
Article:
Tebyanian, Hamid, Avesani, Marco, Vallone, Giuseppe et al. (2021) Semi-device independent randomness from d-outcome continuous-variable detection. Physical Review A. 062424. ISSN: 1094-1622

https://doi.org/10.1103/PhysRevA.104.062424

Semi-device independent randomness from d-outcome continuous-variable detection

Hamid Tebyanian,[1] Marco Avesani,[1] Giuseppe Vallone,[1,2,3] and Paolo Villoresi[1,3]

[1] *Dipartimento di Ingegneria dell'Informazione, Università di Padova, via Gradenigo 6B, 35131 Padova, Italy*
[2] *Dipartimento di Fisica e Astronomia, Università di Padova, via Marzolo 8, 35131 Padova, Italy*
[3] *Istituto di Fotonica e Nanotecnologie - CNR, Via Trasea 7 - 35131 Padova, Italy*

Recently, semi-device independent protocols have attracted increasing attention, guaranteeing security with few hypotheses and experimental simplicity. In this paper, we demonstrate a many-outcomes scheme with the binary phase-shift keying (BPSK) for a semi-device independent protocol based on the energy assumption. We show in theory that the number of certified random bits of the d-outcomes system outperforms the standard scheme (binary-outcomes). Furthermore, we compare the results of two well-known measurement schemes, homodyne and heterodyne detection. Lastly, taking into account the experimental imperfections, we discuss the experimental feasibility of the d-outcome design.

I. INTRODUCTION

In the information security age, data privacy and secure communication are of paramount relevance. It is worth to stress the role of genuine random numbers for privacy and security applications. Nearly all of the protocols dealing with privacy and security relies on random numbers, and the protocol's security is directly connected to the quality of the employed random numbers [1]. Thus, owning certified random numbers is a critical component for guarding the information. Pseudo-random number generators have been popular and widely used in the past few decades. However, the generated numbers are not truly random since the randomness source is based upon a classical phenomenon that is deterministic. In general, random number generators (RNG) can be classified into two major groups, classical and quantum. Due to their determinism, Classical RNG cannot offer high levels of security, while quantum random number generators (QRNG), are qualified candidates for generating genuine and unpredictable random numbers based on the intrinsic randomness of quantum mechanics [2].

Despite the fact that quantum mechanics assures the unpredictability of the generated random numbers, experimental imperfections of QRNG can open a backdoor for eavesdroppers to attack or manipulate the protocol [3]. For instance, the generator's apparatus can be correlated with an external party, or deviate from the expected behaviour. Hence QRNGs can be categorized into three subgroups, trusted-device, semi-device independent (semi-DI), and device-independent (DI) QRNGs [4]. Although the trusted-deceive QRNGs are cheap, fast, and more reliable than the classical generators, they can be compromised due to the security loopholes resulting from trusting the devices. On the other hand, the highest security is achievable by DI QRNGs where randomness is certified by the violation of a Bell inequality, without any trust on any devices [5].

Besides offering highly secure randomness, it also allows the devices to be undependable and, hence, robust against experimental imperfections. Unfortunately, the experimental realization of a loophole-free Bell test is extremely hard to accomplish, and only proof-of-principle experiments were realized, obtaining modest generation rates [6–10]. Taking into account the complexity of this protocol and the low bit rate, the DI QRNGs are still very far from being practical. Indeed, security and speed are the two key features of RNG and both are needed in practical applications.

Semi-DI protocols are an intermediate approach between DI and trusted-device schemes, which offer an optimal trade-off between generation rate, security, and ease-of-implementation [4]. Depending on the protocol needs, assumptions can vary; for very secure protocols, there are fewer assumptions on the device, i.e., single assumption on the overlap or energy of the prepared states [11–16]. Depending on the protocol needs, assumptions can vary; they can be related to the dimension of Hilbert space [17, 18], they may require trusted measurement in the case of source-DI protocols [19–21] or they may assume a trusted source, an in measurement-DI protocols [22, 23]. Recently a new class of protocols has been proposed, where both source and measurement are untrusted and only a single assumption on the overlap or energy of the prepared states is required [11–16]. These protocols can provide an increased security, since they reduce the number of assumptions on the devices.

In this work, we investigate the impact of increasing the number of outcomes of the measurement apparatus given a binary-input semi-DI QRNG [15, 16]. The protocol builds upon the prepare-and-measure scheme, with a single assumption on the maximum energy of the prepared states that implies a lower bound on the state's overlap. The implementation is based on optical continuous variables (CVs), that allow high generation rates.

