UNIVERSITY *of York*

This is a repository copy of *Generalized Time-bin Quantum Random Number Generator with Uncharacterized Devices*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/200259/

White Rose
university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Generalized Time-bin Quantum Random Number Generator with Uncharacterized Devices

Hamid Tebyanian,[1] Mujtaba Zahidy,[2] Ronny Müller,[2] Søren Forchhammer,[2] Davide Bacco,[3] and Leif. K. Oxenløwe[2]

[1]*Department of Mathematics, University of York, Heslington, York, YO10 5DD, United Kingdom*
[2]*Centre of Excellence for Silicon Photonics for Optical Communications (SPOC),*
Department of Electrical and Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark
[3]*Department of Physics and Astronomy, University of Florence, Via Sansone 1, Sesto Fiorentino, 50019, Italy*

Random number generators (RNG) based on quantum mechanics are captivating due to their security and unpredictability compared to conventional generators, such as pseudo-random number generators and hardware-random number generators. This work analyzes evolutions in the extractable amount of randomness with increasing the Hilbert space dimension, state preparation subspace, or measurement subspace in a class of semi-device-independent quantum-RNG, where bounding the states' overlap is the core assumption, built on the prepare-and-measure scheme. We further discuss the effect of these factors on the complexity and draw a conclusion on the optimal scenario. We investigate the generic case of time-bin encoding scheme, define various input (state preparation) and outcome (measurement) subspaces, and discuss the optimal scenarios to obtain maximum entropy. Several input designs were experimentally tested and analyzed for their conceivable outcome arrangements. We evaluated their performance by considering the device's imperfections, particularly the after-pulsing effect and dark counts of the detectors. Finally, we demonstrate that this approach can boost the system entropy, resulting in more extractable randomness.

I. INTRODUCTION

Randomness is indispensable for simulation, gambling, and numerous cryptographic applications, e.g., quantum key distribution (QKD) [1, 2], where the protocol's security is guaranteed by random selections of the encoding and measurement bases [3]. Traditional randomness generators rely on deterministic processes, which are, in principle, predictable. However, unlike the deterministic evolution of classical systems, quantum mechanics grants the ability to generate genuine randomness based on the quantum measurement outcome that is entirely unpredictable [4, 5]. A random number generator (RNG), in general, should deliver unpredictable and secure random numbers by exploiting effective instruments aiming to make it performant, high rate, and commercially affordable. Quantum RNG (QRNG) can be an outstanding choice in satisfying the needs for security, practicality, and affordability; nevertheless, any imperfection in the physical realization may cause information leakage which an eavesdropper could use to predict the QRNG's outcome [6, 7].

Nowadays, QRNGs are commercially available, symbolizing one of the most successful developments of quantum technologies. In Device-dependent (DD) QRNGs, the user must trust the device's performance. This type of QRNG requires a detailed understanding of the functioning of the in-use devices to constrain the output's randomness [8–11]. Although DD QRNGs randomness is guaranteed by quantum theory, any gap between theoretical and real-world implementation, such as experimental errors, device imperfections, or dishonest producers, may enable an adversary to predict the QRNG's outcomes and thus endanger the system's security [12–16]. At the same time, in device-independent (DI) protocols, one can certify randomness without relying on assumptions about the device's performance. These protocols utilize the non-local property of quantum theory to guarantee the output's randomness. DI QRNGs are, therefore, highly secure, and thus no assumptions on the eavesdropper are made. Implementing DI QRNGs, nevertheless, can be demanding as it involves conducting a loophole-free Bell test, which is a challenging experimental task with a typically low generation rate [17].

Contrary to DD and DI QRNGs, semi-device independent QRNGs are based on protocols that allow for high-rate generation, acceptable security, and simplicity in implementation [18–21]. In this class, the performance is boosted by taking a few assumptions on the working principle of the experimental apparatus, e.g., trusting the measurement [22, 23] or the preparation device [19, 24] or weaker hypothesis like bounding the energy or the overlap [25, 26] of the generated states, while guaranteeing the security by accounting for all possible attack attempts within our assumptions [27].

This work studies a class of semi-DI QRNGs founded on the basis of restraining the states' overlap by employing a time-bin encoding scheme and single-photon detection. The overlap bound guarantees that the prepared states are non-orthogonal and hence, no measurement can perfectly distinguish them [26, 28]. While the inability of predicting the outcome of measurement by the user is the source of randomness, the indistinguishability of the state is the source of security, from the perspective of the measurement apparatus. The entropy and extractable randomness are optimized, and compared, with the help of semi-definite programming (SDP). We discuss the improvement in entropy and randomness generation rate with increasing the number of time-bin or input states.

