Tebyanian et al. *EPJ Quantum Technology* (2024) 11:15
https://doi.org/10.1140/epjqt/s40507-024-00227-z

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

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]

*Correspondence:
hamid.tebyanian@york.ac.uk
[1]Department of Mathematics, University of York, Heslington, York, YO10 5DD, United Kingdom
Full list of author information is available at the end of the article

Abstract

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.

1 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

Springer

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 applications.

2 Methods

2.1 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].

2.1.1 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 $|\psi_i\rangle$,

$$|\psi_i\rangle = |0\rangle^{n-m}|\alpha\rangle^{\otimes m} = |0\rangle \otimes |\alpha\rangle \otimes \cdots \otimes |\alpha\rangle \otimes |0\rangle, \tag{1}$$

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:

$$\left| \langle\psi_i| \, |\psi_j\rangle \right| \geq \delta, \quad \forall i \neq j, \tag{2}$$

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. Figure 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

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

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

$$\begin{aligned} |\langle\psi_i| \, |\psi_j\rangle| &= \langle 0|0\rangle^{n-2m+s} \langle 0|\alpha\rangle^{2(m-s)} \langle\alpha|\alpha\rangle^s \\ &= \langle 0|\alpha\rangle^{2(m-s)}, \end{aligned} \tag{3}$$

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 $\mathcal{B}(n, m, s)$ the maximum number of states in any subset $\mathcal{S}$ of the (n, m)-configuration such that all elements in $\mathcal{S}$ have the same value of s pairwise, with s defined as in Eq. (3). It is of relevance to know $\mathcal{B}$ for any configuration as it defines the number of inputs and

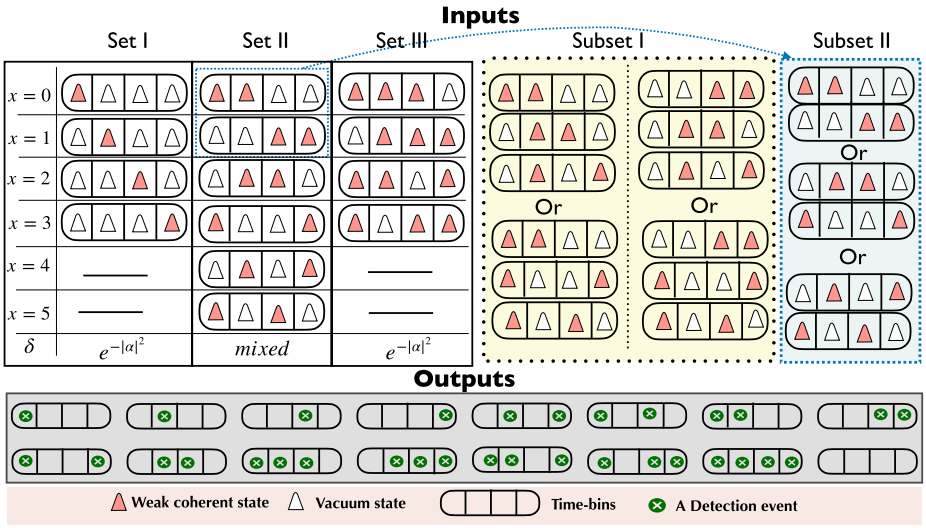

Figure 1 Possible input-output configurations with four time-bin case. Inputs: Sets I, II, and III show input configurations where one, two, and three weak coherent states are positioned in time-bins, respectively. Subsets I and II are subsections of set II where the overlap is mixed. Outputs: 16 possible 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

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 $\mathcal{S}$ 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 $d = 2(m - s)$. Equation (3) can then be written as $|\langle\psi_i||\psi_j\rangle| = \langle 0|\alpha\rangle^d$. In the context of constant weight binary codes, there exists the well-known but open question of determining the maximum number of codewords $\mathcal{A}(n, m, d_{\min})$, where $d_{\min}$ refers to the minimum distance of the code. $\mathcal{B}(n, m, s)$ can be upper-bounded by $\mathcal{A}(n, m, 2(m-s))$ which in turn can be upper-bounded by different theoretical bounds [32–34]. Lower bounds to $\mathcal{A}$, typically by explicit construction [35, 36], cannot be applied to $\mathcal{B}$ as the codes can contain state-pairs with $d > d_{\min}$ which translates to a violation of Eq. (2) since $\delta = \langle 0|\alpha\rangle^d$. 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.

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

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. $\mathcal{B}$ can therefore be lower-bounded by

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

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

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

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. Figure 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.