As shown in [24], for a SDI-QRNG with n inputs subjected to the overlap bound, the measurement apparatus achieving the maximum randomness is obtained by using an $n+1$ outcome POVM and no more than $\log_2(n+1)$ random bits can actually be certified. However, such optimal POVM is not easily obtained with typical CV measurements and we will show that, if the measurement is realized by using homodyne or heterodyne detector, increasing the number of outputs to more than 3 (for 2 in-

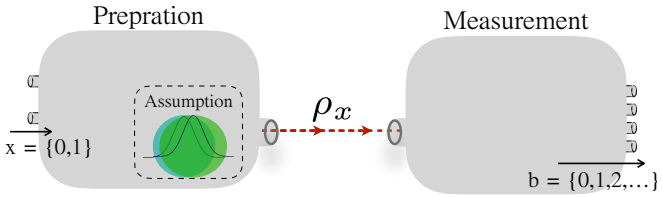

Figure 1. The general design of QRNG protocol. Depending on the input x, the unknown state ρ_0 or ρ_1 is transmitted from the preparation part. A single assumption is present on the state's energy. The measurement device, with no assumptions, performs a generic measurement and outputs $b \in \{0, \ldots, d-1\}$.

puts) will improve the generation rate. In particular, we will report the numerical results of the method employed for randomness estimation, from three to fourteen outcomes, concerning both homodyne and heterodyne detections and then compare it with the binary outcomes result. We will also investigate the generation rate as a function of the system efficiency, showing that the advantage of increasing the number of outcomes decreases with lower efficiency.

II. SDI-QRNG MODEL

A. General framework

The protocol is based on two untrusted devices, the preparation and measurement, and a single assumption corresponding to an upper bound on the prepared state's energy. Similar approaches were presented in [11, 13, 16]. A general scheme of this protocol is shown in Fig. 1:

a preparation device emits the unknown states ρ_x after receiving the binary input $x \in \{0, 1\}$ from the user. The measurement device has d outputs $b \in \{0, 1, \cdots, d-1\}$. By running N times the experiment it is possible to estimate the conditional probabilities $p(b|x)$.

The measurement device is considered as a black box, whose internal working principles are unknown to the user. The preparation device is a 'gray box": the internal working principles are not known but it comes with an assumption, namely an upper bound on the energy of the prepared states

$$\langle \hat{n} \rangle_{\rho_x} \leq \mu \,. \tag{1}$$

As shown in [25], the conditional min-entropy, namely the amount of genuine random bits per measurement run is given by

$$H_{\min} = -\log_2 (P_{\rm g}) \tag{2}$$

where $P_{\rm g}$ is the guessing probability, namely the highest probability that an attacker knowing the internal working principle of the devices can guess the outcomes b, given the input x. It is worth to note that the bound on the energy, whose validity can be checked experimentally, implies a lower bound on the scalar product between the emitted states [13, 16] and thus the approach of [11] can be followed to obtain $P_{\rm g}$ from the experimental data.

By generalizing the approach of [11] with d outcomes, $P_{\rm g}$ can be found as the solution of the following semidefinite programming (SDP)

$$\begin{aligned}
\underset{M_b^{\lambda_0,\lambda_1}}{\text{maximize}} \quad & \widetilde{P}_{\rm g} = \frac{1}{2} \sum_{x=0}^{1} \sum_{\lambda_0,\lambda_1=0}^{d-1} \langle \psi_x | \, M_{\lambda_x}^{\lambda_0,\lambda_1} \, | \psi_x \rangle \\
\text{subject to} \quad & M_b^{\lambda_0,\lambda_1} = (M_b^{\lambda_0,\lambda_1})^\dagger, \\
& M_b^{\lambda_0,\lambda_1} \geq 0, \\
& \sum_{b=0}^{d-1} M_b^{\lambda_0,\lambda_1} = \frac{1}{2} \mathrm{Tr}[\sum_{b=0}^{d-1} M_b^{\lambda_0,\lambda_1}] \mathbb{I}, \\
& \sum_{\lambda_0,\lambda_1=0}^{d-1} \langle \psi_x | \, M_b^{\lambda_0,\lambda_1} \, | \psi_x \rangle = p(b|x) \,, \quad \forall b, x
\end{aligned} \tag{3}$$

where $M_b^{\lambda_0,\lambda_1}$ are 2×2 operators in the 2-dimensional Hilbert space spanned by the orthonormal vectors $|0\rangle$ and $|1\rangle$ and the states $|\psi_x\rangle$ are defined by

$$\begin{aligned}
|\psi_0\rangle &= |0\rangle \,, \\
|\psi_1\rangle &= (1-2\mu) \, |0\rangle + 2\sqrt{\mu(1-\mu)} \, |1\rangle \,.
\end{aligned} \tag{4}$$

The above states $|\psi_x\rangle$ saturates the bound $|\langle \psi_0 | \psi_1 \rangle| \geq 1 - 2\mu$ derived from (1), and can be used in the optimization without loss of generality see [12, 16]. In Eq. (3) we assumed that the input states are prepared with equal probability, namely $p_x = 1/2$.