The main contribution of this work is to investigate the impact of increasing or adjusting the number of time bins on the extractable amount of randomness and the system's generation rate with the security assumption. We found an upper bound on the number of input-output for a general number of time bins and showed that the system's entropy improves with a increasing number of time bins. We also discuss the experimental challenges from both state preparation and measurement points of view. Similarly, we demonstrate that the generation rate increases by optimally dispersing the weak coherent state (WCS) in time-bin configurations, which can significantly enhance this approach's performance for practical
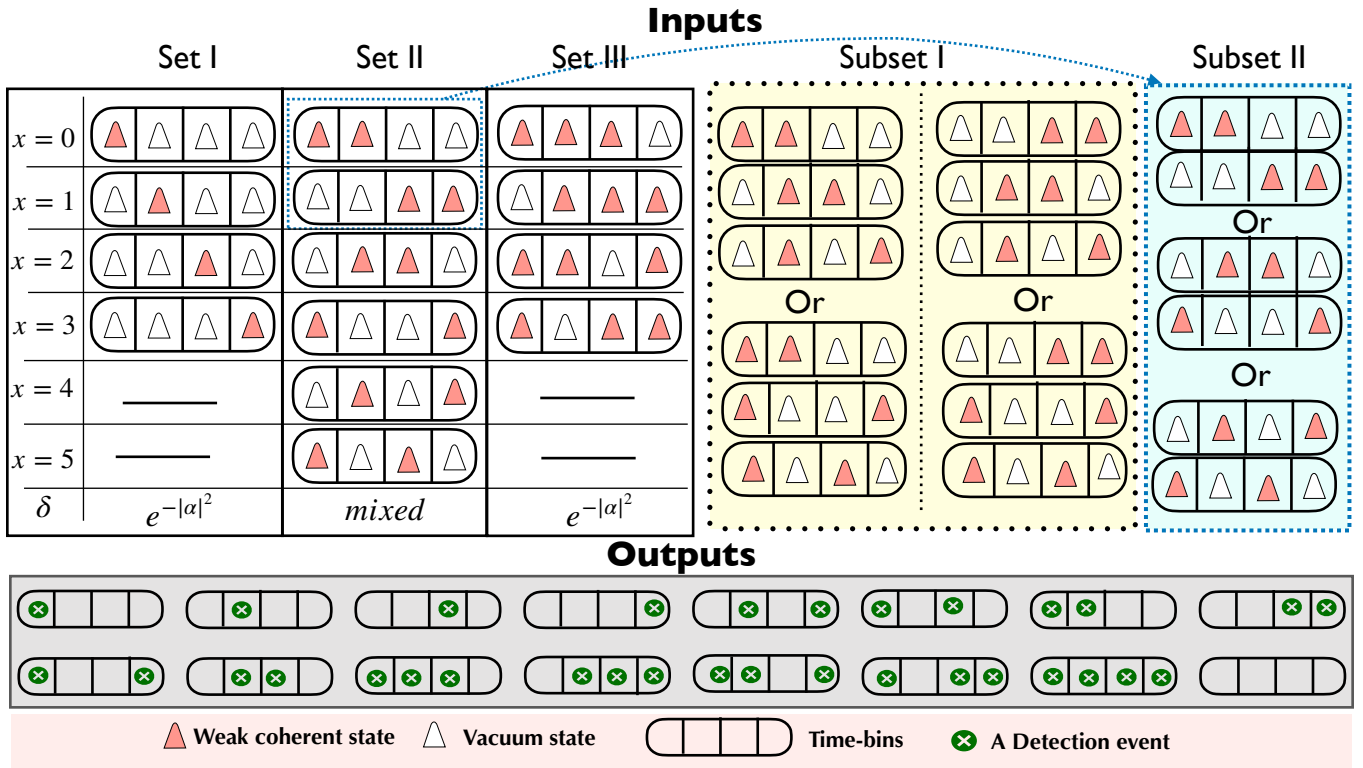
Inputs

Figure 1. Possible input-output configurations with four time-bin case. Inputs: Sets I, II, and III show input configurations where one, two, and three weak coherent states are positioned in time-bins, respectively. Subsets I and II are subsections of set II where the overlap is mixed. Outputs: 16 possible outcome configurations for four time-bin case, where some are theoretically impossible, e.g., obtaining four detection events, while real-world errors such as the detector's dark counts make it probable.

applications.

II. PROTOCOL

The QRNG protocol introduced here is based on the prepare-and-measure scenario, where the prepared states' overlap is bounded while no other assumptions are required on the rest of the setup [25, 29, 30].

A. Preparation and Measurement Stages

Quantum mechanics does not allow any measurement to distinguish non-orthogonal states perfectly [31]. This feature can be used to generate random numbers without trusting the measurement apparatus. Here, we address a general case of non-orthogonal states in a time-bin encoding with n bins and m distributed weak coherent pulses $|\alpha\rangle$. The states $|\psi_i\rangle$,

$$|\psi_i\rangle = |0\rangle^{n-m}|\alpha\rangle^{\otimes m} = |0\rangle \otimes |\alpha\rangle \otimes ... \otimes |\alpha\rangle \otimes |0\rangle, \quad (1)$$

are formed by permuting the m WCSs in the n bins where the rest are filled with vacuum states (VS). The states $|\psi_i\rangle$ are required to respect an overlap condition that satisfies the protocol's assumption:

$$|\langle \psi_i | \psi_j \rangle| \geq \delta, \quad \forall i \neq j, \quad (2)$$

where δ is the overlap bound. The non-zero overlap guarantees the inability to distinguish the states by performing any measurement, hence, allowing to generate secure randomness from the ambiguity therein [31]. A simple illustration of state formation in time-bin encoding can be found in [25].

In this scenario, the general case is defined by allowing the number of time-bins n to increase without any limits as well as the number of WCSs m, where $1 \leq m < n$. We denote a *configuration* of n time-bins and m WCSs with (n,m)-configuration. The number of states in a (n,m)-configuration is given by the binomial coefficient, $C_n^m = n!/(m!(n-m)!)$, formed by all possible combinations of placing m WCSs in n time-bins. However, not all groups of states in a configuration respect the overlap bound, Eq. (2). A careful examination of combinations shows that in an (n,m)-configuration, there are subsets of states with specific overlaps. Each subset is then divided into groups of states that are equivalent w.r.t. the overlap value. Fig. (1) shows the $(4,2)$-configuration and its subsets with different overlap values. To be noted that while the four groups of subset I are not closed w.r.t. each other, adding any elements of another group to any of them violates the overlap bound.

It is easy to show that the number of subsets is equal to

$$\begin{cases} m & \text{if} \quad 2m-n \leq 0 \\ n-m & \text{if} \quad 2m-n > 0. \end{cases}$$

Consequently, a (n,m)-configuration can have a total overlap value of the form

$$|\langle\psi_i|\psi_j\rangle| = \langle0|0\rangle^{n-2m+s}\langle0|\alpha\rangle^{2(m-s)}\langle\alpha|\alpha\rangle^{s}$$
$$= \langle0|\alpha\rangle^{2(m-s)}, \quad (3)$$

where s is the number of coinciding $\langle\alpha|\alpha\rangle$ WCSs. We denote an (n,m)-configuration with s coinciding WCSs as $n_{m,s}$ with $n > m \geq s$.

