---

**Article:**
Tebyanian, Hamid, Zahidy, Mujtaba, Avesani, Marco et al. (2021) Practical Semi-Device Independent Randomness Generation Based on Quantum State's Indistinguishability. Quantum Sci. Technol.. ISSN: 2058-9565

https://doi.org/10.1088/2058-9565/ac2047

---

# Practical Semi-Device Independent Randomness Generation Based on Quantum State's Indistinguishability

Hamid Tebyanian,[1,*] Mujtaba Zahidy,[1,*] Marco Avesani,[1] Andrea Stanco,[1] Paolo Villoresi,[1,2,3] and Giuseppe Vallone[1,2,4]

[1]*Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*
[2]*Padua Quantum Technologies Research Center, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*
[3]*Istituto di Fotonica e Nanotecnologie, CNR, via Trasea 7, IT-35131 Padova, Italy*
[4]*Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, IT-35131 Padova, Italy*

Semi-device independent (Semi-DI) quantum random number generators (QRNG) gained attention for security applications, offering an excellent trade-off between security and generation rate. This paper presents a proof-of-principle time-bin encoding semi-DI QRNG experiments based on a prepare-and-measure scheme. The protocol requires two simple assumptions and a measurable condition: an upper-bound on the prepared pulses' energy. We lower-bound the conditional min-entropy from the energy-bound and the input-output correlation, determining the amount of genuine randomness that can be certified. Moreover, we present a generalized optimization problem for bounding the min-entropy in the case of multiple input and outcomes, in the form of a semidefinite program (SDP). The protocol is tested with a simple experimental setup, capable of realizing two configurations for the ternary time-bin encoding scheme. The experimental setup is easy-to-implement and comprises commercially available off-the-shelf (COTS) components at the telecom wavelength, granting a secure and certifiable entropy source. The combination of ease-of-implementation, scalability, high security level and output-entropy, make our system a promising candidate for commercial QRNGs.

## I. INTRODUCTION

The world of cybersecurity is developing exceedingly fast, and the data encrypted by the traditional encryption methods are facing the danger of being revealed. Producing unpredictable and certified random numbers is a critical part of every cryptographic operation. There are many simple techniques to generate random numbers that rely on a deterministic phenomenon, however, these generators' security cannot be guaranteed since, in principle, they can always be predicted. On the contrary, quantum mechanics provides randomness based on its intrinsic behavior, which theoretically is an unpredictable source of secure random numbers [1, 2].

The most common approach to generate random numbers through a quantum process is by trusting the experiment's apparatus: these protocols are called trusted-device QRNGs. Trusted-device QRNGs are cheap, high-rate, and easy-to-implement [3, 4], although the random numbers' security and privacy could be threatened [5, 6]. In fact, the behaviour of the trusted devices could deviate from the model and classical or quantum side-information could be leaked to the adversary's system, compromising the privacy of the numbers. Therefore, trust in the generator's devices can compromise the security of the system. The highest level of security is offered by an approach called device-independent (DI) [7, 8]. Considering there is no hypothesis on the devices' internal-working regularity, it is highly protected. However, this protocol's drawbacks are the low generation-rate and experimental complexity, making it less practical [9–13].

By introducing few assumptions on the working principles of the devices, it is possible to reduce the experimental complexity while increasing the generation rate; these protocols are called semi-DI [1, 14, 15]. The semi-DI scheme's assumptions can vary depending on users' needs, e.g. source-DI [16–19] have trusted measurement devices, or measurement-DI [20, 21], where the source device is trusted. At the same time, there are protocols with weaker assumptions, e.g., bounding the state's overlap or energy [22–25], granting a higher level of security.

In this work, by extending the approach proposed in [23] we demonstrate a semi-DI QRNG based on the ambiguity in discriminating non-orthogonal quantum states [26]. Non-orthogonal quantum states can not be perfectly distinguished due to the inevitable uncertainty imposed by the quantum theory. This uncertainty can be exploited, as in this protocol, to generate secure and private random numbers. A security estimation based on state overlap and unambiguous state discrimination was first derived in [23, 27] and later implemented for coherent detection schemes in [22, 24, 25].

We generalized the security framework initially presented in [23] in the case of a larger number of inputs and outputs (for more details and comparison, see Appendix B). We implement the protocol with a photonic setup based on a time-bin encoding with two configurations. In both configurations, we consider three inputs, while four and seven outcomes are tested in the respective structures.

The experimental setup is based on a prepare-and-measure scheme that features all-in-fiber commercially off-the-shelf (COTS) components at the telecom wavelength (1550 nm). The output entropy is evaluated given the correlation of the input-output data $p(b|x)$ along with the bound on the input states' energy that is the single measurable condition of this semi-DI QRNG. Furthermore, the user is capable of monitoring on-the-fly that the bound on the energy used to calculate the randomness rate is indeed verified by the given devices. Note that we assume that the inputs are identically and independently distributed (I.I.D. hypothesis).

The reduced number of assumptions with respect to other types of semi-DI QRNG allows to reduce the trust in the employed devices, thus increasing its security, while keeping its

[*] These authors contributed equally to this work.

performance on par with the commercial QRNGs [28]. Finally, this implementation can be further miniaturized by integrating it directly on a chip as shown in [29].

## II. FRAMEWORK

### A. Protocol

The experimental setup is based on a prepare-and-measure scheme, see Fig. 1. A ternary input $x \in \{0,1,2\}$ is fed into the preparation device, which prepares, accordingly, a quantum state $\hat{\rho}_x$, that is sent to the measurement station. Here, after the measurement of the quantum state, the station returns an output $b \in 0,1,\cdots,d-1$. The preparation and measurement devices are considered black boxes, with two simple assumptions on the preparation device: the prepared states are identically and independently distributed (I.I.D. hypothesis) and no correlations between the preparation device and any external device are present. Randomness can be certified if the following bound, easy-to-verify experimentally, holds on the energy of the prepared states:

$$\langle \hat{N} \rangle_{\rho_x} \leq \mu\,, \quad \forall x, \tag{1}$$

where $\hat{N}$ is the photon number operator (i.e. the energy of the state) and $\mu$ is its upper-bound.

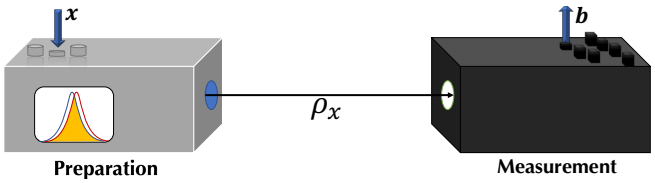


Figure 1. General schematic of the protocol; depending on the input $x$, the preparation device emits a quantum state $\rho_x$, with a single condition on the states' energy. The measurement site outputs $b$ after detecting the received states, as there is no assumption on the receiver side, it can be regarded as a black box.