2.1.2 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]

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

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:

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

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:

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

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. Equation (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 Fig. 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. Figure 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 after-pulsing. 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.

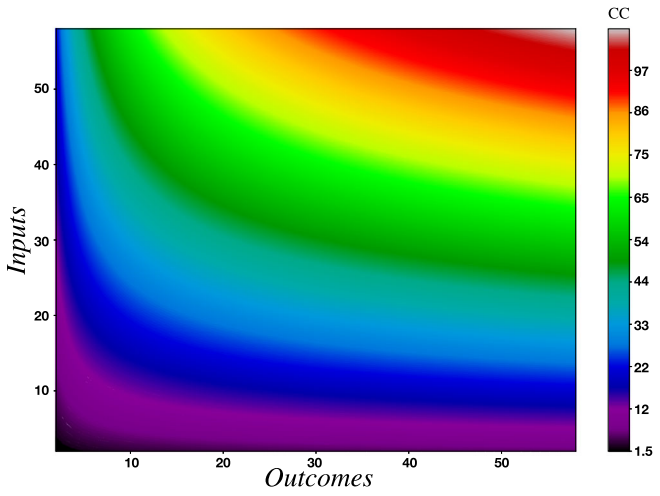

Figure 2 Computational cost (CC), colour bar, as a function of the number of inputs and outputs. Note that the CC is plotted on a logarithmic scale, expressing that CC increases exponentially with the number of IO

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

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

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 1-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;

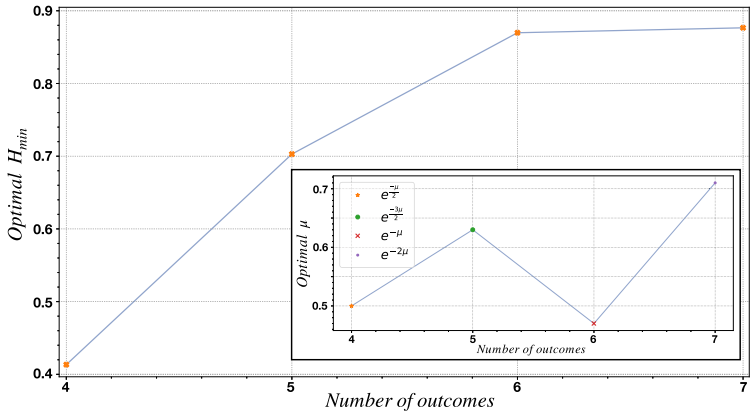

Figure 3 Optimal conditional min-entropy as a function of the number of outcomes with binary input. *Inset:* Optimal mean-photon number (μ), i.e., the μ which delivers the maximum entropy, as a function of the number of outcomes for states with different overlaps

Table 1 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	$\varsigma = e^{-\mu}$
$\|\alpha\rangle\|0\rangle\|0\rangle$ $\|\alpha\rangle\|\alpha\rangle\|0\rangle$	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 – – – –

the inset of Fig. 3 shows the optimal mean-photon number as a function of outcomes for different overlaps. Similarly, a many-input case can be introduced while keeping the outcome minimal. Table 1-bottom shows examples of the possible setting of the many-input approach.

2.1.3 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:

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

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:

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

where $P_\alpha^T(1)$ is the probability of registering a detection when sending $|\alpha\rangle$, η_{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

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

where $P_\alpha(1), P_\varnothing(1)$, ($P_\alpha(0), P_\varnothing(0)$) represent the probability of registering a click (no-click) 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.

2.1.4 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,

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

where $H_{\min}(n_{m,s}, \upsilon, \eta_{\text{det}}, \mu_{\text{optimal}})$ is the maximum extractable entropy from that set considering optimal μ, all the sources of noise, and detector efficiency. As discussed in Sect. 2.1.2, 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.

2.2 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.

Figure 4 shows a schematic representation of the setup. The n-time-bin state is generated by carving a 1550 nm continuous 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

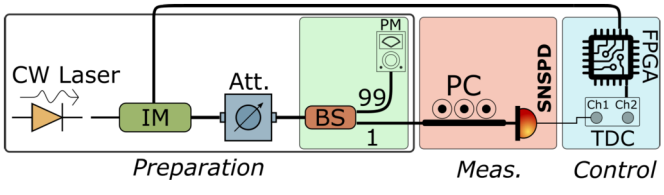

Figure 4 Schematic of the QRNG setup. A continuous wave laser (CW) is carved to form a train of pulses according to the protocol selected by the user. A combination of an attenuator (att.) and a 99:1 beamsplitter bring the power to single photon level where the 99% output is monitored constantly with 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)

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 Hz 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.

