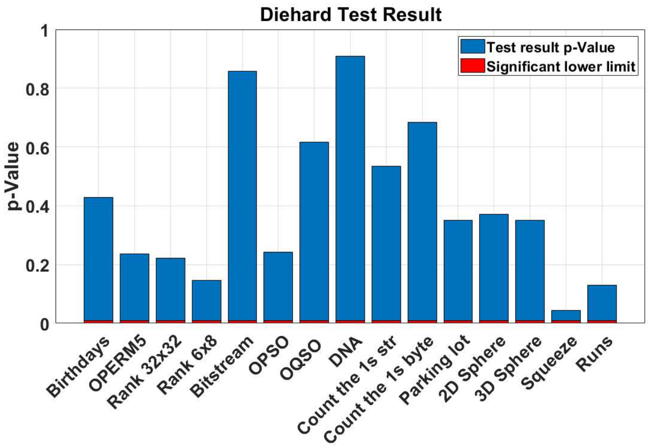

Figure 6. Statistical tests, Diehard, performed on the extracted random bits with their respective p-Values. All the tests were passed successfully as the p-Values obtained were higher than the lower limit 0.01. In the picture, only 15 test results are reported.

V. DISCUSSION

In this work, we successfully shown the possibility of extracting random numbers from crosstalk in an OAM carrying fiber, where the crosstalk is responsible for creating a superposition of OAM modes. In particular, after giving the description of the DD and semi-DI protocol, we realized the single input protocol (DD) and we demonstrated the possibility of extracting randomness from crosstalk profiles with a rate of more than 10 Mbit/sec. The quality of the randomness has been certified by executing conventional Diehard tests which have been successfully passed. Nonetheless, it must be noted that passing Diehard tests is a good sign for a genuine quantum randomness extraction, however, they must me regarded as preliminary tests. Indeed, they constitute a necessary but not sufficient step to claim the randomness as truly quantum.

The second and more promising scheme of a QRNG based on OAM mode crosstalk in a RCF has been discussed in Section II A 2. It implies a multi-input source seeding the RCF, thus increasing the overall secuirity (semi-DI case). An experimental proposal of this protocol is shown in Figure 4 (B). It can be realized with a fast switch consisting of intensity modulators and an integrated silicon chip [27, 38], which enables us to excite different modes at a high rate.

The RCF length is a critical parameter for being able to implement the proposed QRNG schemes. However, we emphasize that having a short enough optical pulse will allow us to reduce the length of the fiber as well as to distinguish more OAM modes. Indeed, besides those used in our experiment, the RCF can support more modes [28], and by exploiting them a significant gain in randomness extraction per detection can be obtained, leading to a more efficient QRNG.

As future plans, along with the experimental realization of the semi-DI protocol, a second approached to both Case I and II can be followed by exploiting superposition states as input to the fiber. Indeed, using a superposition of multiple OAM modes as the input state of the RCF reduces the overall loss as the fiber will act only as a mean to separate the modes in time, whereas in the proposed idea, the superposition is created at the interface of RCF by misalignments.

We believe this work can be the opening point of a new generation of QRNGs based on OAM, thus creating a wide room for improvements in this promising field.

Acknowledgment: We thank Roger Colbeck for helpful discussion.

Research funding: This work is supported by the Center of Excellence SPOC - Silicon Photonics for Optical Communications (ref DNRF123), by the EraNET Cofund Initiatives QuantERA within the European Union's Horizon 2020 research and innovation program grant agreement No. 731473 (project SQUARE), and by VILLUM FONDEN, QUANPIC (ref. 00025298). H. T. acknowledges the Innovate UK Industrial Strategy Challenge Fund (ISCF), project 106374-49229 AQuRand (Assurance of Quantum Random Number Generators).

Conflict of interest statement: The authors declare no conflicts of interest regarding this article.

Data availability: The data that support the findings of this study are available from the corresponding author upon reasonable request.