In the following, we will only consider the case of equality in Eq. (2). We denote with $\mathscr{B}(n,m,s)$ the maximum number of states in any subset $\mathscr{S}$ of the (n,m)-configuration such that all elements in $\mathscr{S}$ have the same value of s pairwise, with s defined as in Eq. (3). It is of relevance to know $\mathscr{B}$ for any configuration as it defines the number of inputs and possible outputs in our prepare-and-measure QRNG protocol. This question is closely related to *constant weight binary codes*. To see this, we can identify bins that contain a WCS with '1' and bins that contain the vacuum state with '0', such that we identify each state in a (n,m)-configuration with a binary vector of length n and weight m. Each subset $\mathscr{S}$ can then be directly identified with a code of length n, Hamming distance d, and weight m, where Hamming distance and s are related as $d = 2(m-s)$. Eq. (3) can then be written as $|\langle\psi_i|\psi_j\rangle| = \langle0|\alpha\rangle^{d}$. In the context of constant weight binary codes, there exists the well-known but open question of determining the maximum number of codewords $\mathscr{A}(n,m,d_{\min})$, where $d_{\min}$ refers to the minimum distance of the code. $\mathscr{B}(n,m,s)$ can be upper-bounded by $\mathscr{A}(n,m,2(m-s))$ which in turn can be upper-bounded by different theoretical bounds [32–34]. Lower bounds to $\mathscr{A}$, typically by explicit construction [35, 36], cannot be applied to $\mathscr{B}$ as the codes can contain state-pairs with $d > d_{\min}$ which translates to a violation of Eq. (2) since $\delta = \langle0|\alpha\rangle^{d}$. Increasing d reduces the overlap value and therefore reduces the ambiguity in their measurement. Instead, we show here an explicit lower bound C by simple construction: For $2m-n \leq 0$, all codewords share s '1's at the same positions. Distribute the remaining $m-s$ ones in the remaining $n-s$ slots so that there is no coinciding ones, and fill the $R = n - \lfloor\frac{n-s}{m-s}\rfloor(m-s) - s$ leftover columns with zeros.

$$\mathscr{B} = \overbrace{\begin{bmatrix} 1 & \dots & 1 & 1 & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & 1 & 0 & \dots & 0 & 1 & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\ 1 & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 & 1 & \dots & 1 & 0 & \dots & 0 \end{bmatrix}}^{n-s}$$
$$\underbrace{\quad}_{s}\underbrace{\quad}_{m-s}\underbrace{\quad}_{m-s}\underbrace{\quad}_{m-s}\underbrace{\quad}_{R}$$

This results in $C = \lfloor\frac{n-s}{m-s}\rfloor$ different states. If instead $2m - n > 0$, all codewords share $n+s-2m$ zero positions and the remaining $2m-s$ slots are divided into sections with $m-s$ zeros. $\mathscr{B}$ can therefore be lower-bounded by

$$\mathscr{B}(n,m,s) \geq C(n,m,s) = \begin{cases} 1 & \text{if } n+s-2m < 0 \\ \lfloor\frac{n-s}{m-s}\rfloor & \text{if } 2m \leq n \\ \lfloor\frac{2m-s}{m-s}\rfloor & \text{if } 2m > n \end{cases} \quad (4)$$

In the absence of noise or errors, the number of all possible outcomes, B, follows from the click or no-click event when a state is sent. For an $n_{m,s}$-configuration, the number of distinct outcomes is obtained as

$$B = C(2^m - 1) - 2^{m-s} + 1. \quad (5)$$

In the no-frills case, only one WCS is placed, $m = 1$, in each time-bin regardless of the number of bins, see Fig. 1 (set I). There are always $B = n + 1$ possible outcomes in this case — one for each input plus one for the no-click (indeterminate) event, which occurs randomly, suggesting that the entropy should be minimal. Fig. 1 (Set II and III) shows the cases with $m = 2$ and $m = 3$, respectively. Note that the case with $m = 2$ WCSs has two subsets with 1 and 2 coinciding WCSs with 4 equivalent groups for $m = 2$ and 3 for $m = 3$. In the ideal situation, the number of outcomes follows Eq. (5). However, in a real implementation, due to noise, dark counts, or after-pulsing, all $B = 2^n$ outcomes, shown in Fig. 1 for $n = 4$ - Outputs, are probable although with negligible probability. These errors and imperfections are viewed as classical side-information serving the adversary to predict the measurement outcome. All sorts of probable classical side-information and correlations (between preparation and measurement sides) are considered in the security estimation. The user can monitor these correlations and stop the protocol in case of observing considerable noise.

B. Security estimation

Despite the fact that the generation of random numbers in a QRNG is based on the intrinsic probabilistic nature of quantum mechanics, the raw data outcome is a mixture of the sequences generated from deterministic classical sources and quantum processes. Therefore, it is essential to estimate the amount of extractable randomness in a defined protocol and later use it to exclude the classical contribution. The quantity min-entropy ($H_{\min}$) measures the maximum extractable randomness provided that an adversary can optimally guess the generator's outcome knowing the working principle of the devices. To account for any side information, we used conditional min-entropy and considered only classical side-information. Throughout this work, we assumed a trusty source with no quantum correlation to the outside world.