The variables $\lambda \equiv (\lambda_0, \lambda_1)$ represent the classical information available to anyone knowing the internal working of the device. The operators $M_b^{\lambda_0\,\lambda_1}$ are related to possible physical realizations of the measurement device that are compatible with the observed probabilities $p(b|x)$. More precisely, for each value of the pair $(\lambda_0\,\lambda_1)$, the value $q_\lambda = \frac{1}{2}\mathrm{Tr}[\sum_b M_b^{\lambda_0,\lambda_1}]$ represents the probability that the measurement device is actually implementing the POVM defined by the operators $\{\Pi_b^{\lambda_0\,\lambda_1}\}$ where $\Pi_b^{\lambda_0\,\lambda_1} = M_b^{\lambda_0\,\lambda_1}/q_\lambda$.

It is worth noticing that the above approach is general and does not depends on the actual implementation of the preparation and measurement devices. The min-entropy is directly calculated by using only the value of the energy bound μ and the measured output probabilities $p(b|x)$, independently of their physical realization. We observe that larger $H_{\min}$ can be obtained whenever the probabilities $p(b|x)$ allow to better distinguish the two input states.

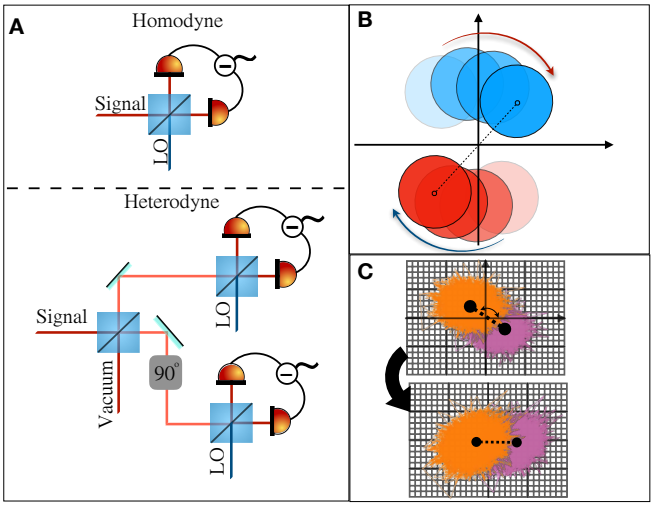

Figure 2. Homodyne and heterodyne detection. a) Representation of the two detection schemes, b) Effects of the phase instability on the received states, c) Offline phase compensation for heterodyne detection.

B. Implementation with continuous variables

We now illustrate the amount of randomness that can be obtained by using single-mode optical continuous variables defined by the creation operator $\hat{a}^\dagger$.

1. *Preparation*

In the preparation part, we employed the Binary Phase Shift-Keying (BPSK) system, where the source, a continuous-wave (CW) laser, emits two coherent states with the same mean-photon number and a π phase shift $|\psi_0\rangle = |\alpha\rangle$ and $|\psi_1\rangle = |-\alpha\rangle$. We can use the representation of a coherent state in Fock space to define $|\alpha\rangle$ as $|\pm\alpha\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{(\pm\sqrt{\mu}e^{i\phi})^n}{\sqrt{n!}} |n\rangle$, where $\alpha = \sqrt{\mu}e^{i\phi}$, μ is the mean photon number and ϕ is the relative phase between the signal and the local oscillator (LO). We here assume that the LO is chosen such that $\phi = 0$. Note that the input x should be uncorrelated with λ and independent of the devices. Thus they can be generated from a standard RNG (e.g., Pseudo RNG). We note that the mean photon number for each state $|\psi\rangle$ is upper-bounded by the quantity μ given in Eq. (1). We note that states with non-vanishing overlap cannot be deterministically distinguished, unlike orthogonal states.

2. *Measurement*

Homodyne and heterodyne tomography are two primary and well-established detection schemes for measuring CV states of light, see Fig. 2. By homodyning, the quantum state is measured from samples obtained from projected Wigner functions, whereas heterodyne detection directly samples phase space coordinates from the Husimi Q-function [26, 27]. For what regards Semi-DI QRNG protocols, both heterodyne and homodyne detection have been employed at the receiver side, as shown in [16] and [15], respectively. In these works, the (potentially) infinite outcomes of the CV measurement are grouped into two disjoint sets, corresponding to a binary outcome. Here we consider the more general case in which the physical outcomes can be grouped into a larger number of sets.