3 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, leading to a different input-output correlation and entropy. As shown in Fig. 5, 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.

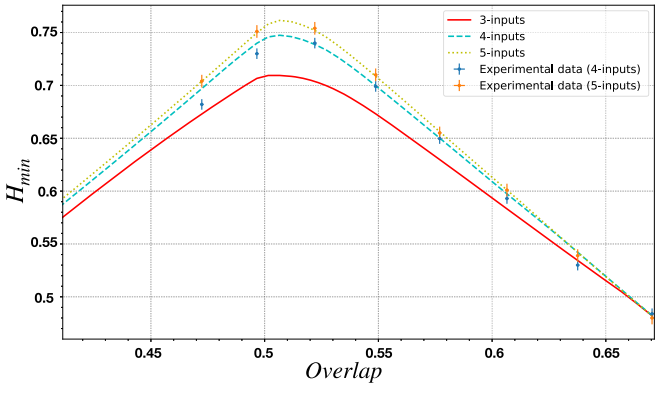

Figure 5 Conditional min-entropy as a function of states' total overlap. The solid, dashed, and dotted curves represent the theoretical predictions for 3, 4, and 5 input configurations, respectively. At the same time, the blue and orange dots show the experimental data for 4 and 5 input cases measured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

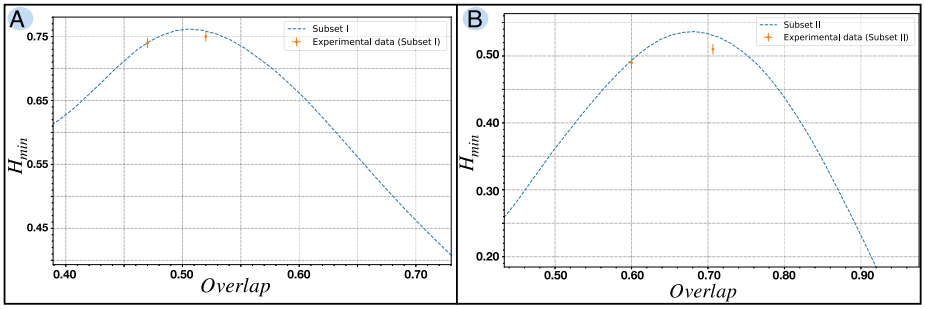

Figure 6 Conditional min-entropy as a function of states' total overlap for Subsets I (A) and II (B) represented in Fig. 1. In both figures, the dashed line shows the theoretical predictions, and the orange dots represent the experimental data

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.

Our research introduces significant improvements in QRNG, particularly in terms of noise analysis, adaptability, and security:

- We provide a detailed noise assessment, improving the system's real-world applicability by accounting for practical operational challenges. This comprehensive approach sets our work apart from existing studies that may overlook these critical factors.
- Our protocol features adjustable input-output configurations, offering a more flexible and scalable solution compared to previous models. This adaptability is crucial for keeping pace with technological advancements in quantum systems.
- We enhance the security measures within our QRNG model without compromising efficiency. This balance is achieved through systematic theoretical analysis, ensuring our system is not only more secure but also remains practical for broader application scenarios.
- The potential for chip integration demonstrates our protocol's readiness for future technological developments.

Overall, our work marks a substantial advancement in QRNG by addressing several fundamental limitations in existing models while maintaining practicality for users by emphasizing versatility and enhanced security. It extends beyond traditional binary or ternary systems, utilizing a time-bin encoding approach that integrates often-neglected noise factors like afterpulsing probability. This consideration not only bolsters the security but also adapts to various input-output configurations. While our current setup prioritizes theoretical validation over maximizing the generation rate, achieving the rate of about 9.01 Mbits/s, the rate can be improved using higher rate components.

Recognizing that finite data sizes in experimental setups might introduce security issues, our analysis accounts for these finite-size effects. It is critical to incorporate these consid-

erations to accurately calculate the conditional min-entropy, particularly in scenarios with limited data availability. Appendix A presents our approach to this challenge, outlining the mathematical adjustments made to the SDP objective function and their direct impact on min-entropy estimations under finite-size conditions.