The conditional min-entropy on the variable b conditioned on classical side-information E reads [37]

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

where P_{guess} is the maximum probability that an adversary can guess the measurement outcome with a complete understanding of the devices' working principle and classical noises. In a semi-DI framework, the guessing probability should be maximized over all possible preparation and measurement strategies. P_{guess} reads:

$$P_{\text{guess}} = \max_{p(x),\psi_x,M_b^\varsigma} \left\{ \sum_{x=0}^{I-1} p(x) \sum_\varsigma \max_b \left[\langle\psi_x|M_b^\varsigma|\psi_x\rangle \right] \right\}, \quad (7)$$

where $p(x)$ is the probability of transmitting input x, $M_b^\varsigma = P(\varsigma)\Pi_b^\varsigma$ are weighted measurement strategies over all positive operator valued measurements (POVM), and ς, known by the adversary, represents the classical correlations between the measurement devices and environment (e.g., adversary). Each POVM Π_b^ς, labeled by ς, can be implemented with probability $P(\varsigma)$. I and B are the numbers of inputs and outcomes, respectively. As shown in [38], the maximizations in Eq. (7) can be grouped as they occur for the same value of b at given x, this would significantly ease up the optimization process. Therefore the total number of possible measurement strategies for given input would be B^I, thus $\varsigma \in \{\varsigma_0, \ldots, \varsigma_{I-1}\}$, where $\varsigma_s \in \{0, \ldots, B-1\}$. Following the same approach presented in [25, 26, 39], P_{guess} for the balanced input case, $p(x) = 1/I$, can be written as:

$$P_{\text{guess}} = \frac{1}{I} \max_{\{M_b^\varsigma, \hat{\rho}_x\}} \sum_{x=0}^{I-1} \sum_{\varsigma} \text{Tr}[\hat{\rho}_x M_{\varsigma_x}^\varsigma], \tag{8}$$

where $\hat{\rho}_x = |\psi_x\rangle\langle\psi_x|$, and $\text{Tr}[\hat{\rho}_x M_b^\varsigma] = p(b|x)$ is the conditional probability of obtaining outcome b given input x. Eq.(8) suggests that P_{guess} depends on the state's overlap rather than input state $\hat{\rho}_x$. Besides, the optimization problem in Eq.(8) can be bounded to a I-dimensional Hilbert space; for more detail, see [25, 26, 38].

The optimization problem in P_{guess} can be efficiently solved by casting it into semi-definite programming (SDP), which is a numerical tool for solving complex optimization problems.

Following the same argument presented in [25, 26, 38, 39], we can show that for the protocol under study, strong duality holds which means both the primal and dual forms of the SDP exist. By feeding the SDP with the experimental conditional probabilities $P(b|x)$ and defining the overlap bound, the SDP can numerically optimize P_{guess}. Afterward, the conditional min-entropy, Eq. (6), can be calculated.

It should be noted that the security estimation is applicable for multiple input-output (IO) cases. The number of inputs can vary from 2 to the number of available states in an equivalence group in a $n_{m,s}$-configuration. For example, one can choose to send only 2 out of 4 states in set I in figure (1). The computational cost (CC) is associated with the number of IO in the system and can affect the system's overall generation rate. This is due to an increment in the time it takes to execute the SDP, which in turn leads to a decrease in the system's overall efficiency. Thus, it is important to be mindful of the impact of increased computational complexity when considering adding more IO to the system. Fig. (2) shows the CC as a function of the number of IO obtained on a personal computer.

Given a specific input, an outcome probability is a function of mean photon number per pulse μ, detector efficiency η_{det}, noise in the form of background light, dark count, and afterpulsing. An approach to reduce the complexity of SDP is to group the outcomes, from an adversary point of view. This will drastically reduce the complexity of SDP.

It can be explained in a $n_{1,0}$-configuration where, in the absence of noise, there are $n + 1$ different outcomes. The common outcome is the no-click one, and the others are 1-click due to the WCS. In this case, a new variable ($E \in$
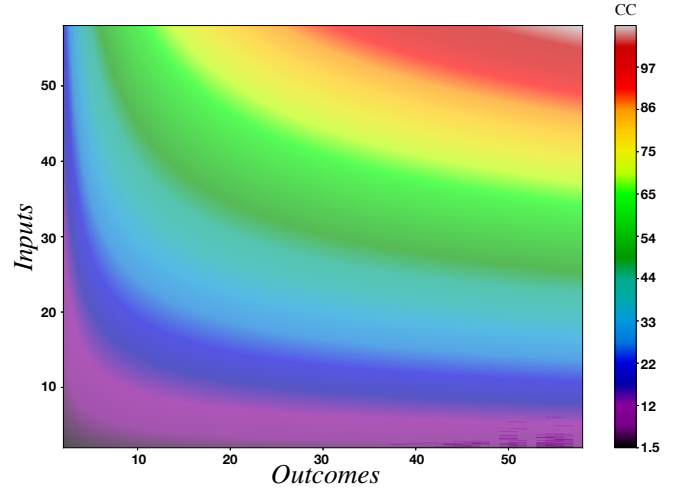

Figure 2. Computational cost (CC), colour bar, as a function of the number of inputs and outputs. Note that the CC is plotted on a logarithmic scale, expressing that CC increases exponentially with the number of IO.

$\{0, 1\}$) can be assigned to the outcomes in which $E = 0$ corresponds to the no-click event, all '0', while E is 1 for $b \in \{\underbrace{100\cdots0}_{n}, 010\cdots0, \cdots, 0\cdots01\}$.

$$P_{\text{guess}} = \max_{p(x), \rho_x} \left\{ \sum_{x=0}^{2} p(x) \right.$$
$$\left. \sum_{\varsigma_0, \varsigma_1, \varsigma_2 = 0}^{1} \max\left\{ \text{Tr}[\hat{\rho}_x M_{E=0}^{\varsigma_0, \varsigma_1, \varsigma_2}], 1 - \text{Tr}[\hat{\rho}_x M_{E=0}^{\varsigma_0, \varsigma_1, \varsigma_2}] \right\} \right\} \tag{9}$$

For configurations with more WCSs more variables (corresponding to E) should be specified as there would be more indeterminate events.

The many-outcome approach is a computationally simplified, effective, and efficient method of increasing entropy without significantly increasing CC. This is a result of comparing the computational cost with increasing the number of inputs versus the number of outcomes which shows that the former increases faster, see Fig. (2). Hence, in an $n_{m,s}$ configuration, an efficient strategy is to keep the number of inputs fixed and low and increase the number of outcomes.