If $\mu$ is below a certain threshold, the emitted states must be close to the vacuum, and so they must share some unavoidable overlap. According to quantum mechanics, non-orthogonal quantum states can not be deterministically distinguished meaning that outcomes of any measurement cannot be predicted with certainty.

From this simple idea it is possible to show that the amount of extractable randomness can be evaluated only by knowing the energy bound and the input-output correlations $P(b|x)$, in a semi-DI way. Indeed, the observation of certain correlations certifies that no pre-established strategies can fully reproduce the measured outcomes. The values of the correlations allow to certify their quantum nature and allows to bound the amount of entropy in the outcomes.

The scheme can be described as follows: the preparation device produces quantum states $\hat{\rho}_x$ while the measurement device performs a positive-operator valued measurement (POVM) $\hat{\Pi}_b^\lambda$. The classical variable $\lambda$, known to the adversary (e.g. the producer of the devices), represents the correlations between the measurement devices and the adversary. Each different realization $\hat{\Pi}_b^\lambda$ labeled by $\lambda$ can be implemented with probability $p_\lambda$. The input-output correlations $P(b|x)$ can then be written as

$$p(b|x) = \sum_\lambda p_\lambda \,\mathrm{Tr}[\hat{\rho}_x \hat{\Pi}_b^\lambda], \tag{2}$$

In order to bound the amount of private randomness that can be certified we need to bound, the guessing probability $P_{\text{guess}}$: the latter represents the maximum probability of guessing the outcome of the measurement device $b$ from the adversary point of view which has full knowledge of the fundamental working principle of the experiment apparatus and the input $x$. $P_{\text{guess}}$ can be evaluated as follows:

$$P_{\text{guess}} = \max_{\{p_\lambda, \hat{\rho}_x, \hat{\Pi}_b^\lambda\}} \left( \sum_x p_x \sum_\lambda p_\lambda \max_b \left\{ \mathrm{Tr}\left[\hat{\rho}_x \hat{\Pi}_b^\lambda\right] \right\} \right), \tag{3}$$

where $p_x$ is the probability of transmitting $x$. We assume that the probability of sending different inputs ($x$) is balanced $p_x = \frac{1}{3}$. The overall maximization is performed on the states and operators $\{p_\lambda, \hat{\rho}_x, \hat{\Pi}_b^\lambda\}$ that are compatible with the observed correlations and thus satisfy the constraint of Eq. (2).

Following the same approach shown in [23], since the preparation device shares no correlation with the environment, the maximum $P_{\text{guess}}$ is achieved when the states $\hat{\rho}_x$ are pure states, $\hat{\rho}_x = |\psi_x\rangle\langle\psi_x|$. Since the energy bound (1) implies on pure states a bound on their overlap (see [25, 30]) $|\langle\psi_x|\psi_y\rangle| \geq 1 - 2\mu \equiv \delta$, the choice that maximize $P_{\text{guess}}$ is obtained when the bound is saturated, namely $|\langle\psi_x|\psi_y\rangle| = \delta$, $\forall x, y$. Then, without losing generalities, the three states $|\psi_x\rangle$ can be then written as a linear combination of three orthonormal states $|0\rangle$, $|1\rangle$, $|2\rangle$ as follows:

$$\begin{aligned} |\psi_0\rangle &= |0\rangle\,, \\ |\psi_1\rangle &= \delta\,|0\rangle + \sqrt{1-\delta^2}\,|1\rangle\,, \\ |\psi_2\rangle &= \delta\,|0\rangle + \delta\sqrt{\frac{1-\delta}{1+\delta}}\,|1\rangle + \sqrt{\frac{1+\delta-2\delta^2}{1+\delta}}\,|2\rangle \end{aligned} \tag{4}$$

while $P_{\text{guess}}$ can be written as

$$P_{\text{guess}} = \frac{1}{3} \max_{\{p_\lambda, \Pi_b^\lambda\}} \left( \sum_{x=0}^{2} \sum_\lambda^{d-1} p_\lambda \max_b \left[ \langle\psi_x|\,\Pi_b^\lambda\,|\psi_x\rangle \right] \right) \tag{5}$$

It is possible to cast Eq. (5) into an semi-definite programming (SDP) problem, which can be efficiently solved (see appendix A). By inserting the input-output correlations $p(b|x)$ into the SDP, we can obtain a bound $P_g$ on the guessing probability and the conditional min-entropy[31] that quantifies the amount of private randomness

$$H_{\min} = -\log_2\{P_g\}. \tag{6}$$

Finally, after obtaining a bound on the min-entropy, secure

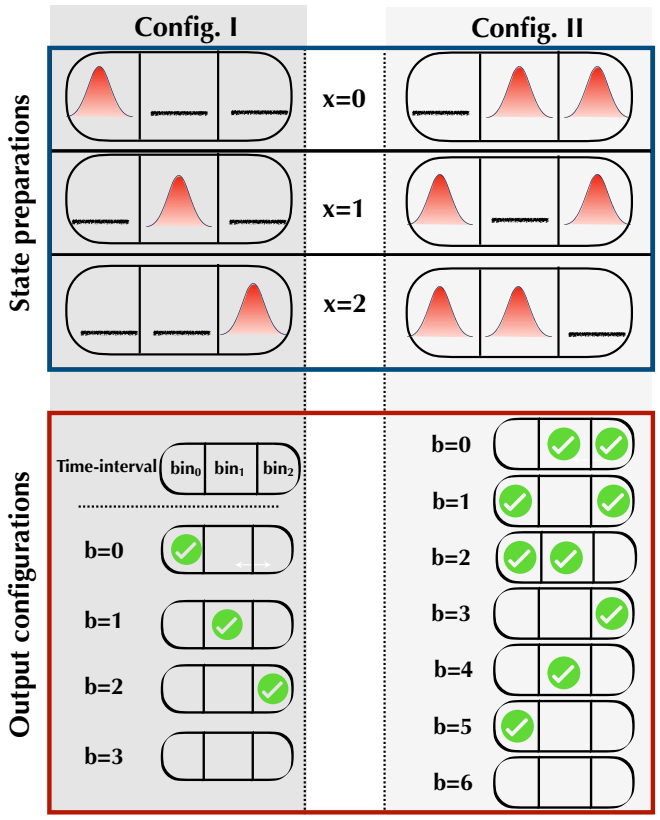


Figure 2. *Blue-box:* Proposed states preparation configurations; in Config. I, there is one weak-coherent state in each time-bin, while the second configuration owns two weak-coherent states per time-bin. *Red-box:* possible detection outcomes for the Config. I (left-side), and Config. II (right-side).

and private random numbers can be obtained thanks to the Leftover Hashing Lemma, using a Toeplitz randomness extractor [32].