In prepare-and-measure schemes, one plausible adversarial strategy is for Eve to fake measurement outcomes independent of the actual inputs. This type of attack could compromise the randomness of the output. Appendix B delves into this specific scenario, studying its impact on our system, assessing that the protocol can detect and mitigate such attacks, and ensuring the reliability and security of the generated randomness.

4 Randomness test

The initial outcomes from our QRNG, characterized by low min-entropy, are refined through a Toeplitz hash function designed for randomness extraction [40]. This transformation enhances the quality of the raw data into high-grade random numbers [41]. Figure 7 displays the results of subjecting these enhanced numbers to the NIST Statistical Test Suite [42], with p-values for each test depicted. The suite's tests comprehensively assess the statistical randomness, and as indicated, all p-values surpass the significance level, affirming that the randomness criteria are met. Note, however, that while the NIST suite's clearance is a fundamental requirement, it does not solely confirm the quantum nature of the random numbers. Thus, the successful passage of these tests should be seen as meeting a basic standard for any QRNG rather than as proof of inherent quantum randomness.

5 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

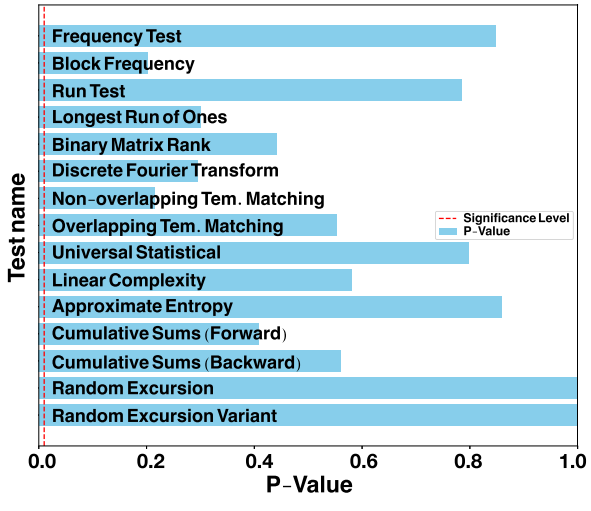

Figure 7 The plot shows p-values from NIST statistical tests for the randomness of output from our QRNG. Each test's p-value exceeds the significance threshold, indicating successful passage. The significance level, shown by the dashed red line conventionally set at 0.01 for NIST tests, represents the probability of rejecting a true null hypothesis. In this context, our data is doubtful to have occurred by chance, thus confirming its statistical randomness

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.

Appendix A: Finite-size effects

In this appendix, we describe the calculation of the conditional min-entropy that systematically accounts for the impacts of finite experimental data sizes. This enhanced approach is essential in evaluating the security and reliability of the generated sequences, ensuring a more robust and scientifically rigorous assessment.

The optimization process in guessing probability Eq. (8) is convex and can be numerically solved by transforming it into a semidefinite programming (SDP) version. The duality is held for this optimization problem, indicating both primal and dual forms exist. The primal form of an SDP directly addresses the original optimization problem, aiming to maximize the objective function under certain constraints. In contrast, the dual form derived from the primal simplifies the problem by providing bounds on the primal objective value. The dual form is preferred for its ability to provide an upper bound on the guessing probability, as opposed to the lower bound offered by the primal form. The dual form then can be written as

$$P_g = \min_{H^{\Lambda}, v_{bx}} \left[-\sum_{x=0}^{n-1} \sum_{b=0}^{d-1} v_{bx} p(b|x) \right] \tag{A.1}$$

where scalar coefficient v_{bx} is the Lagrange multipliers for each primal problem constraint. We refer to Refs [25, 26, 39] for a detailed mathematical derivation for primal and dual calculation. Using the dual form ensures conservative estimates that crucially do not overestimate the min-entropy, thereby safeguarding the integrity of QRNG. Additionally, it offers the flexibility of recalculating bounds without requiring exhaustive optimization in each iteration, thereby streamlining real-time operations and optimizing the resources needed for entropy estimation.

We start by considering quantum measurement outcomes as independent Bernoulli random variables, $X_1, X_2, \ldots, X_n$, with the aggregate outcome given by their sum:

$$S_n = \sum_{i=1}^{n} X_i \tag{A.2}$$

The summation S_n represents the total count of a particular outcome across all measurements, offering a cumulative perspective of the quantum measurement results. This aggregate outcome necessitates the computation of its mean and variance, essential statistical measures that contribute to the QRNG's assessment:

$$\mu_n = E[S_n], \qquad \sigma_n^2 = \mathrm{Var}(S_n) \tag{A.3}$$

A lower bound on the mean, considering error tolerance ε, reads:

$$\mu_{\mathrm{L}} = \mu_n - \sqrt{\frac{\sigma_n^2}{2} \ln\left(\frac{1}{\varepsilon}\right)} \tag{A.4}$$

The confidence interval surrounding the mean, $CI(S_n)$ is then given by:

$$CI(S_n) = [\mu_n - \delta, \mu_n + \delta] \tag{A.5}$$

with δ as the margin of estimation error.