The many-outcome approach is studied for the continuous variable (CV) case in Ref. [39] where the focus is on heterodyne and homodyne detectors with binary input. In the time-bin encoding scheme, we can control the number of outcomes by adjusting the number of time-bins or the number of WCS in each configuration. It should be noted that the overlap bound is not considered in this argument and should be added as criteria when solving the SDP. As an example with dual input, it is shown in Fig. (3) that conditional entropy rises when the number of outcomes increases.

As shown in table (I)-top, the overlap could be different from case to case; this causes the optimal value of conditional min-entropy to take place at different mean-photon numbers; the inset of Fig. (3) shows the optimal mean-photon number

Table I. **Many-input vs Many-outcome approach.** *Top:* Many-outcomes approach with binary input; Examples of many-outcome scenarios with two input states. Note that the overlap value differs in each case. *Bottom:* Many-input approach with categorizing the outcomes. Note: x and – represent detection and no-detection events, respectively.
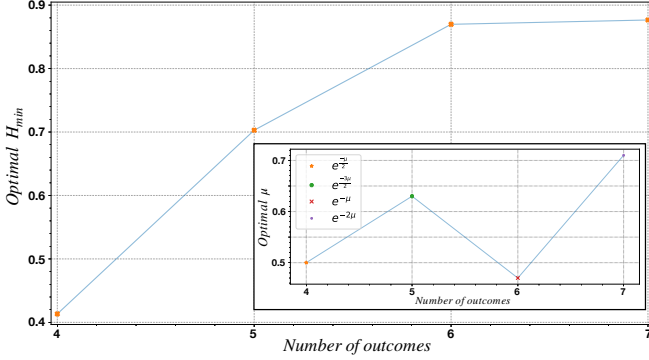
Binary state	Possible outcomes (noise-less)				Overlap
$\|\alpha\rangle\|0\rangle$ $\|0\rangle\|\alpha\rangle$	x − − x	− − − x			$\varsigma = e^{-\mu}$
$\|\alpha\rangle\|0\rangle\|0\rangle$ $\|\alpha\rangle\|\alpha\rangle\|0\rangle$	x − − x x −	− − − x − −			$\varsigma = e^{-\frac{\mu}{2}}$
$\|0\rangle\|0\rangle\|\alpha\rangle$ $\|\alpha\rangle\|\alpha\rangle\|0\rangle$	− − x x x −	− x − x − −	− − −		$\varsigma = e^{-\frac{3\mu}{2}}$
$\|0\rangle\|\alpha\rangle\|\alpha\rangle$ $\|\alpha\rangle\|\alpha\rangle\|0\rangle$	− x x x x −	− x − x − −	− − x − − −		$\varsigma = e^{-\mu}$
$\|0\rangle\|0\rangle\|\alpha\rangle\|\alpha\rangle$ $\|\alpha\rangle\|\alpha\rangle\|0\rangle\|0\rangle$	− − x x x x − −	− x − − x − − −	− − x − − − − x	− − − −	$\varsigma = e^{-2\mu}$

Input	$\|\alpha\rangle\|0\rangle$, $\|0\rangle\|\alpha\rangle$	$\|\alpha\rangle\|0\rangle\|0\rangle$, $\|0\rangle\|\alpha\rangle\|0\rangle$, $\|0\rangle\|0\rangle\|\alpha\rangle$	$\|\alpha\rangle\|0\rangle\|0\rangle\|0\rangle$, $\|0\rangle\|\alpha\rangle\|0\rangle\|0\rangle$ $\|0\rangle\|0\rangle\|\alpha\rangle\|0\rangle$, $\|0\rangle\|0\rangle\|0\rangle\|\alpha\rangle$
Output	x −, − x, − −	x − −, − x −, − − x, − − −	x − − −, − x − − − − x −, − − − x − − − −

Figure 3. Optimal conditional min-entropy as a function of the number of outcomes with binary input. *Inset:* Optimal mean-photon number (μ), i.e., the μ which delivers the maximum entropy, as a function of the number of outcomes for states with different overlaps.

as a function of outcomes for different overlaps. Similarly, a many-input case can be introduced while keeping the outcome minimal. Table (I)-bottom shows examples of the possible setting of the many-input approach.

C. Conditional Probability

Given the inputs and the outputs, one can compute the input-output correlation by employing the conditional probability $p(b|x)$, i.e., the probability of receiving outcome b given input x:

$$p(b|x) = \sum_{\varsigma} p_{\varsigma} \mathrm{Tr}[\hat{\rho}_x \hat{\Pi}_b^{\varsigma}], \qquad (10)$$

where $\hat{\rho}_x$ are the prepared states, $\hat{\Pi}_b^{\varsigma}$ are the POVMs describing the measurement, ς the classical variable provided to the adversary which describes the classical correlations between the experimental devices and the adversary.

The detector's dark count rate (DCR) and ambient light are usually considered constant (on average); as they are independent of the incident photon's energy. However, the likelihood of obtaining an afterpulse click is directly related to the system's repetition rate. Some detection events may not be caused by a WCS but could be afterpulses of an earlier detection event—the higher the system's repetition rate, the higher the chance of an afterpulse in the subsequent time-bins. Consequently, it is critical to consider the afterpulsing effect for practical situations.

The probability of registering a detection event in the Tth bin is mainly subject to the presence of a WCS in that bin and afterpulsing due to detections in the earlier bins. Assuming that afterpulsing only happens due to a detection event in the immediate bin before, the probability of detection in bin T can be written as:

$$
\begin{aligned}
P_\alpha^T(1) &= 1 - e^{-\eta_{\det}L|\alpha|^2} + \varepsilon + P_{ap}P_\alpha^{T-1}(1) \\
&= 1 - e^{-\eta_{\det}L|\alpha|^2} \\
&\quad + \varepsilon + P_{ap}(1 - e^{-\eta_{\det}L|\alpha|^2} + \varepsilon + P_{ap}P_\alpha^{T-2}(1)) \\
&\cdots \\
&= \frac{1 - e^{-\eta_{\det}L|\alpha|^2} + \varepsilon}{1 - P_{ap}}.
\end{aligned}
\qquad (11)
$$

where $P_\alpha^T(1)$ is the probability of registering a detection when sending $|\alpha\rangle$, $\eta_{\det}$ and L are detector efficiency and source-measurement loss, ε is for devices' imperfections and classical noises, e.g., dark counts, background noise, etc., and P_{ap} represents the afterpulse probability due to a detection event at one bin distance which is the intrinsic character of a single-photon avalanche diode (SPAD) that can be characterized experimentally. In Eq. (11), we substituted $P_\alpha^{T-2}(1)$ with its value and formed a geometric series to find the result.