### B. Implementation

The semi-DI protocol with ternary inputs and multiple outcomes described in the previous section can be implemented in different ways. In this work we present two configurations based on the ternary time-bin encoding shown in the top box of Fig. 2. In the first configuration (Config. I), the transmitter emits a coherent state $|\alpha\rangle$ once every three bins, while in the other two time-bins the vacuum state is present. In contrast, in the second configuration (Config. II), the vacuum state and weak coherent pules are reversed. For both configurations we choose $\mu = |\alpha|^2$ such that the condition written in eq. (1) is satisfied.

The main advantage of such implementations is the low experimental complexity of the state's preparation and the possibility to easily monitor the energy of the prepared states. For the first configuration (Config. I), shown in Fig. 2 (lower box), four possible outcomes $b \in \{0,1,2,3\}$ are considered, where $b = 0$, $b = 1$, and $b = 2$ occur when a detection is registered in the early ($bin_0$), middle ($bin_1$), and late ($bin_2$) time-interval, respectively, and if no click or more than one click is recorded, then the outcome is $b = 3$. On the other hand, for the second configuration (Config. II), a larger number of outcomes are possible. Let's for instance consider the case where $x = 0$ is chosen for Config. II (see Fig. 1). Due to the low values of $\alpha$ imposed by the energy bound and the non-unity efficiency of the detectors, it is possible that only one of the two pulses is detected ($b = 3$ or $b = 4$ in Fig. 2), or no pulses at all ($b = 6$ in Fig. 2). Thus, the total number of outcomes is increased from four to seven, with respect to the previous configuration.

### C. Input-output Correlation

Depending on the input $x$, the transmitter sends one of the ternary states represented in Fig. 1. We underline that the input $x$ are identically distributed and independent from the devices. The states are measured at the receiver through a single-photon detector, in this case, a superconducting nanowire single-photon detector (SNSPD) [33]. Based on the detection events and their arrival times, the receiver outputs $b \in \{0,1,2,3\}$, or $\{0,1,2,3,4,5,6\}$. Given the inputs $x$, and outputs $b$, we can compute the input-output correlation of the measurement and preparation devices $p(b|x)$, namely the probability of obtaining outcome $b$ given the input $x$.

In practice, the experimental setup is always combined with imperfections, mainly originated from the experimental apparatus; therefore, considering an ideal measurement would over-simplify our detection model. For example, the detector's dark count, background noise or imperfections in the state preparation, could lead to a theoretically impossible detection event. Therefore, we take these effects into account by introducing a value $\varepsilon$ associated with the noise. We point out that the parameter $\varepsilon$ is only useful for a correct modeling of the expected experimental probabilities, but it is not used in the $P_{\text{guess}}$ evaluation and it has no impact on the security and performances of the protocol.

The models used to describe the conditional probabilities $p(b|x)$ are the following:

Config. I, $\forall x \in \{0,1,2\}$

$$\begin{aligned} p(b=x|x) &= (1-\xi+\xi\varepsilon)(1-\varepsilon)^2\,, \\ p(b\neq x \wedge b\neq 3|x) &= \xi\varepsilon(1-\varepsilon)^2\,, \\ p(b=3|x) &= 1-p(b\neq 3|x)\,, \end{aligned} \tag{7}$$

where $\xi = |\langle\alpha|0\rangle|^2 = e^{-|\alpha|^2}$.

Config. II, $\forall x \in \{0,1,2\}$

$$\begin{aligned} p(b=x|x) &= (1-\xi+\xi\varepsilon)^2(1-\varepsilon)\,, \\ p(b=\varnothing_x|x) &= (1-\xi+\xi\varepsilon)\xi(1-\varepsilon)^2\,, \\ p(b=\varnothing''_x|x) &= \varepsilon\xi^2(1-\varepsilon)^2\,, \\ p(b\neq x \wedge b<3|x) &= (1-\xi+\xi\varepsilon)\varepsilon\xi(1-\varepsilon)\,, \\ p(b=6|x) &= 1-p(b\neq 6|x)\,. \end{aligned} \tag{8}$$

where $\varnothing' \in \{b=6\}$, $\varnothing_0 \in \{b=3, b=4\}$, $\varnothing_1 \in \{b=3, b=5\}$,

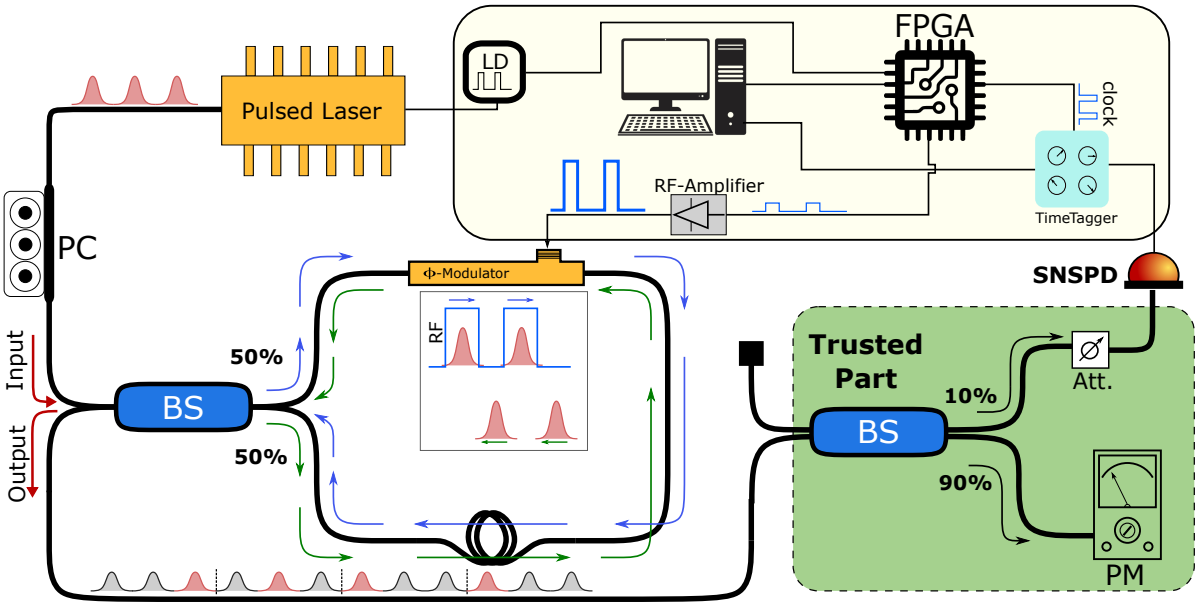


Figure 3. Experimental setup: A pulsed laser emits pulses at 1550 nm to a polarization controller (PC) and then a Sagnac interferometer (SI). One path in the SI is experiencing either an extra 0 or $\pi$-phase shift with respect to the other one. The two parts interfere and recombine at the beam-splitter (BS). Depending on the phase shift, light is redirected to either output or back to the input. Later the single photons are detected with a single-photon detector, in this case, an SNSPD. A time to digital converter (TDC) converts the SNSPD detection event to time-stamps which are analyzed in post-processing. A field-programmable gate array (FPGA) provides the electrical signal to drive the laser driver (LD), phase modulator, and synchronization clock.