This model presents a robust foundation for evaluating the impact of finite-size effects on the security and reliability of the system. For the estimation of conditional probabilities $\tilde{p}(b|x) = \frac{n_{b,x}}{n_x}$ and their confidence interval is determined by the security parameter ϵ:

$$CI\big(\tilde{p}(b|x)\big) = \left[\tilde{p}(b|x) - \sqrt{\frac{-\ln(\epsilon)}{2n_x}}, \tilde{p}(b|x) + \sqrt{\frac{-\ln(\epsilon)}{2n_x}}\right]. \tag{A.6}$$

The introduction of finite-size effects into this formulation is achieved through adjustments to the dual SDP objective function:

$$P_g \geq \min\left[-\sum_{x=0}^{n-1}\sum_{b=0}^{d-1}\big(\nu_{bx}\tilde{p}(b|x) + |\nu_{bx}|\Delta(\epsilon, n)\big)\right] \tag{A.7}$$

with $\Delta(\epsilon, n)$ encapsulating the finite-size correction. Although not providing an exact bound, Eq. (A.7) addresses the extreme scenarios encountered in single-shot measurements. This approach ensures the equation's relevance and effectiveness in finite-size regimes, making it a versatile tool in quantum computation analysis.

Moreover, the concept of smooth conditional min-entropy extends over multiple rounds, indexed as n, and is intricately related to the conditional min-entropy computed for an individual round. This intricate relationship is presented in the [43, 44], where it is expressed as:

$$H_{\min}^{\epsilon}\big(\rho_{XE}^{\otimes n}|E^n\big) \geq nH_{\min}^{\epsilon/n}(\rho_{XE}|E) \geq nH_{\min}(\rho_{XE}|E), \tag{A.8}$$

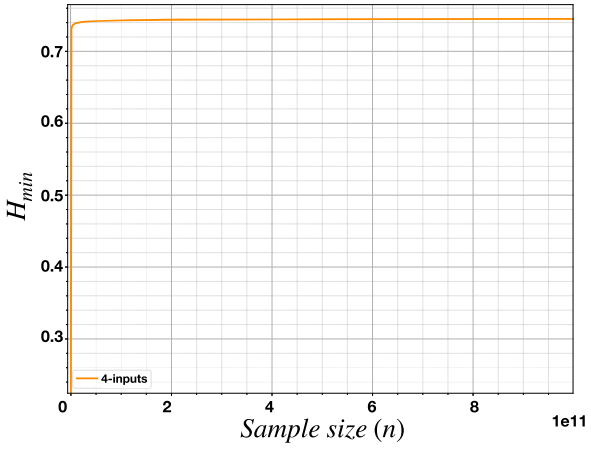

Figure 8 Conditional min-entropy as a function of sample size is presented for a system with 83% detection efficiency, along with a security parameter, $\epsilon = 10^{-9}$ for the 4-inputs case, see Fig. 5

where ρ_{XE} is the classical-quantum state, encapsulating the classical random variable X and its quantum counterpart ρ_E^x, which is associated with an adversary. Given that the bound applies to a wide range of quantum-side information scenarios, it naturally extends to our specific situation where we deal only with classical side information.

Figure 8 illustrates the entropy variation as a function of the experimental data size, specifically for a system operating at 83% efficiency with an epsilon value of 1×10^{-9}. This graph effectively demonstrates that, beyond a certain sample size threshold, the impact of finite size effects becomes negligible. In our experimental setup, this threshold is identified at a minimum sample size of 5×10^{11}, maintaining a security parameter of $\epsilon = 10^{-9}$, which assures the accurate probability estimation and subsequent entropy computation.

Appendix B: Fake data attack

A vital element of our semi-DI QRNG framework is the implementation of an overlap bound. The overlap directly influences the security of the randomness generation process, as it dictates the degree of uncertainty that an adversary faces in predicting the outcomes of quantum measurements. To better illustrate the fact see Fig. 9 (A). Consider measuring a set of quantum states (i.e., coherent states in phase-space representation for better visualization of the point) with high overlap and obtaining the measurement outcome in the intersection area (shown by the cross). It is impossible to know whether the blue or red circle was the transmitted state for the depicted measurement result.