The rest of the probabilities can be expressed as

$$
\begin{aligned}
P_\alpha(0) &= 1 - P_\alpha(1) \\
P_\varnothing(1) &= P_{ap}\left(\frac{1 - e^{-\eta_{\det}L|\alpha|^2} + \varepsilon}{1 - P_{ap}}\right) + \varepsilon \\
P_\varnothing(0) &= 1 - P_\varnothing(1),
\end{aligned}
\qquad (12)
$$

where $P_\alpha(1)$, $P_\varnothing(1)$, $\big(P_\alpha(0), P_\varnothing(0)\big)$ represent the probability of registering a click $\big($no-click$\big)$ event when states $|\alpha\rangle$ and $|0\rangle$ are transmitted. Given Eqs. (11) and (12), we can compute all the possible conditional probabilities for any input-output dimension.

D. Randomness Generation Rate

Besides security, the randomness generation rate is another key parameter of any QRNG. We previously discussed the

security estimation for the general case with multiple input-output in the presence of classical side information and noise and how it scales up. Here, we consider the eventual generation rate in the time-bin protocol.

For a weak coherent pulse source with repetition rate f, the input-state generation, comprised of n time-bins, scales down as f/n. However, the extractable randomness is determined by $H_{\min}$, Eq. (6), and the number of states available in an equivalence group in a $n_{m,s}$-configuration. Hence, the rate can be written as,

$$R = \frac{f}{n} \cdot |n_{m,s}| \cdot H_{\min}(n_{m,s}, \upsilon, \eta_{\det}, \mu_{\text{optimal}}), \qquad (13)$$

where $|n_{m,s}|$ is the cardinality of the input-state set and $H_{\min}(n_{m,s}, \upsilon, \eta_{\det}, \mu_{\text{optimal}})$ is the maximum extractable entropy from that set considering optimal μ, all the sources of noise, and detector efficiency. As discussed in section (II B), a general solution for $H_{\min}$ considering all the parameters is not feasible to present and this quantity needs to be calculated and optimized for each case.

It should be noted that we assume f being below the detector's dead-time to avoid missing a signal. Additionally, the analysis considers all the possible inputs and outcomes. The investigation would become more straightforward in the case of the many-input or many-outcome approaches.
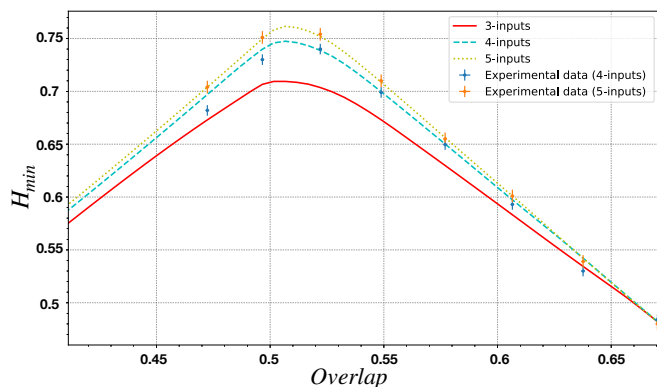

Figure 4. Conditional min-entropy as a function of states' total overlap. The solid, dashed, and dotted curves represent the theoretical predictions for 3, 4, and 5 input configurations, respectively. At the same time, the blue and orange dots show the experimental data for 4 and 5 input cases measured with SPAD with 83 % efficiency.

III. EXPERIMENTAL IMPLEMENTATION

This section investigates the experimental implementation and some practical considerations of this protocol. According to the protocol, the detection apparatus is considered a black box with no assumption on its performance. However, state generation must respect an overlap criteria, Eq. (2), which translates in two conditions; limited mean photon number μ per WCS and WCS positioning in an n-time-bin state.

Fig. (5) shows a schematic representation of the setup. The n-time-bin state is generated by carving a 1550 nm continu-
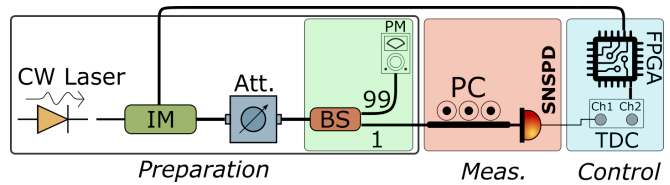

Figure 5. Schematic of the QRNG setup. A continuous wave laser (CW) is carved to form a train of pulses according to the protocol selected by the user. A combination of an attenuator (att.) and a 99:1 beamsplitter bring the power to single photon level where the 99% output is monitored constantly with a power meter (PM) to certify the overlap condition. The single photons are then sent to a detector (SNSPD) for measurement. The polarization controller (PC) adjusts the polarization to maximize efficiency. The detection events are registered with a time-to-digital converter (TDC). State generation and measurement are governed and synchronized with the field programmable gate array (FPGA).

ous wave laser (CW) into pulses with 120 ps pulse width and a repetition rate of 31.25 MHz. Two cascaded intensity modulators, shown as one in the setup, guarantee high extinction ratio and perfect state generation. The repetition rate is chosen such that it matches the detector's dead-time and to minimize the chance of no-detection events. A field programmable gate array (FPGA) generates the electrical signal to drive the intensity modulators and to synchronize the measurement apparatus. To verify the overlap criteria, WCS placement is controlled such that the final state matches a subset, see Fig. (1). A 99:1 beamsplitter separates the signal with the 99% arm redirected to a power meter (PM). A variable optical attenuator (VOA) then sets the mean photon number to μ_{optimal} extracted from the security estimation process.