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241

[2] D. Bacco, I. Vagniluca, D. Cozzolino, S. M. M. Friis, L. Høgstedt, A. Giudice, D. Calonico, F. S. Cataliotti, K. Rottwitt, and A. Zavatta, "Toward fully-fledged quantum and classical communication over deployed fiber with up-conversion module," *Advanced Quantum Technologies*, vol. 4, no. 7, p. 2000156, 2021. [Online]. Available: https:

//onlinelibrary.wiley.com/doi/abs/10.1002/qute.202000156

[3] B. Da Lio, D. Bacco, D. Cozzolino, Y. Ding, K. Dalgaard, K. Rottwitt, and L. K. Oxenløwe, "Experimental demonstration of the dpts qkd protocol over a 170 km fiber link," *Applied Physics Letters*, vol. 114, no. 1, p. 011101, 2019. [Online]. Available: https://doi.org/10.1063/1.5049659

[4] R. Versluis and C. Hagen, "Quantum computers scale up: Constructing a universal quantum computer with a large number of qubits will be hard but not impossible," *IEEE Spectrum*, vol. 57, no. 4, pp. 24–29, 2020.

[5] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, "Quantum conference key agreement: A review," *Advanced Quantum Technologies*, vol. 3, no. 11, p. 2000025, 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.202000025

[6] H.-J. Cao, L.-Y. Ding, Y.-F. Yu, and P.-F. Li, "A electronic voting scheme achieved by using quantum proxy signature," *International Journal of Theoretical Physics*, vol. 55, no. 9, pp. 4081–4088, Sep 2016. [Online]. Available: https://doi.org/10.1007/s10773-016-3036-5

[7] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, p. 015004, Feb 2017. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.89.015004

[8] L.-Y. Deng and D. K. J. Lin, "Random number generation for the new century," *The American Statistician*, vol. 54, no. 2, pp. 145–150, 2000. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/00031305.2000.10474528

[9] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information*, vol. 2, no. 1, p. 16021, 11 2016. [Online]. Available: http://www.nature.com/articles/npjqi201621

[10] M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan, D. A. Ritchie, and A. J. Shields, "Efficient and robust quantum random number generation by photon number detection," *Applied Physics Letters*, vol. 107, no. 7, p. 071106, 2015. [Online]. Available: https://doi.org/10.1063/1.4928732

[11] R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation," 2011.

[12] G. Gras, A. Martin, J. W. Choi, and F. Bussières, "Quantum entropy model of an integrated quantum-random-number-generator chip," *Phys. Rev. Applied*, vol. 15, p. 054048, May 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevApplied.15.054048

[13] P. J. Brown, S. Ragy, and R. Colbeck, "A framework for quantum-secure device-independent randomness expansion," *IEEE Transactions on Information Theory*, vol. 66, no. 5, pp. 2964–2987, 2020.

[14] M.-H. Li *et al.*, "Experimental realization of device-independent quantum randomness expansion," *Phys. Rev. Lett.*, vol. 126, p. 050503, Feb 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.126.050503

[15] G. Foletto, M. Padovan, M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Experimental test of sequential weak measurements for certified quantum randomness extraction," *Phys. Rev. A*, vol. 103, p. 062206, Jun 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.103.062206

[16] H. Tebyanian, M. Zahidy, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, "Semi-device independent randomness generation based on quantum state's indistinguishability," *Quantum Science and Technology*, aug 2021. [Online]. Available: https://doi.org/10.1088/2058-9565/ac2047

[17] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Semi-device-independent heterodyne-based quantum random-number generator," *Phys. Rev. Applied*, vol. 15, p. 034034, Mar 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevApplied.15.034034

[18] D. Rusca, H. Tebyanian, A. Martin, and H. Zbinden, "Fast self-testing quantum random number generator based on homodyne detection," *Applied Physics Letters*, vol. 116, no. 26, p. 264004, 2020. [Online]. Available: https://doi.org/10.1063/5.0011479