The preparation and measurement devices may be classically correlated, but they are not permitted to share quantum entanglement.

A potential security threat in the randomness generation process involves an adversary, Eve, who might attempt to compromise the system by simulating the conditional probability distributions, $P(b|x)$. This strategy involves Eve deliberately altering the outcomes in a way that falsely appears to result from genuine quantum processes. In this scenario, Eve would alter the outputs to resemble those produced by quantum randomness, posing a challenge to the authenticity of the randomness generation.

The security estimation is designed to assess and validate the randomness of the outcomes based on the observed correlations between the preparation inputs and measure-

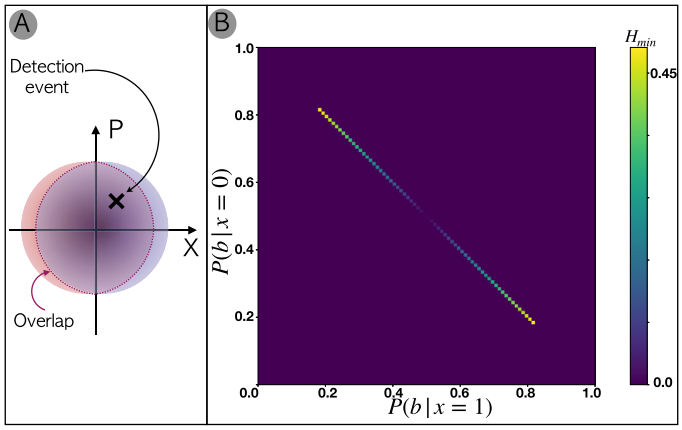

Figure 9 A) Illustration of binary quantum states with significant overlap, exemplified here by coherent states in phase space. Depending on the input x, either the red or blue state is transmitted. Due to their high overlap, measurements in the intersecting area yield uncertain information about the source, making it impossible for measurement strategies to perfectly distinguish between these states. B) The plot displays potential conditional probabilities with min-entropy values depicted through a colour scale. It demonstrates that any correlation not meeting the set assumptions results in a min-entropy value of zero, indicating zero extractable randomness

ment outcomes, given the states' overlap. When an adversary attempts to simulate or replicate the probability distributions, the protocol's security estimation mechanism discerns between authentic quantum randomness and fabricated outcomes by returning zero entropy for the invalid data set.

The optimization process for computing min-entropy involves the conditional probabilities $P(b|x)$ and the overlap parameter into an SDP solver. This numerical optimizer then searches over all feasible preparation and measurement strategies permitted by the overlap bound. For each strategy, it calculates the corresponding guessing probability – the probability that an adversary could correctly guess the measurement outcome. The negative logarithm of the optimized guessing probability then gives the min-entropy. Deriving an analytical solution for the min-entropy is highly complex due to the optimization across a large strategy space. The SDP solver approach provides an efficient numerical method that rigorously bounds the maximal guessing probability achievable within the physical limits imposed. The computed min-entropy represents a certified lower bound on the extractable randomness in our semi-DI framework by minimizing this guessing probability over all allowable quantum strategies respecting the overlap assumption. Figure 9 (B) represents the protocol's capabilities, mapping the min-entropy against various conditional probabilities $P(b|x)$. The x-axis represents $P(b|x = 0)$ and the y-axis $P(b|x = 1)$, with the min-entropy values depicted through an intuitive colour-coding scheme.

A pivotal observation from this plot is the predominance of zero entropy across a significant portion of the probability distribution space, with non-zero entropy confined to a narrowly defined region. This distinct pattern is a direct consequence of the specific overlap bound which is also established in our protocol.

The narrow range of conditions that produce non-zero min-entropy is an effective filter against adversarial tampering. It sharply distinguishes authentic quantum randomness from fabricated or intercepted data. For an adversary, mimicking the specific $P(b|x)$ conditions that yield valid quantum randomness is a significant challenge. Our semi-DI QRNG

protocol, designed with a specific overlap bound and thorough security checks, effectively counters attempts to simulate quantum randomness.

Acknowledgements
This work is supported by the Center of Excellence SPOC (ref DNRF123), Innovations fonden project FireQ (No. 9090-00031B), and EraNET Cofund Initiatives QuantERA within the European Union's Horizon 2020 research and innovation program grant agreement No. 731473 (project SQUARE). H. T. acknowledges the Innovate UK Industrial Strategy Challenge Fund (ISCF), project 106374-49229 AQuRand (Assurance of Quantum Random Number Generators).