The quantum states are then sent and measured with a superconducting nanowire single photon detector (SNSPD) with 30 ns dead-time, 80 DCR, and 83% detection efficiency. The detection events are then registered with a time-to-digital converter (TDC) with 1 ps resolution and are analyzed for randomness extraction.

It is worth noting that in the time-bin encoding, detector's dead-time is the main limiting factor for high repetition rate state generation.

IV. RESULTS & DISCUSSION

This section presents the theoretical and experimental min-entropy of different configurations, intending to validate the theoretical estimations. Foremost, the input-output correlation $P(b|x)$ is estimated by performing several measurements with various overlaps and gathering the detector's outcomes b for given input x. The extractable amount of randomness is evaluated by inserting the input-output correlation and states' overlap into the SDP, which numerically computes the min-entropy.

We consider the simplest case: supplying one bin with a WCS and filling the rest of the bins with VS. Possible outcome configurations increase by raising the number of inputs,
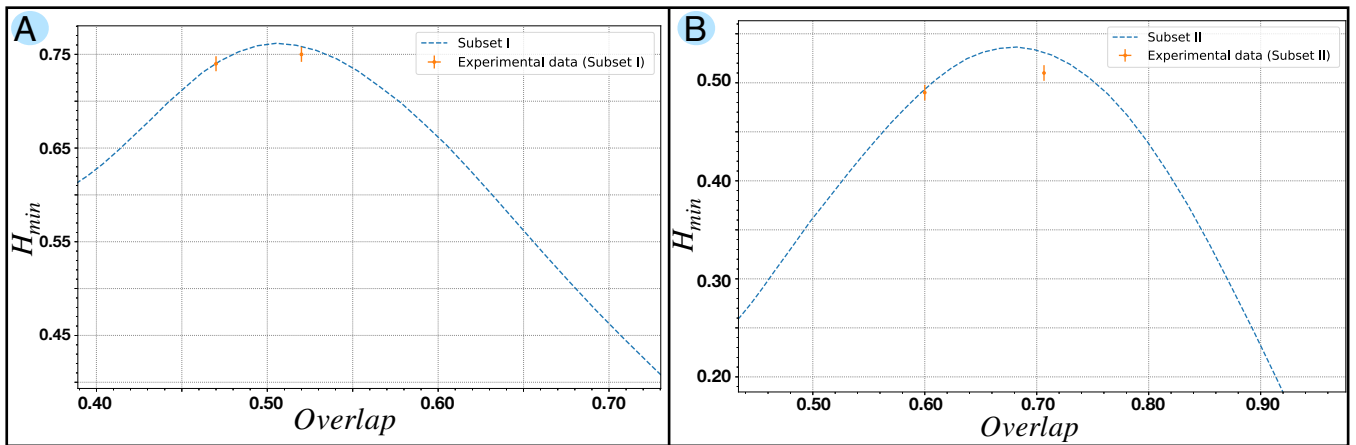
Figure 6. Conditional min-entropy as a function of states' total overlap for Subsets I (A) and II (B) represented in Fig. 1. In both figures, the dashed line shows the theoretical predictions, and the orange dots represent the experimental data.

leading to a different input-output correlation and entropy. As shown in Fig. 4, the amount of extractable randomness conditioned on the classical side-information increases for the cases with a higher number of inputs.

Alternative forms of input configurations with more WCSs can also be considered. Paying attention to the 4-input case as an example, as shown in Fig. 1, instead of using the typical input configurations (set I, II, and III), one can implement subsets I and II, which require a ternary and binary initial seed rather than quartet one, downsizing the computational complexity, see Fig. 2. In Fig. (6), the conditional min-entropy is plotted as a function of states' overlap for subsets I and II. The dashed curve is the expected theoretical results obtained for our experimental parameters which is in acceptable agreement with the experimental data taken from SNSPD with 83% detection efficiency and for various mean photon numbers.

The maximum conditional min-entropy for subsets I and II is 0.759 and 0.546, respectively, which are remarkably higher compared to typical binary and ternary input configurations at ∼ 0.2 and ∼ 0.25 obtained with detectors with 80% and higher than 90% detection efficiencies, respectively [25, 26]. It should be noted that this higher rate entropy is achievable without the need of adjusting the optical setup and can be done in the signal preparation and post-processing stage. Furthermore, the randomness generation rate scaled from 0.11 and 0.083 to 0.1897 and 0.136 which is a considerable improvement achieved only by redefining the transmitted states.

V. CONCLUSION

In conclusion, we demonstrated a semi-DI QRNG based on the prepare-and-measure scenario exploiting a time-bin encoding scheme and single-photon detection technique investigating multiple input-output cases. Furthermore, the protocol is experimentally implemented using commercial-off-the-shelf components in a simple all-in-fibre optical setup at telecom wavelength, allowing a straightforward tunable input

configuration needless of an optical switch. We show that by holding the number of inputs(outcomes) fixed (minimal), known as the many-outcome (many-inputs) approach, one can increase the system entropy while keeping the computational complexity low. Additionally, a comprehensive study of time-bin encoding semi-DI QNRG is presented where, depending on the needs, one can select appropriate time-bin settings.

Besides, we compared this protocol's results with binary and ternary-input systems and showed that our protocol is capable of generating more randomness with the same optical setup. The proposed protocol features advanced security since it only demands bounding the prepared states' overlap; the rest of the setup is not required to be characterized and can be classically correlated with the adversary. Alternatively, this protocol can be implemented in a different wavelength where single photon avalanche diodes (SPADs) have better detection efficiency, thus making this proposal chip-integrable. In a nutshell, the semi-DI protocols' main advantage is to ease up the implementation complexity and enhance the generation rate preserving a high level of security. This paper demonstrates a semi-DI QRNG based on the overlap bound with an easy-to-implement experimental setup which can produce random numbers at a high rate with robust security applicable for various input-output configurations.