$\varnothing_2 \in \{b=4, b=5\}$, $\varnothing_0'' \in \{b=5\}$, $\varnothing_1'' \in \{b=4\}$, and $\varnothing_2'' \in \{b=3\}$. Inserting these probabilities to the SDP (Eq. A3), we can compute the expected achievable min-entropy $H_{min}$ with our system.

The advantage of this scheme compared with other solutions based on coherent detection is the simplicity of the experimental setup, which does not require any complex phase-correction stabilization or further post-processing. These advantages are particularly relevant for real-time implementations. On the other hand, the possible drawback could be the random number generation rate, which, compared with similar continuous-variable systems [24, 25], is drastically lower, due to the high dead-time of the current SPDs [34].

## III. EXPERIMENT

The experimental setup is depicted in Fig. 3. The realization is based on an all-in-fiber scheme with components that are commercially available off-the-shelf (COTS). The setup's core is a fast and self-stabilized optical switch based on Sagnac interferometer (SI)[35], capable of operating up to GHz range. The switch is comprised of a (50 : 50) polarization-maintaining (PM) fiber-beamsplitter (BS), PM fiber delay line and a $LiNbO_3$ phase modulator (MPZ-LN-20 by iXblue). The (50 : 50) BS is used to split a pulse in two that travel in the Sagnac loop clockwise (CW) and counter-clockwise (CCW). The phase modulator applies a 0 or $\pi$-phase shift to the CW pulse while leaving the CCW one intact. The two parts are then recombined again at the BS and according to the phase modulation value are either redirected to the trusted part and then measurement unit or send back toward the laser where it is blocked by the internal isolator. The main advantage of the self-compensating Sagnac implementation over other types of intensity modulators is its resilience against phase fluctuations, ensuring very high extinction ratio at the output as well as high speed and long-term stability. Unlike other intensity modulator this device does not requires to be stabilized in temperature or bias voltage.

A pulsed laser emitting at 1550 nm with 2 ns pulse-width and fixed repetition rate of 10 MHz generates the train of pulses, which is first sent to a polarization controller (PC) and then to the input port of the switch. The input power is controlled accurately by changing its polarization via the polarization controller, where the PM-fiber BS acts as a polarizer. The output port of the switch is connected to a (90 : 10) PM-fiber BS, where the 90% output is used to monitor the power and the 10% is further transmitted along the optical path for the randomness generation.

A field programmable gate array (FPGA) board (ZedBoard by Avnet) provides the electrical signals to trigger the laser driver (LD) as well as phase modulation and a clock signal to synchronize the events. The phase modulation signal is amplified with an RF amplifier and then is used to drive the phase modulator. States $\rho_x$ are generated by properly switching the input pulse, removing two (one) from every three pulses of the pulse train in Config. I (II). A typical output of the optical switch for Config. I is depicted in Fig. 3. An arbitrary sequence can be fed into the FPGA to perform the switching. Two sequences of randomly distributed states, according to

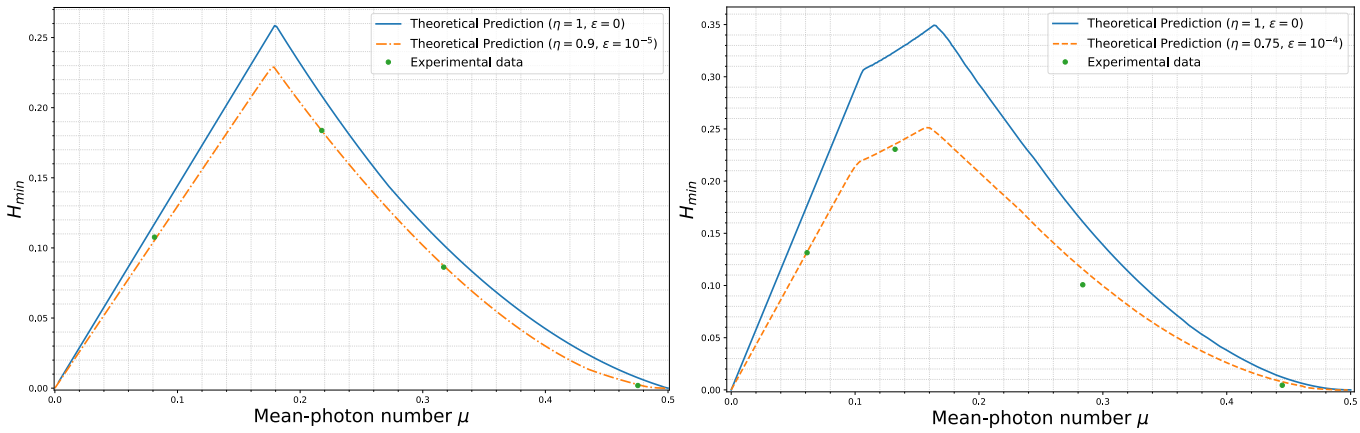


Figure 4. The conditional min-entropy as a function of the mean-photon number $\mu$ for Config. I (left-side), and Config. II (right-side). The dashed and solid-line curves show the theoretical prediction with and without the experimental loss, respectively. The green dots represent the experimental data. An SNSPD with detection efficiency equal to 75% is used for Config. II, while an SNSPD with higher detection efficiency, 90%, is used for the Cofing. I.

Config. I and II, are created and used for the experiment.

Finally, the mean photon number at the exit of the transmitter is regulated with extra attenuation (Att.) set properly at the beginning of the experiment and is left fixed to maintain the ratio of the output power and monitor. Prior to each run, the power is monitored and the average mean photon number per pulse is registered for the SDP and post-processing stages.

For the measurement, we exploited SNSPDs with different detection efficiencies to inspect matching of the results with the theoretical predictions for each configuration. Further analysis of the performances as a function of the detection efficiency is contained in Appendix B. The very low dark count and dead-time of SNSPDs allow for measurement and symbol detection at high repetition rates where, for example, $\mu$-second range hold-off time of single-photon avalanche diodes (SPAD) limits the detection rate to tens of kilo-symbols per second. Detection events are tagged with a time-to-digital converter (TDC) and the data is sent to a computer for post-processing. From the set of detections $b$ and the string of input $x$, it was possible to obtain the experimental conditional probabilities $p(b|x)$ for both configurations shown in Fig. 2.