Funding
Not applicable.

Abbreviations
RNG, random number generator; QRNG, quantum random number generator; QKD, quantum key distribution; DD, device-dependent; DI, device-independent; SDP, semi-definite programming; WCS, weak coherent state; VS, vacuum states; CC, computational cost; IO, input-output; CV, continuous variable; DCR, dark count rate; SPAD, single-photon avalanche diode; SNSPD, superconducting nanowire single photon detector; TDC, time-to-digital converter; FPGA, field-programmable gate array; CW, continuous wave; PM, power meter; PC, polarization controller.

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

Declarations

Competing interests
The authors declare no competing interests.

Author contributions
H.T. and M. Z. conceived the idea. M. Z. performed the experiment. H. T., M. Z., and R. M. analyzed the data and the model. D. B. and S. F. supervised the project. All the authors contributed to the manuscript.

Author details
[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.

Received: 30 May 2023 Accepted: 26 February 2024 Published online: 05 March 2024

References

1. Ding Y, Bacco D, Dalgaard K, Cai X, Zhou X, Rottwitt K, Oxenløwe LK. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. npj Quantum Information. 2017;3:25.
2. Zahidy M, Liu Y, Cozzolino D, Ding Y, Morioka T, Oxenløwe LK, Bacco D. Photonic integrated chip enabling orbital angular momentum multiplexing for quantum communication. Nanophotonics. 2021. https://doi.org/10.1515/nanoph-2021-0500.
3. Acín A, Masanes L. Certified randomness in quantum physics. Nature. 2016;540:213.
4. Mannalath V, Mishra S, Pathak A. A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness. 2022.
5. Almaraz Luengo E, Leiva Cerna M, García Villalba LJ, Hurley-Smith D, Hernandez-Castro J. Sensitivity and uniformity in statistical randomness tests. Journal of Information Security and Applications. 2022;70:103322.
6. Stipcevic M. Quantum random number generators and their applications in cryptography. Itzler MA, editor. Advanced Photon Counting Techniques VI. International Society for Optics and Photonics (SPIE, 2012) vol. 8375. p. 20–34.
7. Herrero-Collantes M, Garcia-Escartin JC. Quantum random number generators. Rev Mod Phys. 2017;89:15004.
8. Zahidy M, Tebyanian H, Cozzolino D, Liu Y, Ding Y, Morioka T, Oxenløwe LK, Bacco D. Quantum randomness generation via orbital angular momentum modes crosstalk in a ring-core fiber. AVS Quantum Sci. 2022;4:011402. https://doi.org/10.1116/5.0074253.
9. Gras G, Martin A, Choi JW, Bussières F. Quantum entropy model of an integrated quantum-random-number-generator chip. Phys Rev Appl. 2021;15:054048.
10. Yuan ZL, Lucamarini M, Dynes JF, Fröhlich B, Plews A, Shields AJ. Robust random number generation using steady-state emission of gain-switched laser diodes. Appl Phys Lett. 2014;104:261112. https://doi.org/10.1063/1.4886761.
11. Huang L, Zhou H, Feng K, Xie C. Quantum random number cloud platform. npj Quantum Inf. 2021;7:107.
12. Brown PJ, Ragy S, Colbeck R. A framework for quantum-secure device-independent randomness expansion. IEEE Trans Inf Theory. 2020;66:2964.
13. Colbeck R. Quantum and relativistic protocols for secure multi-party computation. 2011. arXiv:0911.3814 [quant-ph].
14. Colbeck R, Kent A. Private randomness expansion with untrusted devices. J Phys A, Math Theor. 2011;44:095305.
15. Foletto G, Padovan M, Avesani M, Tebyanian H, Villoresi P, Vallone G. Experimental test of sequential weak measurements for certified quantum randomness extraction. Phys Rev A. 2021;103:062206.
16. Bhavsar R, Ragy S, Colbeck R. Improved device-independent randomness expansion rates from tight bounds on the two sided randomness using chsh tests. 2021.