The POVM of homodyne and heterodyne receivers can be represented respectively by:

$$\begin{aligned} \Pi^{(\mathrm{hom})}(X) &= |X\rangle\langle X| \\ \Pi^{(\mathrm{het})}(\beta) &= \frac{1}{\pi}|\beta\rangle\langle\beta| \end{aligned} \tag{5}$$

where $|X\rangle$ is the eigenstate of the $\hat{X} = (\hat{a}+\hat{a}^\dagger)/\sqrt{2}$ operator and $|\beta\rangle$ is the coherent state with complex amplitude β.

The corresponding probability densities associated to the measurement of the states $\left|\pm\sqrt{\mu}\right\rangle$ are given by

$$\begin{aligned} \mathcal{P}_{\pm}^{(\mathrm{hom})}(X) &= \sqrt{\frac{2}{\pi}} e^{-2(X\mp\sqrt{\eta\mu})^2}, \\ \mathcal{P}_{\pm}^{(\mathrm{het})}(\beta) &= \frac{1}{\pi} e^{-(X\mp\sqrt{\eta\mu})^2} e^{-Y^2}, \end{aligned} \tag{6}$$

with real X, Y and $\beta = X + iY$. In the above equations we included the overall efficiency η of the channel and of the receiver devices. In order to obtain d possible outcomes $b = 0, 1, \cdots d-1$ we need to partition the real line (X) or the phase space (β) into d disjoint sets.

In the homodyne case, it is necessary to choose $d-1$ increasing real numbers $X_1 < X_2 < \ldots < X_{d-1}$ such that the outcome probabilities for $b = 0, \cdots, d-1$ can be written as

$$\begin{aligned} p^{(\mathrm{hom})}(b|x) &= \frac{1}{\sqrt{\pi}} \int_{X_b}^{X_{b+1}} e^{-(X-(-1)^x\sqrt{2\eta\mu})^2} dX \\ &= \frac{1}{2}\Big[\mathrm{erf}(X_{b+1} - (-1)^x\sqrt{2\eta\mu}) \\ &\qquad - \mathrm{erf}(X_b - (-1)^x\sqrt{2\eta\mu})\Big] \end{aligned} \tag{7}$$

with the convention that $X_0 = -\infty$ and $X_d = +\infty$. We note that from Eq. (6) to Eq. (7) we have performed a change of the integration variable.

In the heterodyne case, we may define a partition of the phase space $\{\Lambda_b\}$ with d elements. The output probabilities can be written as

$$\begin{aligned} p^{(\mathrm{het})}(b|x) &= \frac{1}{\pi} \int_{\Lambda_b} e^{-(X-(-1)^x\sqrt{\eta\mu})^2} e^{-Y^2} dX dY \\ &= \frac{e^{-\eta\mu}}{\pi} \int_{\Lambda_b} r e^{-r^2+2r(-1)^x\sqrt{\eta\mu}\cos\theta} dr d\theta \end{aligned} \tag{8}$$

In the following we will analyse the achievable randomness by considering the above measurements. We will consider the cases with an increasing number of outcomes and we compare it with the results obtained with 2 outcomes and already reported in [15, 16].

III. RESULTS

A. Homodyne detection

We start by considering the Homodyne detection with perfect efficiency ($\eta = 1$). Due to the symmetry of the prepared states, the partition of the real axis is optimal when is symmetric around the origin. For instance, the configuration corresponding to 2, 3, 4 and 6 outcome are shown in table I and are illustrated in Fig. 3.

outcomes	X_0	X_1	X_2	X_3	X_4	X_5	X_6
2	$-\infty$	0	$+\infty$	/	/	/	/
3	$-\infty$	$-L_1$	$+L_1$	$+\infty$	/	/	/
4	$-\infty$	$-L_1$	0	$+L_1$	$+\infty$	/	/
6	$-\infty$	$-L_2$	$-L_1$	0	$+L_1$	$+L_2$	$+\infty$

Table I. Definition of the partitions of the real axis corresponding to different output configurations for the homodyne detection.

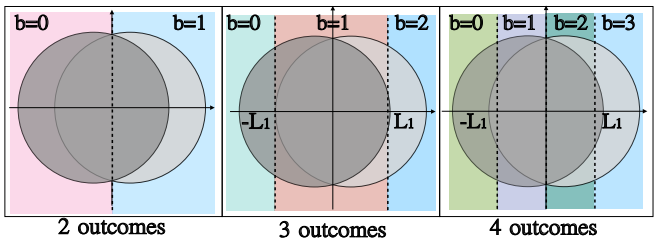

Figure 3. Homodyne measurement configurations.