## IV. RESULTS

This section presents the results obtained from the experimental data. We compare this experimental results with the model given by Eq. (7) and Eq. (8) After implementing the experimental setup, represented in Fig. 3, we performed several measurement-runs with various mean-photon numbers $\mu$. The mean-photon number is determined by a calibrated optical powermeter per operation run, represented in the green box in Fig. 3. Collecting the receiver's outcomes $b$, and given the input sequence $x$, we calculate the input-output correlation $p(b|x)$. The extractable amount of randomness is then estimated by inserting $p(b|x)$ and $\mu$'s experimental values into the SDP code.

Fig. 4 shows the conditional min-entropy per measurement, as a function of the mean-photon number for the two supported configurations. The experimentally obtained error value for Config. I and II are $\varepsilon = 10^{-5}$, and $\varepsilon = 10^{-4}$ respectively. The difference in the $\varepsilon$ values is due to the switch performance, noise and dark count rate (DCR) of the detectors which are $\simeq$ 70cps and $\simeq$ 1400cps in free-running, respectively.

This shows an excellent stability and performance of the switch as well as the detectors. In both plots, the blue curve represents the theoretical prediction without considering detection loss (perfect detector), while in the dashed orange curve, the losses (e.g., detector's efficiency) are also considered. The green dots correspond to the experimental data obtained with two SNSPDs with different efficiencies; 90% (used for Config. I), and 75% (used for Config. II). Comparing the experimental data and theoretical predictions, we see an excellent agreement between them.

From the theoretical model, the maximum conditional min-entropy with a lossless detector is 0.258, and 0.349 bits per measurement for Config. I and II, respectively. They occur when the mean-photon number $\mu$ is roughly around 0.18, and 0.164 for Config. I and II.

Nevertheless, taking the losses into consideration, the conditional min-entropy recedes from its optimum value. Indeed the output entropy is very sensitive to the detector efficiency and losses. A comprehensive study of the amount of extractable randomness versus detectors' efficiency for two different assumptions (energy and overlap) is presented in Appendix B. Taking into account the parameters $\eta$ and $\varepsilon$ that model our experiment, the maximum min-entropy that can be achieved experimentally are 0.183 and 0.23 for Config. I and II, respectively. We point our that the two configurations were not tested experimentally at their optimal points, but we tested they systems for some $\mu$ values as a proof-of-principle demonstration.

Exploiting an optical switch rather than modulating the

pulses directly on the laser has the advantage of avoiding fluctuations in mean photon number per pulse at the source due to laser cavity relaxation time. Besides, implementing binary or ternary states and states with higher number of time bins, e.g., 4, 5, etc., and various configurations can be readily done with this experimental setup, provided that the input to the FPGA is modified accordingly. Appendix B compares the conditional min-entropy for several time-bins strategies.

Finally, it should be noted that this is a proof-of-principle experiment, and it can be significantly improved and optimized in forthcoming works, particularly by utilizing integrated photonics.

## V. CONCLUSION

In conclusion, we have presented a practical semi-DI QRNG based on ternary input and measurements with multiple outcomes. Furthermore, we showed that it is possible to realize two different implementations with a simple setup based on time-bin encoding. In addition, we compared our results with a binary modulated system and showed that by increasing the number of inputs from two to three, the output randomness increases accordingly. The proposed protocol features an increased security with respect to common QRNG, since it only requires two simple assumptions and a measurable condition on the prepared pulses' energy. The latter condition is experimentally easier to verify respect to other semi-DI protocol, for example based on an overlap bound. Simultaneously, the protocol is practical, since it can be implemented with a simple all-fiber optical setup at telecom wavelength with only commercial off-the-shelf components. The performances of this proof-of-principle implementation could be further increased using faster repetition rates, faster modulation or integrated optics.

The proposed setup can also be useful to test higher dimensional states from an experimental point of view. In fact, this implementation only requires binary electrical signals even for higher dimensional states, while coherent systems require multi-amplitude modulations, increasing the complexity of the driving electronics. Compared to the security estimation presented in [30], our security evaluation requires an additional assumption (I.I.D hypothesis). Nevertheless, our protocol can be readily generalized for more input-outcome cases, while it is not clear how the security estimation provided in [30] can be generalized for more input and outputs. Indeed, one of the main objectives of semi-DI protocols is to facilitate the implementation and improve the generation rate while keeping the security relatively high, which is contemplated in our protocol. To conclude, our work shows how the increased number of input and output can improve the secure generation rate of QRNG in the semi-DI framework for future devices with simple experimental setups and high-security levels.

## ACKNOWLEDGMENTS

This work was supported by: "Fondazione Cassa di Risparmio di Padova e Rovigo" with the project QUASAR funded within the call "Ricerca Scientifica di Eccellenza 2018"; MIUR (Italian Minister for Education) under the initiative "Departments of Excellence" (Law 232/2016); EU-H2020 program under the Marie Sklodowska Curie action, project QCALL (Grant No. GA 675662).

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Information **2**, 16021 (2016).
[2] A. Acín and L. Masanes, Nature **540**, 213 (2016).
[3] A. Stanco, D. G. Marangon, G. Vallone, S. Burri, E. Charbon, and P. Villoresi, Phys. Rev. Research **2**, 023287 (2020).
[4] F. Regazzoni, E. Amri, S. Burri, D. Rusca, H. Zbinden, and E. Charbon, "A high speed integrated quantum random number generator with on-chip real-time randomness extraction," (2021), arXiv:2102.06238 [quant-ph].
[5] J. Thewes, C. Lüders, and M. Aßmann, Phys. Rev. A **100**, 052318 (2019).
[6] A. Kuznetsov, O. Nariezhnii, I. Stelnyk, T. Kokhanovska, O. Smirnov, and T. Kuznetsova, *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, **2**, 713 (2019).
[7] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and et al., Nature **464**, 1021–1024 (2010).
[8] P. J. Brown, S. Ragy, and R. Colbeck, IEEE Transactions on Information Theory **66**, 2964 (2020).
[9] W.-Z. Liu *et al.*, Nature Physics (2021), 10.1038/s41567-020-01147-2.
[10] Y. Liu *et al.*, Nature **562**, 548 (2018), arXiv:1807.09611.
[11] Y. Zhang *et al.*, Phys. Rev. Lett. **124**, 010505 (2020).
[12] M.-H. Li *et al.*, Phys. Rev. Lett. **126**, 050503 (2021).
[13] G. Foletto, M. Padovan, M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Experimental test of sequential weak measurements for certified quantum randomness extraction," (2021), arXiv:2101.12074 [quant-ph].
[14] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).
[15] A. Tavakoli, "Semi-device-independent framework based on restricted distrust in prepare-and-measure experiments," (2021), arXiv:2101.07830 [quant-ph].
[16] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).
[17] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Unbounded randomness from uncharacterized sources," (2020), arXiv:2010.05798 [quant-ph].
[18] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Nature Communications **9**, 5365 (2018).
[19] 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, Phys. Rev. X **10**, 041048 (2020).
[20] Z. Cao, H. Zhou, and X. Ma, New Journal of Physics **17**, 125011 (2015).
[21] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Physical Review A **94** (2016), 10.1103/physreva.94.060301.
[22] H. Tebyanian, M. Avesani, G. Vallone, and P. Villoresi, "Semi-