17. Li M-H, Zhang X, Liu W-Z, Zhao S-R, Bai B, Liu Y, Zhao Q, Peng Y, Zhang J, Zhang Y, Munro WJ, Ma X, Zhang Q, Fan J, Pan J-W. Experimental realization of device-independent quantum randomness expansion. Phys Rev Lett. 2021;126:050503.
18. Sun L-L, Zhang X, Zhou X, Li Z-D, Ma X, Fan J, Yu S. 2022. Certifying randomness in quantum state collapse.
19. Jones CL, Ludescher SL, Aloy A, Mueller MP. Theory-independent randomness generation with spacetime symmetries. 2022.
20. Wang C, Primaatmaja IW, Ng HJ, Haw JY, Ho R, Zhang J, Zhang G, Lim C. Provably-secure quantum randomness expansion with uncharacterised homodyne detection. Nat Commun. 2023;14:316.
21. Drahi D, Walk N, Hoban MJ, Fedorov AK, Shakhovoy R, Feimov A, Kurochkin Y, Kolthammer WS, Nunn J, Barrett J, Walmsley IA. Certified quantum random numbers from untrusted light. Phys Rev X. 2020;10:041048.
22. Dai H, Chen B, Zhang X, Ma X. Intrinsic randomness under general quantum measurements. 2022.
23. Avesani M, Tebyanian H, Villoresi P, Vallone G. Unbounded randomness from uncharacterized sources. Commun Phys. 2022;5:273.
24. Nie Y-Q, Guan J-Y, Zhou H, Zhang Q, Ma X, Zhang J, Pan J-W. Experimental measurement-device-independent quantum random-number generation. Phys Rev A. 2016;94:060301.
25. Tebyanian H, Zahidy M, Avesani M, Stanco A, Villoresi P, Vallone G. Semi-device independent randomness generation based on quantum state's indistinguishability. Quantum Sci Technol. 2021;6:045026.
26. Brask JB, Martin A, Esposito W, Houlmann R, Bowles J, Zbinden H, Brunner N. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. Phys Rev Appl. 2017;7:054018.
27. Ma X, Yuan X, Cao Z, Qi B, Zhang Z. Quantum random number generation. npj Quantum Inf. 2016;2:16021.
28. Van Himbeeck T, Woodhead E, Cerf NJ, García-Patrón R, Pironio S. Semi-device-independent framework based on natural physical assumptions. Quantum. 2017;1:33.
29. Tebyanian H. Randomness generation with untrusted devices. In: 2022 Workshop on Recent Advances in Photonics (WRAP). 2022. p. 1–2.
30. Avesani M, Tebyanian H, Villoresi P, Vallone G. Semi-device-independent heterodyne-based quantum random-number generator. Phys Rev Appl. 2021;15:034034.
31. Barnett SM, Croke S. Quantum state discrimination. Adv Opt Photonics. 2009;1:238.
32. Johnson S. A new upper bound for error-correcting codes. IRE Trans Inf Theory. 1962;8:203.
33. Agrell E, Vardy A, Zeger K. Upper bounds for constant-weight codes. IEEE Trans Inf Theory. 2000;46:2373.
34. Schrijver A. New code upper bounds from the terwilliger algebra and semidefinite programming. IEEE Trans Inf Theory. 2005;51:2859.
35. Brouwer A, Shearer J, Sloane N, Smith W. A new table of constant weight codes. IEEE Trans Inf Theory. 1990;36:1334.
36. Montemanni R, Smith D. Heuristic algorithms for constructing binary constant weight codes. IEEE Trans Inf Theory. 2009;55:4651.
37. Tomamichel M, Schaffner C, Smith A, Renner R. Leftover hashing against quantum side information. IEEE Trans Inf Theory. 2011;57:5524.
38. Bancal J-D, Sheridan L, Scarani V. More randomness from the same data. New J Phys. 2014;16:033011.
39. Tebyanian H, Avesani M, Vallone G, Villoresi P. Semi-device-independent randomness from **d**-outcome continuous-variable detection. Phys Rev A. 2021;104:062424.
40. Krawczyk H. Lfsr-based hashing and authentication. In: Advances in cryptology—CRYPTO'94. Berlin: Springer; 1994. p. 129–39.
41. Frauchiger D, Renner R, Troyer M. True randomness from realistic quantum devices. 2013. arXiv:1311.4547 [quant-ph].
42. Lawrence EB III et al. SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology; 2010.
43. Renner R. Security of quantum key destribution. Int J Quantum Inf. 2008;6:1.
44. Curty M, Xu F, Cui W, Lim CCW, Tamaki K, Lo HK. Finite-key analysis for measurement-device-independent quantum key distribution. Nat Commun. 2014;5:1. arXiv:1307.1081.

Publisher's Note