The amount of extractable genuine random bits is estimated by numerically solving the dual of the SDP optimization problem given by Eq. (3), constrained by the conditional probabilities $p^{\text{hom}}(b|x)$, obtained from Eq. (7), together with the energy bound assumption μ. The results are further optimized over the values L_k. The value of the min-entropy as a function of the energy bound μ are shown in Fig. 7 for the 2, 4 and 6 outcome cases.

As shown in Fig. 7, by increasing the measurement outcomes the min-entropy monotonically increases over the entire range of μ, meaning that more randomness can be certified. It is worth to note that, starting from the same physical implementation (homodyne measurement) and changing the post-processing (namely by changing the partitions of the outcomes) different values of the min-entropy can be obtained.

One could ask what happens by further increasing the number of outcomes. As shown in Fig. 5, improvements

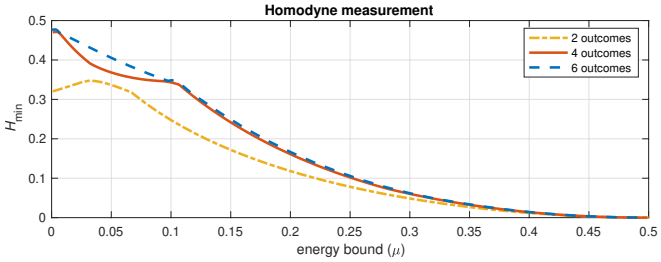

Figure 4. Min-entropy as a function of the energy bound μ for homodyne detection and different numbers of outcomes.

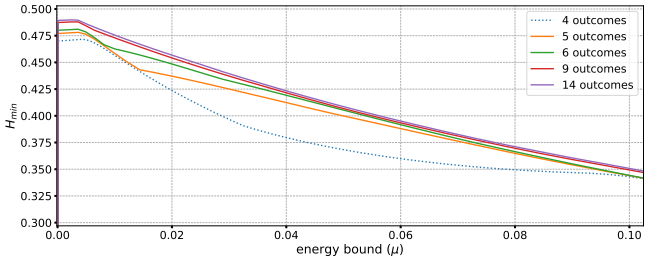

Figure 5. Min-entropy for large number of outcomes plotted for small μ values.

are obtained for small values of μ by increasing the number of outcomes up to 14. In Fig. 6 the best min-entropy (with optimized μ) is shown in function of the number of outcomes. The data suggest that larger min-entropy will be obtained by further increasing the number of outcomes towards a seemingly asymptotic value of 0.5.

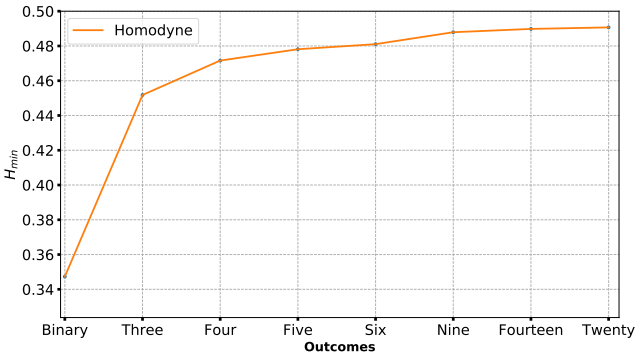

Figure 6. Maximum min-entropy (with optimized μ and $\eta = 1$) for the different number of outcomes for homodyne detection.

We now present the results obtained with inefficient system, namely by considering $\eta < 1$. This parameter η is used to model the effect of different experimental imperfections, such as the losses of the channel, the limited efficiency of the receiver's detectors or the electronic noise of the detection apparatus. We carried out the same analysis described above by considering different values of η. We show in Fig. 7 the min-entropy as a function of μ for different values of η and for 2 and 4 outcomes. The

corresponding optimal value of L_1 for the 4-outcome case are shown in Fig. 8. From the figures, it can be shown that when the efficiency decreases, the advantage of using more outcomes is less evident, but it is still present.

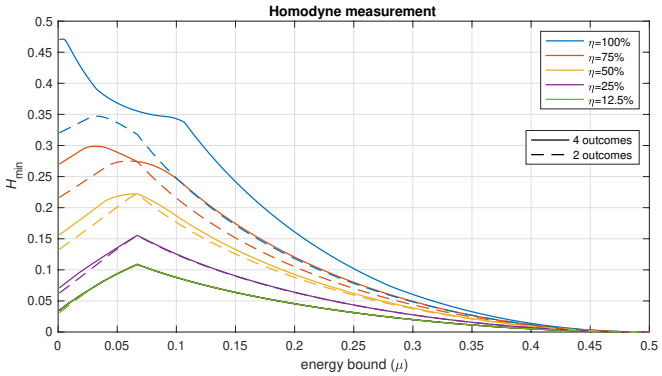

Figure 7. Min-entropy as a function of the energy bound μ for the homodyne detector. We compared the 2-outcome (dashed line) and 4-outcome (solid line) scheme, for different values of the efficiency η.