device independent randomness from d-outcome continuous-variable detection," (2020), arXiv:2009.08897 [quant-ph].
[23] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Physical Review Applied **7**, 054018 (2017).
[24] D. Rusca, H. Tebyanian, A. Martin, and H. Zbinden, Applied Physics Letters **116** (2020), 10.1063/5.0011479, arXiv:2004.08307.
[25] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Phys. Rev. Applied **15**, 034034 (2021).
[26] S. M. Barnett and S. Croke, Adv. Opt. Photon. **1**, 238 (2009).
[27] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Quantum **1**, 33 (2017).
[28] G. Gras, A. Martin, J. W. Choi, and F. Bussières, "Quantum entropy model of an integrated qrng chip," (2020), arXiv:2011.14129 [quant-ph].
[29] N. Leone, D. Rusca, S. Azzini, G. Fontana, F. Acerbi, A. Gola, A. Tontini, N. Massari, H. Zbinden, and L. Pavesi, APL Photonics **5**, 101301 (2020), https://doi.org/10.1063/5.0022526.
[30] T. Van Himbeeck and S. Pironio, arXiv preprint arXiv:1905.09117 (2019).
[31] R. Konig, R. Renner, and C. Schaffner, IEEE Transactions on Information Theory **55**, 4337 (2009).
[32] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Transactions on Information Theory **57**, 5524 (2011).
[33] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, R. J. Warburton, H. Zbinden, and F. Bussières, Applied Physics Letters **112**, 061103 (2018), https://doi.org/10.1063/1.5010102.
[34] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Review of Scientific Instruments **82**, 071101 (2011), https://doi.org/10.1063/1.3610677.
[35] G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Opt. Lett. **43**, 5110 (2018).
[36] J.-D. Bancal, L. Sheridan, and V. Scarani, New Journal of Physics **16**, 033011 (2014).
[37] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex optimization* (Cambridge university press, 2004).

## Appendix A: Generalized Semi-definite Programming for $n$-input $d$-outcome

### 1. Primal

This appendix presents a generalized expression of the guessing probability optimization problem shown in Eq.3, in the form of a semidefinite program (SDP). This optimization is used to derive a bound on the min-entropy for a $n$-input $d$-outcome semi-DI QRNG protocol based on an energy bound, generalizing the approach proposed in [23]. The generalized form of guessing probability for $n$-input $d$-outcomes reads:

$$P_{\text{guess}} = \frac{1}{n} \max_{\{\rho_x^{\boldsymbol{\lambda}}, p_{\boldsymbol{\lambda}}, \Pi_b^{\boldsymbol{\lambda}}\}} \left( \sum_{x=0}^{n-1} \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \max_b \left\{ \text{Tr}\left[\rho_x^{\boldsymbol{\lambda}} \Pi_b^{\boldsymbol{\lambda}}\right] \right\} \right), \tag{A1}$$

where $\Pi_b^{\boldsymbol{\lambda}}$ with $b = 0, \cdots, d-1$ represent positive-operator valued measurement (POVM) operators in a $n$ dimensional Hilbert space and the states $\rho_x$ satisfy the constraint $p(b|x) = \sum_{\boldsymbol{\lambda}} p_{\boldsymbol{\lambda}} \text{Tr}[\hat{\rho}_x \hat{\Pi}_b^{\boldsymbol{\lambda}}]$. In the above equation, we assume the probability of transmitting $x \in \{0, \ldots, n-1\}$ is identical and equal to $p_x = \frac{1}{n}$. The variable $\boldsymbol{\lambda}$ labels a possible "strategy". As discussed in [23] and [36], all strategies in which the inner maximization over $b$ in equation (A1) occurs for the same value of $b$ at given $x$ can be grouped. Consequently, it is sufficient to consider at most $d^n$ strategies when maximizing equation (A1) over all potential measurement strategies. Then, each strategy can be labeled as $\Lambda = (\lambda_0, \cdots, \lambda_{n-1})$, where $\lambda_k = 0, \cdots, d-1$, and $\sum_\Lambda := \sum_{\lambda_0=0}^{d-1} \cdots \sum_{\lambda_{n-1}=0}^{d-1}$ is defined for simplicity. The value of $\lambda_x$ indicates that the $b = \lambda_x$ outcome maximizes $\text{Tr}\left[\rho_x \Pi_b^\Lambda\right]$ when the state $\hat{\rho}_x$ is sent. By absorbing the weight $p_\Lambda$ into the normalization of POVMs, $M_b^\Lambda = p_\Lambda \Pi_b^\Lambda$, Eq. (A1) can be rewritten as

$$P_{\text{guess}} = \frac{1}{n} \max_{\{M_b^\Lambda\}} \sum_{x=0}^{n-1} \sum_{\Lambda} \text{Tr}\left[\rho_x M_{\lambda_x}^\Lambda\right], \tag{A2}$$

As discussed in the main text, the states $\rho_x$ can be chosen to be pure $\rho_x = |\psi_x\rangle\langle\psi_x|$. If the energy constraint is imposed, then the states $\{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$ can be can be express as a linear combination of an orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ with fixed overlap $|\langle\psi_x|\psi_y\rangle| = \delta$ for $x \neq y$.

The maximization of the guessing probability $P_{\text{guess}}$ can be cast as an SDP, whose primal form can be written as follows

$$\begin{aligned}
\underset{M_b^\Lambda}{\text{maximize}} \quad & P_{\text{g}} = \frac{1}{n} \sum_{x=0}^{n-1} \sum_{\Lambda} \langle\psi_x| M_{\lambda_x}^\Lambda |\psi_x\rangle \\
\text{subject to} \quad & M_b^\Lambda = (M_b^\Lambda)^\dagger, \\
& M_b^\Lambda \geq 0, \\
& \sum_{b=0}^{d-1} M_b^\Lambda = \frac{1}{n} \text{Tr}[\sum_{b=0}^{d-1} M_b^\Lambda] \mathbb{I}, \\
& \sum_{\Lambda} \langle\psi_x| M_b^\Lambda |\psi_x\rangle = p(b|x), \quad \forall b, x
\end{aligned} \tag{A3}$$

where $M_b^\Lambda$ are $n \times n$ Hermitian semi-positive matrices. This maximization defines an SDP, converging to optimal bounds on $P_{\text{guess}}$ given the constraints on the overlap or the energy and the observed data $p(b|x)$.