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] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits, npj Quantum Information 3, 25 (2017).

[2] 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, Nanophotonics doi:10.1515/nanoph-2021-0500 (2021).

[3] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature 540, 213 (2016).

[4] V. Mannalath, S. Mishra, and A. Pathak, A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness (2022).

[5] E. Almaraz Luengo, M. Leiva Cerna, L. J. García Villalba, D. Hurley-Smith, and J. Hernandez-Castro, Sensitivity and uniformity in statistical randomness tests, Journal of Information Security and Applications 70, 103322 (2022).

[6] M. Stipcevic, Quantum random number generators and their applications in cryptography, in Advanced Photon Counting Techniques VI, Vol. 8375, edited by M. A. Itzler, International Society for Optics and Photonics (SPIE, 2012) pp. 20 – 34.

[7] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Reviews of Modern Physics 89, 15004 (2017).

[8] M. Zahidy, H. Tebyanian, D. Cozzolino, Y. Liu, Y. Ding, T. Morioka, L. K. Oxenløwe, and D. Bacco, Quantum randomness generation via orbital angular momentum modes crosstalk in a ring-core fiber, AVS Quantum Science 4, 011402 (2022), https://doi.org/10.1116/5.0074253.

[9] G. Gras, A. Martin, J. W. Choi, and F. Bussières, Quantum entropy model of an integrated quantum-random-number-generator chip, Phys. Rev. Applied 15, 054048 (2021).

[10] 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 104, 261112 (2014), https://doi.org/10.1063/1.4886761.

[11] L. Huang, H. Zhou, K. Feng, and C. Xie, Quantum random number cloud platform, npj Quantum Information 7, 107 (2021).

[12] P. J. Brown, S. Ragy, and R. Colbeck, A framework for quantum-secure device-independent randomness expansion, IEEE Transactions on Information Theory 66, 2964 (2020).

[13] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation (2011), arXiv:0911.3814 [quant-ph].

[14] R. Colbeck and A. Kent, Private randomness expansion with untrusted devices, Journal of Physics A: Mathematical and Theoretical 44, 095305 (2011).

[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 103, 062206 (2021).

[16] R. Bhavsar, S. Ragy, and R. Colbeck, Improved device-independent randomness expansion rates from tight bounds on the two sided randomness using chsh tests (2021).

[17] M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, Y. Liu, Q. Zhao, Y. Peng, J. Zhang, Y. Zhang, W. J. Munro, X. Ma, Q. Zhang, J. Fan, and J.-W. Pan, Experimental realization of device-independent quantum randomness expansion, Phys. Rev. Lett. 126, 050503 (2021).

[18] L.-L. Sun, X. Zhang, X. Zhou, Z.-D. Li, X. Ma, J. Fan, and S. Yu, Certifying randomness in quantum state collapse (2022).

[19] C. L. Jones, S. L. Ludescher, A. Aloy, and M. P. Mueller, Theory-independent randomness generation with spacetime symmetries (2022).

[20] C. Wang, I. W. Primaatmaja, H. J. Ng, J. Y. Haw, R. Ho, J. Zhang, G. Zhang, and C. Lim, Provably-secure quantum randomness expansion with uncharacterised homodyne detection, Nature Communications 14, 316 (2023).

[21] D. Drahi, N. Walk, M. J. Hoban, A. K. Fedorov, R. Shakhovoy, A. Feimov, Y. Kurochkin, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, Certified quantum random numbers from untrusted light, Phys. Rev. X 10, 041048 (2020).

[22] H. Dai, B. Chen, X. Zhang, and X. Ma, Intrinsic randomness under general quantum measurements (2022).

[23] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Unbounded randomness from uncharacterized sources, Communications Physics 5, 273 (2022).

[24] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Experimental measurement-device-independent quantum random-number generation, Phys. Rev. A 94, 060301 (2016).

[25] 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 6, 045026 (2021).

[26] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, Physical Review Applied 7, 054018 (2017).

[27] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quantum Information 2, 16021 (2016).

[28] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum 1, 33 (2017).

[29] H. Tebyanian, Randomness generation with untrusted devices, in 2022 Workshop on Recent Advances in Photonics (WRAP) (2022) pp. 1–2.

[30] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Semi-device-independent heterodyne-based quantum random-number generator, Phys. Rev. Applied 15, 034034 (2021).

[31] S. M. Barnett and S. Croke, Quantum state discrimination, Adv. Opt. Photon. 1, 238 (2009).

[32] S. Johnson, A new upper bound for error-correcting codes, IRE Transactions on Information Theory 8, 203 (1962).

[33] E. Agrell, A. Vardy, and K. Zeger, Upper bounds for constant-weight codes, Information Theory, IEEE Transactions on 46, 2373 (2000).

[34] A. Schrijver, New code upper bounds from the terwilliger algebra and semidefinite programming, Information Theory, IEEE Transactions on 51, 2859 (2005).

[35] A. Brouwer, J. Shearer, N. Sloane, and W. Smith, A new table of constant weight codes, IEEE Transactions on Information

Theory **36**, 1334 (1990).

[36] R. Montemanni and D. Smith, Heuristic algorithms for constructing binary constant weight codes, Information Theory, IEEE Transactions on **55**, 4651 (2009).

[37] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover Hashing Against Quantum Side Information, IEEE Trans-

actions on Information Theory **57**, 5524 (2011).

[38] J.-D. Bancal, L. Sheridan, and V. Scarani, More randomness from the same data, New Journal of Physics **16**, 033011 (2014).

[39] H. Tebyanian, M. Avesani, G. Vallone, and P. Villoresi, Semi-device-independent randomness from d-outcome continuous-variable detection, Phys. Rev. A **104**, 062424 (2021).