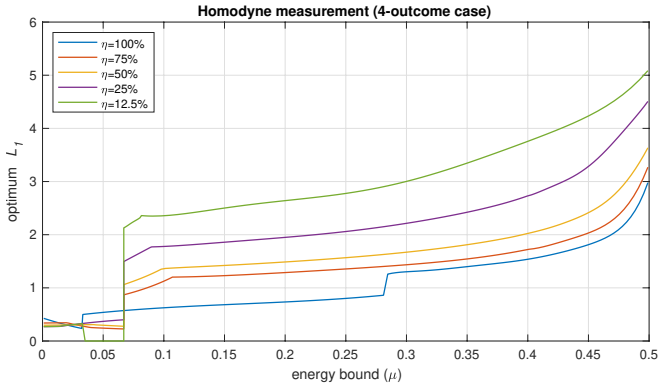

Figure 8. Optimal value of L_1 for the symmetric 4-outcome configuration for different system efficiency η.

B. Heterodyne detection

Homodyne detection is only sensitive to one field quadrature, e.g., X_ϕ sampling only a projection of the phase space. Heterodyne detection, on the other hands, performs a joint "noisy" measurement of two conjugated field quadratures, $\tilde{X}_\phi$ and $\tilde{P}_\phi$, thus sampling the entire phase-space. The number of possible (and potentially optimal) partitions for heterodyne detection is larger than homodyne, due to the increased dimensionality of the measurement.

Similar to homodyne, it is possible to choose a "strip" partition, namely the configuration illustrated in Fig. 3: the phase-space is subdivided in vertical strips whose boundaries are defined by the increasing real numbers $X_1 < X_2 < \ldots < X_{d-1}$. Looking at Eq. (7) and (8) it is possible to note that the heterodyne measurement with this configuration and efficiency η is equivalent to the homodyne measurement with efficiency $\eta/2$. Thus, we can directly refer to Fig. 7 for the results.

Other possible configurations are displayed in Fig. 9. By running the SDP for all the configurations represented in Fig. 9, we obtained a min-entropy that is always lower than the one obtained with the configuration shown in Fig. 3.

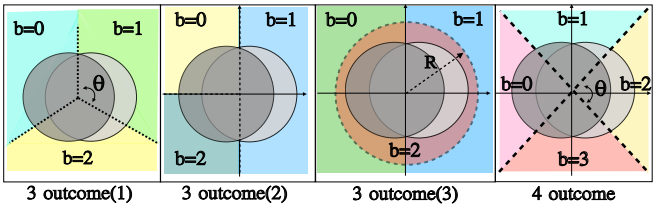

Figure 9. Alternative partitions of the phase space for Heterodyne measurement

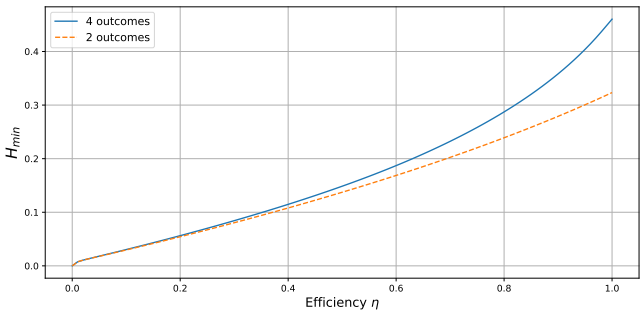

Figure 10. Min-entropy as a function of efficiency η for the homodyne detection concerning 2 and 4 outcomes configuration. The mean-photon number μ and range L are chosen in a way that the min-entropy is maximized.

IV. PRACTICAL CONSIDERATIONS

The main focus of this work is studying the influence of extending the number of outcomes on Semi-DI QRNG based on an energy bound and homodyne or heterodyne detection. We focused on homodyne and heterodyne detection because they are the most common measurement schemes employed in CV protocols. Moreover, recent experiments [15, 16], employed these measurements schemes to implement energy-bounded Semi-DI QRNG protocols. These works could benefit from this analysis, without any modifications to the experimental setup. In fact, the presented results show an enhancement of the certifiable min-entropy with respect to the binary case for ideal detection and no losses. However, we note that in practical implementations the expected improvement is reduced. In fact, additional losses, limited detector's

efficiency and excess noise of the receiver apparatus contribute to a reduction of the correlations $p(b|x)$, limiting the advantage of these schemes, as shown in Fig. 10.