The maximization is performed over all measurement strategies $M_b^\Lambda$ meaning that the computational cost increases with the number of outcomes. In this case, we can also derive the dual SDP, whose derivation is described in the next section.

### 2. Dual

The dual SDP has three critical benefits when compared with the primal version: it gives an upper-bound on the guessing probability rather than a lower-bound. In this way, conservative bounds are obtained, which never overestimates the min-entropy. Further, the dual form enables recomputing

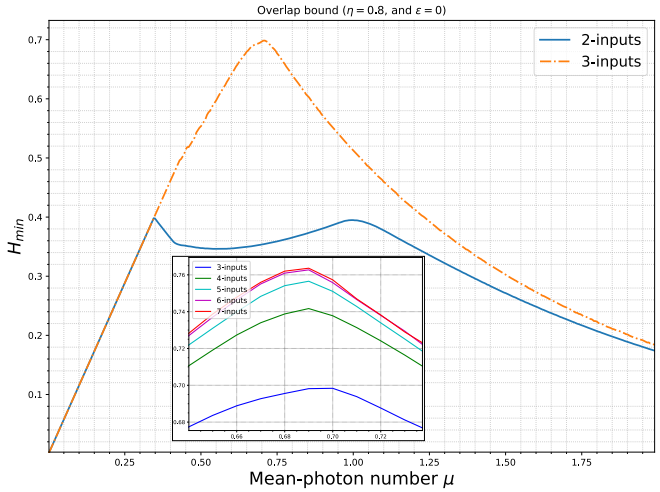


Figure 5. The conditional min-entropy as a function of mean-photon number for a different number of inputs based on overlap assumption when the detector efficiency is 80%. 2-inputs describes two time-intervals; one is empty, the other has a weak-pulse (similar to [23]), and 3-inputs is depicted in Fig. 1. *Inset*: more numbers of inputs is represented.

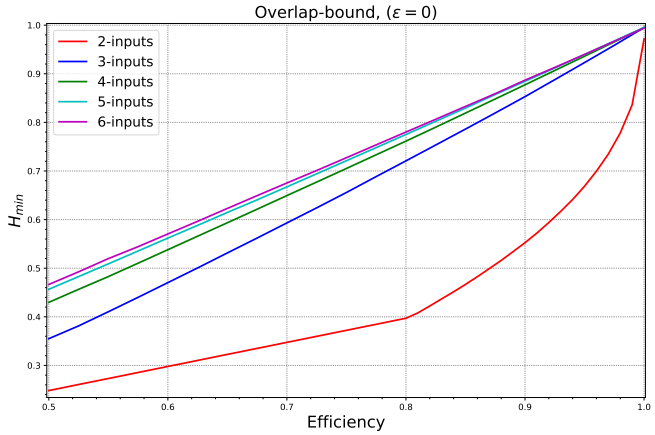


Figure 6. The maximum achievable conditional min-entropy (with optimal mean-photon number) as a function of the detector's efficiency.

bounds without running a full optimization for real-time operation, reducing the entropy estimation resources. Lastly, the finite-size effects can be easily taken into account with this formulation. Here, we use Lagrangian duality [37], with an approach a similar to the one used in [23, 36]. We define the Lagrangian associated with the problem (A3) as:

$$\begin{aligned}\mathscr{L} =& \frac{1}{n}\sum_{x=0}^{n-1}\sum_{\Lambda}\mathrm{Tr}[\rho_x(\sum_{b=0}^{d-1}\delta_{\lambda_x,b}M_b^{\Lambda})] + \sum_{\Lambda,b}\mathrm{Tr}[G_b^{\Lambda}M_b^{\Lambda}] + \\ &+ \sum_{\Lambda}\mathrm{Tr}[H^{\Lambda}\sum_{b}\left(M_b^{\Lambda} - \frac{1}{n}\mathrm{Tr}[M_b^{\Lambda}]\right)] + \\ &+ \sum_{x,b}\nu_{bx}\{\sum_{\Lambda}\mathrm{Tr}[\rho_x M_b^{\Lambda}] - p(b|x)\},\end{aligned} \tag{A4}$$

where $n\times n$ Hermitian matrices $H^{\Lambda}$, $G_b^{\Lambda}$, and scalar coefficient $\nu_{bx}$ are introduced as the Lagrange multipliers to each constraint in the primal problem. $\lambda_0,\ldots,\lambda_{n-1}$ and $b$ range from 0 to $d-1$, and $x$ ranges from 0 to $n-1$. The next step is finding the supremum of the Lagrangian over the primal variables $M_b^{\Lambda}$. Now we minimize $\mathscr{L}$ over the Lagrangian multipliers to get a tighter bound on the guessing probability, so we have

$$\overbrace{\sup_{M_b^{\Lambda}}(\mathscr{L})}^{\chi} = \sup_{M_b^{\Lambda}}\{\sum_{\Lambda,b}\mathrm{Tr}[M_b^{\Lambda}J_b^{\Lambda}] - \sum_{x,b}\nu_{bx}p(b|x)\}, \tag{A5}$$

where

$$J_b^{\Lambda} = \sum_x \rho_x(\frac{1}{n}\sum_{b=0}^{d-1}\delta_{\lambda_x,b} + \nu_{bx}) + G_b^{\Lambda} + H^{\Lambda} - \frac{1}{n}\mathrm{Tr}[H^{\Lambda}]. \tag{A6}$$

Considering there is no constraint on $M_b^{\Lambda}$ in the Lagrangian, the supremum in Eq. (A5) will be infinite, except $J_b^{\Lambda}$ is restricted to be zero; thus we require that $J_b^{\Lambda} = 0$.