[19] L. Huang, H. Zhou, K. Feng, and C. Xie, "Quantum random number cloud platform," *npj Quantum Information*, vol. 7, no. 1, p. 107, Jul 2021. [Online]. Available: https://doi.org/10.1038/s41534-021-00442-x

[20] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," *Quantum Science and Technology*, vol. 3, no. 2, p. 025003, feb 2018. [Online]. Available: https://doi.org/10.1088/2058-9565/aaa38f

[21] T. Roger, T. Paraiso, I. D. Marco, D. G. Marangon, Z. Yuan, and A. J. Shields, "Real-time interferometric quantum random number generation on chip," *J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B137–B142, Mar 2019. [Online]. Available: http://www.osapublishing.org/josab/abstract.cfm?URI=josab-36-3-B137

[22] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," *Applied Physics Letters*, vol. 104, no. 26, p. 261112, 2014. [Online]. Available: https://doi.org/10.1063/1.4886761

[23] C. Kollmitzer, S. Petscharnig, M. Suda, and M. Mehic, "Quantum random number generation," in *Quantum Science and Technology*. Springer International Publishing, 2020, pp. 11–34. [Online]. Available: https://doi.org/10.1007/978-3-319-72596-3_2

[24] H. Tebyanian, M. Avesani, G. Vallone, and P. Villoresi, "Semi-device independent randomness from d-outcome continuous-variable detection," 2020.

[25] Y. Shen, X. Wang, Z. Xie, C. Min, X. Fu, Q. Liu, M. Gong, and X. Yuan, "Optical vortices 30 years on: Oam manipulation from topological charge to multiple singularities," *Light: Science & Applications*, vol. 8, no. 1, p. 90, Oct 2019. [Online]. Available: https://doi.org/10.1038/s41377-019-0194-2

[26] S. Ramachandran and P. Kristensen, "Optical vortices in fiber," *Nanophotonics*, vol. 2, no. 5-6, pp. 455–474, 2013. [Online]. Available: https://doi.org/10.1515/nanoph-2013-0047

[27] M. Zahidy, Y. Liu, D. Cozzolino, Y. Ding, T. Morioka, L. K. Oxenløwe, and D. Bacco, "Photonic integrated chip enabling orbital angular momentum multiplexing for quantum communication," 2021.

[28] P. Gregg, P. Kristensen, and S. Ramachandran, "Conservation of orbital angular momentum in air-core optical fibers," *Optica*, vol. 2, no. 3, pp. 267–270, 2015.

[29] M. B. Ruskai, "Inequalities for quantum entropy: A review with conditions for equality," *Journal of Mathematical Physics*, vol. 43, no. 9, pp. 4358–4375, 2002. [Online]. Available: https://doi.org/10.1063/1.1497701

[30] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE mobile computing and communications review*, vol. 5, no. 1, pp. 3–55, 2001.

[31] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min-and max-entropy," *IEEE Transactions on Information theory*, vol. 55, no. 9, pp. 4337–4347, 2009.

[32] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.

[33] J.-Y. Haw, S. Assad, A. Lance, N. Ng, V. Sharma, P. K. Lam, and T. Symul, "Maximization of extractable randomness in a quantum random-number generator," *Physical Review Applied*, vol. 3, no. 5, p. 054004, 2015.

[34] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Left-over hashing against quantum side information," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5524–5535, 2011.

[35] L. Allen, M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, "Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes," *Phys. Rev. A*, vol. 45, no. 11, p. 8185, 1992.

[36] R. RENNER, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 06, no. 01, pp. 1–127, 2008. [Online]. Available: https://doi.org/10.1142/S0219749908003256

[37] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Left-over hashing against quantum side information," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5524–5535, 2011.

[38] Y. Liu, L. S. Rishøj, Y. Ding, Q. Saudan, L. K. Oxenløwe, and T. Morioka, "Orbital angular momentum mode multiplexing and data transmission using a silicon photonic integrated mux," in *Optical Fiber Communication Conference (OFC) 2021*. Optical Society of America, 2021, p. F4A.5.