We note that, as shown in Fig. 7, there is almost no improvement when the general inefficiency of the experiment η is lower than 12.5%. Any experimental realization that would like to exploit the advantage of many-outcome configuration should be designed in order to achieve high efficiency.

Although by the homodyne detection higher randomness can be certified with respect to heterodyne detection, the former it is susceptible to errors in the setting of the phase ϕ between the signal and the LO. Indeed, phase errors induces information loss in homodyne detection, whose magnitude depends on the active phase stabilization response time and precision. It is possible to show that a homodyne detection with phase error $\delta\phi$ is equivalent to a homodyne detection with no phase error and efficiency $\eta = |\cos(\delta\phi)|$. In Fig. 11 we show the optimal min-entropy for a 4-outcome homodyne detection as a function of the phase error. As an example, if the phase error is below 15°, the min-entropy may fluctuate between 0.47 and 0.4. On the other hand, heterodyne detection is robust with respect to phase error as long as the sampling rate is much larger than the phase drift: in the latter case, phase-compensations techniques can be used to track and correct phase fluctuations, with minimal impact on the min-entropy. As described in [16], for the heterodyne detection phase drifts can be compensated via software during the post-processing of the data (see also Fig.2 c).

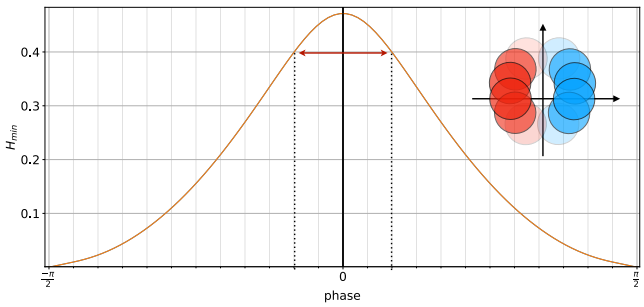

Figure 11. Optimal min-entropy as a function of phase error for 4-outcomes homodyne detection.

V. CONCLUSION

We have demonstrated a semi-DI QRNG with d-outcomes for binary-encoded optical coherent states based on heterodyne or homodyne detection. We compared our results with the binary-outcomes case, and we showed the number of certified random bits improves by increasing the number of outcomes. In this framework, we observed that the homodyne receiver beats the heterodyne receiver in terms of generated randomness. Numerically, we found an asymptotic upper bound of 0.5 as the number of random bit per measurement in the limit of infinite outcomes.

Moreover, in the heterodyne case we found the partition of the phase space into vertical "strip" allow an higher generation rate with respect to other configuration (see Fig. 7). Physically, this could be interpreted by a better discrimination between the two input states with the strip configuration compared to other phase-space partitions.

From previous analysis [24], it is known that the maximum entropy for binary input setup is $\log_2(3) \simeq 1.5849$, while our analysis seems to indicate that with homodyne and heterodyne measurement one can never exceed 0.5 bit of randomness per measurement. We leave for future works the formal proof of the above observation.

It is worth to note that the improvement is significant for perfect detection efficiency, while it decreases in case of losses. Hence, owning efficient and low-noise detectors is essential for exploiting d-outcomes configuration and obtaining higher randomness with respect to the binary-outcome setting. Finally, we illustrated how to apply the d-outcome configuration to the experimental data.

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).

Appendix A: Dual SDP

In the present section, we report how to dualize the primal form of SDP Eq.(3). The SDP duality gives an approach to upper bound the optimal value of maximization problems, or a lower bound for minimization problems [28]. The dual SDP has several advantages over the primal version. First, the dual optimization problem returns an upper-bound on the guessing probability, while the primal problem returns a lower-bound. Thus, even if the solver doesn't converge to the exact optimal point, the dual solution will never overestimate the true content of randomness, providing reliable bounds. Secondly, for real-time operation, the dual problem enables to recompute (sub-optimal) bounds without the need of running a full optimization, reducing the resources needed for the entropy estimation. Finally, in the dual problem the finite-size effects can be taken into consideration efficiently, thanks to the linear dependance of the $p(b|x)$ in the objective function. Note that in the real experiment,

the conditional probabilities $p(b|x)$ are calculated over finite raw data; thus, finite-size effects must be accounted for estimating the bound.