However, given that the operators $G_b^{\Lambda}$ are positive semidefinite, due to the second constraint of the primal SDP (A3), this is equivalent to cut $G_b^{\Lambda}$ from Eq. (A5) and expecting the rest of the expression to be negative semidefinite. Consequently, we have the dualized SDP as

$$P_g^* = \min_{H^{\Lambda},\nu_{bx}}[-\sum_{x=0}^{n-1}\sum_{b=0}^{d-1}\nu_{bx}p(b|x)] \tag{A7}$$

subjected to

$$H^{\Lambda} = (H^{\Lambda})^{\dagger}, \tag{A8}$$

$$\sum_x \rho_x(\frac{1}{n}\sum_{b=0}^{d-1}\delta_{\lambda_x,b} + \nu_{bx}) + H^{\Lambda} - \frac{1}{n}\mathrm{Tr}[H^{\Lambda}]\mathbb{I} \leq 0, \tag{A9}$$

## Appendix B: Overlap bound and many inputs

In this section we compare the energy bound considered so far $\langle\hat{N}\rangle_{\rho_x} \leq \mu$ with the overlap bound assumption $\langle\psi_x|\psi_y\rangle \geq \delta$ proposed in [23]. The advantage of the overlap bound assumption is that the QRNG could operate in a broader mean-photon number range and higher rates can be achieved. However, from the experimental point of view, testing the energy bound is easier than ensuring that the overlap bound is satisfied. We note that the bound on the energy imposes a bound on the overlap (see[27]), but not the other way around. We will also compare the performances of the proposed implementation when the number of inputs are increased.

### 1. Overlap bound

To apply the overlap instead of the energy bound, we should change the assumption to

$$|\langle\psi_i|\psi_j\rangle| \geq e^{-\mu}, \quad x,y \in \{0,1,2\}, \; x \neq y. \tag{B1}$$

For the estimation of the min-entropy with the overlap bound, we use the security framework described in the text (and in Appendix A), with the only difference of the substitution of the overlap in Eq.4 with the one given by Eq. B1.

In Fig. 5, the conditional min-entropy is plotted as a function of the mean-photon number for binary and ternary time-bin (Config. I) encoding schemes when the detector's efficiency is 80%. As shown, the maximum value of conditional min-entropy increases from 0.4 to 0.7, which is a significant improvement.

We also show in the inset of Fig. 5 the numerical results obtained by increasing the number of inputs to four, five, six and seven. It is worth to notice that, besides the extra experimental and computational complexity added by increasing the inputs, a negligible growth in the conditional min-entropy's maximum value is observed. Therefore, the ternary time-bin encoding scheme provides an excellent trade-off between the achievable conditional min-entropy and computational complexity. It should be pointed out that when the number of inputs increases, the number of possible outcomes rise accordingly, and the guessing probability should be optimized over more measurement and preparation strategies. Thus, the optimization problem—either as a form of dual or primal SDP—would require more time to be determined, which reduces the system's rate. Notwithstanding, for a chosen number of input/output, the dual form can boost the generation rate compared to the primal form, since it allows to compute (sub-optimal) bounds without running a full optimization (the value of $P_g^*$ is linear in the experimental values $p(b|x)$. We further show in Fig. 6 the maximum achievable min-entropy (maximized of the possible $\mu$ values) in function of the detector's efficiency. From the figure it is evident that increasing the number of outcomes from 2 to three increases the resistance to inefficiency. As expected, the maximum achievable min-entropy decreases by reducing the detector's efficiency, but only for 3 or more inputs it shows a quasi-linear behavior in function of the efficiency.

The gap between 2-inputs and 3-inputs cases grows when the detector efficiency decreases, while for the rest inputs, the gap is almost constant, see Fig. 6. This shows that the ternary encoding scheme is more robust to the detector efficiency than the binary one, which is an advantage as the typical single-photon detector's efficiency ranges from 0.5 to 0.95.

### 2. Energy bound with many inputs

In this subsection, by employing the general SDP form given in the Appendix A, we study the effect of changing the detector efficiency and the number of inputs when the energy bound is considered. Let's first consider the effect of detector efficiency, when no error are present ($\varepsilon = 0$). In Fig. 7 we show the maximum value of the min-entropy that can be achieved in function of the detection efficiency. Fig. 7 shows that increasing the number of inputs always improves the generation rate also when detection inefficiencies are taken into account. Consequently, it is possible to find the optimal trade-off between the computational complexity, entropy value, and robustness to the detector's efficiency. Fig. 8 shows the maximum min-entropy and the corresponding optimal value of $\mu$ as a function of the number of inputs in the noiseless perfect-efficiency case ($\eta = 1$, $\varepsilon = 0$). The data indicate that the optimal mean-photon number grows with the number of inputs and seemingly reaches a plateau of about 0.25 for high number of inputs ($> 9$). The 2-inputs results shown in Figs. (6) and (7) illustrate that the binary inputs preparation scheme is less sensitive to the efficiency when the energy bound is considered.

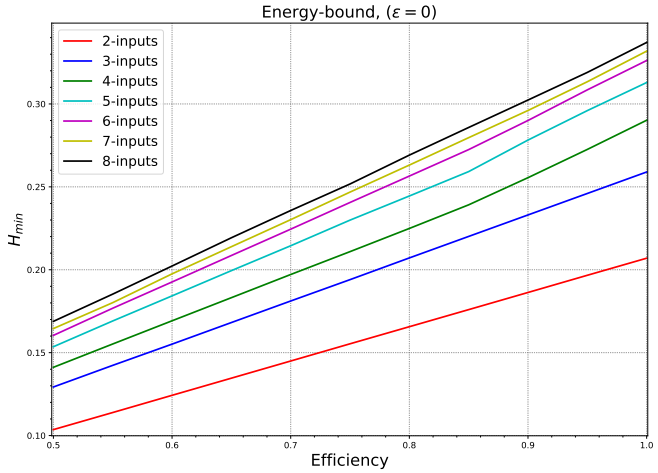


Figure 7. The maximal achievable conditional min-entropy (with optimal mean-photon number) as a function of the detector's efficiency when the energy bound is considered.

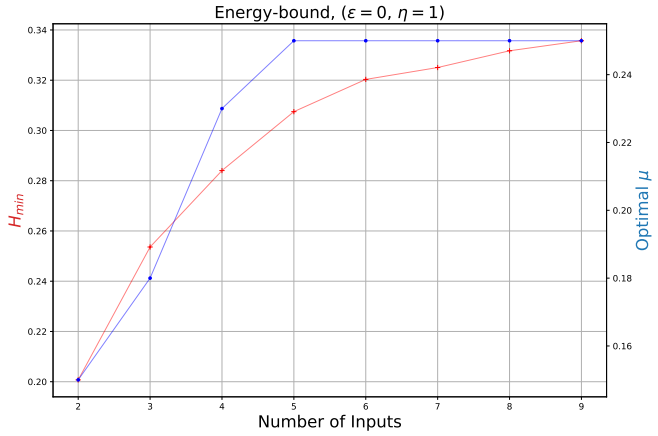


Figure 8. The maximum conditional min-entropy $H_{min}$ and the corresponding optimal value of $\mu$ (for $\eta = 1$) is plotted as a function of inputs. The value of the optimal $\mu$ raises when the number of inputs increases and asymptotically reaches a plateau of $\sim 0.25$.