By using the Lagrangian duality [28], with an approach a similar to the one used in [11], the dualized SDP can be written as

$$P_g^* = \min_{H^{\lambda_0,\lambda_1},\nu_{bx}} [-\sum_{x=0,1}\sum_{b=0}^{d-1}\nu_{bx}p(b|x)] \tag{A1}$$

subjected to

$$\begin{aligned} &H^{\lambda_0,\lambda_1} = (H^{\lambda_0,\lambda_1})^\dagger, \\ &\sum_x \rho_x(\frac{1}{2}\sum_{b=0}^{d-1}\delta_{\lambda_x,b}+\nu_{bx}) \\ &\quad + H^{\lambda_0,\lambda_1} - \frac{1}{2}\mathrm{Tr}[H^{\lambda_0,\lambda_1}]\mathbb{1} \leq 0 \end{aligned} \tag{A2}$$

where $H_b^{\lambda_0,\lambda_1}$ are 2×2 Hermitian matrices.

As we can see, the objective function of dual SDP is a linear function of the conditional probability distribution $p(b|x)$, and the these are not appearing in the constraints. Hence, after solving the dual SDP one time and obtaining a valid set of parameters ν_{bx}^*, it is possible to obtain a (sub-optimal) bound for a new set of experimental probabilities $p(b|x)$, by evaluating the objective linear function with the set of parameters ν_{bx}^*. This estimation doesn't require the full optimization of the SDP, which can be slow and could limit the rate in real-time operation. A similar appproach is not possible with the primal version that needs to run full optimization of the SDP for every new set of $p(b|x)$.

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

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

[3] A. Acín and L. Masanes, "Certified randomness in quantum physics," Nature **540**, 213–219 (2016).

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

[5] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, "Device-independent quantum random-number generation," Nature **562**, 548–551 (2018), arXiv:1807.09611.

[6] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y. K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, "Experimentally generated randomness certified by the impossibility of superluminal signals," Nature **556**, 223–226 (2018).

[7] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín, "Unbounded randomness certification using sequences of measurements," Phys. Rev. A **95**, 020102 (2017).

[8] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, *et al.*, "Device-independent randomness expansion against quantum side information," arXiv preprint arXiv:1912.11159 (2019).

[9] M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, Y. Liu, Q. Zhao, Y. Peng, J. Zhang, Y. Zhang, W. J. Munro, X. Ma, Q. Zhang, J. Fan, and J.-W. Pan, "Experimental realization of device-independent quantum randomness expansion," (2019), arXiv:1902.07529 [quant-ph].

[10] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink, and E. Knill, "Experimental low-latency device-independent quantum randomness," Phys. Rev. Lett. **124**, 010505 (2020).

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

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

[13] T. Van Himbeeck and S. Pironio, "Correlations and randomness generation based on energy constraints," arXiv preprint arXiv:1905.09117 (2019).

[14] D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, "Self-testing quantum random-number generator based on an energy bound," Phys. Rev. A **100**, 062338 (2019).

[15] D. Rusca, H. Tebyanian, A. Martin, and H. Zbinden, "Fast self-testing quantum random number generator based on homodyne detection," Applied Physics Letters **116** (2020), 10.1063/5.0011479, arXiv:2004.08307.

[16] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Semi-device-independent heterodyne-based quantum random number generator," (2020), arXiv:2004.08344 [quant-ph].

[17] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, "Self-testing quantum random number generator," Phys. Rev. Lett. **114**, 150501 (2015).

[18] G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, "Exper-

imental quantum randomness generation invulnerable to the detection loophole," arXiv preprint arXiv:1410.3443 (2014).

[19] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," Nature Communications **9**, 5365 (2018).

[20] Z. Cao, H. Zhou, X. Yuan, and X. Ma, "Source-independent quantum random number generation," Phys. Rev. X **6**, 011020 (2016).

[21] D. G. Marangon, G. Vallone, and P. Villoresi, "Source-Device-Independent Ultrafast Quantum Random Number Generation," Physical Review Letters **118**, 060503 (2017).

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

[23] Z. Cao, H. Zhou, and X. Ma, "Loss-tolerant measurement-device-independent quantum random number generation," New Journal of Physics **17** (2015).

[24] M. Ioannou, J. B. Brask, and N. Brunner, "Upper bound on certifiable randomness from a quantum black-box device," Phys. Rev. A **99**, 052338 (2019).

[25] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover Hashing Against Quantum Side Information," IEEE Transactions on Information Theory **57**, 5524–5535 (2011).

[26] C. R. Müller, C. Peuntinger, T. Dirmeier, I. Khan, U. Vogl, C. Marquardt, G. Leuchs, L. L. Sánchez-Soto, Y. S. Teo, Z. Hradil, and J. Řeháček, "Evading vacuum noise: Wigner projections or husimi samples?" Phys. Rev. Lett. **117**, 070801 (2016).

[27] N. Walker, "Quantum theory of multiport optical homodyning," Journal of Modern Optics **34**, 15–60 (1987), https://doi.org/10.1080/09500348714550131.

[28] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex optimization* (Cambridge university press, 2004).