

Improving semi-device-independent randomness certification by entropy accumulation

Carles Roch i Carceller^{1,2,*}, Lucas Nunes Faria¹, Zheng-Hao Liu¹, Nicolò Sguerso¹, Ulrik Lund Andersen¹,

Jonas Schou Neergaard-Nielsen¹, and Jonatan Bohr Brask^{1,†}

¹Center for Macroscopic Quantum States (bigQ), Department of Physics, *Technical University of Denmark*, 2800 Kongens Lyngby, Denmark

²Department of Physics and NanoLund, *Lund University*, Box 118, 22100 Lund, Sweden



(Received 1 May 2025; accepted 4 August 2025; published 25 August 2025; corrected 30 September 2025)

Certified randomness guaranteed to be unpredictable by adversaries is central to information security. The fundamental randomness inherent in quantum physics makes certification possible from devices that are only weakly characterized, i.e., requiring little trust in their implementation. It was recently shown that the amount of certifiable randomness can be improved using the so-called entropy accumulation theorem generalized to prepare-and-measure settings. Furthermore, this approach allows a finite-size analysis which avoids assuming that all rounds are independent and identically distributed. Here, we demonstrate this improvement in semi-device-independent randomness certification from untrusted measurements.

DOI: [10.1103/dwdv-89bj](https://doi.org/10.1103/dwdv-89bj)

I. INTRODUCTION

Randomness is a fundamental resource [1] for a variety of applications in the modern world, including information security [2,3], simulations of physical systems [4–8], games, and gambling. Cryptographic protocols in particular require unpredictability relative to potential adversaries of the random numbers used to generate keys.

For pseudo-random number generators [9] and randomness generated from classical physical processes, certification of unpredictability requires assumptions about the information and computational power available to the adversaries. The inherent randomness of quantum measurements, on the other hand, enables randomness certification directly from fundamental physical laws and measurable properties of the devices used [10–13]. From a characterization of states and measurements on a given system, the entropy (quantifying unpredictability) relative to any adversary constrained by quantum mechanics can be bounded. In fact, by exploiting quantum nonlocality [14], the need for a thorough characterization can even be eliminated, allowing randomness certification in a black-box setting, provided the devices violate a Bell inequality [15–17]. This corresponds to a very strong level of security, known as device independence (DI), since minimal trust in the devices is required [18–22]. DI schemes, however, are also more technologically challenging to implement than device-dependent ones with

well-characterized devices. Hence, it is desirable to identify good trade-offs between ease of implementation and how little trust is required to certify randomness, i.e., to explore semi-DI quantum random number generators (QRNGs). A number of different prepare-and-measure schemes with fully uncharacterized sources [23–32] or measurements [33–41] have been explored. Other approaches present semi-DI protocols restricted by dimension [42–44], energy [45–48], contextuality [49] or overlaps between the state preparations [50]. The semi-DI protocol presented in work fits into the latter, i.e., the considered state preparations are partially characterized with a bound on their overlaps, leaving the measurement device as a black box.

Randomness in a variable b with respect to an adversary Eve is typically certified by bounding the capacity of this adversary of guessing b . Here, we look at a semi-DI prepare-and-measure scenario assuming only pure state preparations with bounded overlaps and untrusted measurements with b as measurement outcomes. Considering that Eve has bounded knowledge and control over the setup used to generate b , one can find certifiable bounds on Eve's guessing probability p_g which can be used to compute the min-entropy $H_{\min} = -\log_2(p_g)$ [51] of the measurement record. While the single-round min-entropy has served as a benchmark quantifier of randomness, it has been shown that one can bound the min-entropy of a sequence of outcomes in terms of the single-round Shannon entropy instead if the experiment runs over a large number of rounds [52]. This provides more randomness but the statement is valid only under the unrealistic assumption that all rounds are independent and identically distributed (i.i.d.). However, it has recently been shown that one can circumvent the i.i.d. limitation [53–56], in particular using the so-called entropy accumulation theorem (EAT) generalized to prepare-and-measure scenarios [54,55]. Despite its promising breakthrough in DI quantum cryptography, the EAT has found limited practical applicability in semi-DI QRNG frameworks. The main reason lies in the difficulty of finding the suitable

*Contact author: carles.roch_i_carceller@teorfys.lu.se

†Contact author: jonatan.brask@fysik.dtu.dk

Published by the American Physical Society under the terms of the *Creative Commons Attribution 4.0 International* license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI. Funded by *Bibsam*.

mathematical tools known as *min-trade-off* functions required to apply the EAT [57]. These are arbitrary affine functions on the observable frequencies which lower bound the von Neumann entropy. The difficulty of finding min-trade-off functions boils down to computing affine lower bounds on a nonlinear quantity such as the von Neumann entropy. Many works address this issue by computing the bounds on the min-entropy, which is far more accessible through semidefinite program techniques. Here, we address this issue by computing affine lower bounds on the Shannon entropy based on semidefinite programming duality.

In this work, we demonstrate a simple semi-DI QRNG to showcase the power of the EAT in prepare-and-measure scenarios. Based on semidefinite program duality, we present a method to produce min-trade-off functions and, together with the generalized version of the EAT applicable to prepare-and-measure scenarios, deal with finite size effects without assuming i.i.d. rounds. Here, we aim to certify randomness versus classically correlated eavesdroppers. Indeed, fundamental bounds on certifiable randomness require to consider eavesdroppers with access to the most powerful tools available in nature, i.e., quantum correlations. In reality however, harnessing nonlocal correlations from long-lived entanglement is extremely difficult with current technologies. Moreover, even if entanglement can be successfully generated, it needs to be stored in order to gather accumulated information after each experimental round. Thus, if the absence of quantum memories within the devices can be verified, quantum side information can be quickly ruled out [58]. Here, we assume we find ourselves in that case: we only allow classical side information in the sense that our randomness bounds are only valid for classically correlated eavesdropping entities. In the end, assuming the nature of the side information in a quantum randomness certification protocol is a matter of security setting. In quantum cryptography, for instance, with spatially separated communicating parties, a malicious third party has a wider margin to become entangled compared to a prepare-and-measure QRNG scenario, where all the action can be closed up in a microchip.

Our protocol is able to certify more than one bit of randomness per round from measurements on a single quantum state. We implement the scheme in a setup using time-bin encoded states and single-photon detection. The protocol employs a prepare-and-measure setup with three states and a single three-outcome measurement. The scheme is semi-DI in the sense that the only assumption on the source is a bound on the pair-wise overlap of the prepared states, and the measurement is completely uncharacterized. Randomness is extracted from one of the inputs, and the amount of certified randomness achievable with the generalized EAT is compared with the traditional min-entropy approach. The other two inputs enable self-testing the device, by exploiting that the setup can also be interpreted in terms of a state discrimination task.

In quantum state discrimination [59–61], a measurement device aims to determine which state out of a known set was prepared, subject to certain constraints. In unambiguous state discrimination (USD) [62–64], the error rate is nullified, at the cost of adopting an additional measurement event which gives no information on which state was prepared (formally called an inconclusive event). The minimum attainable rate of

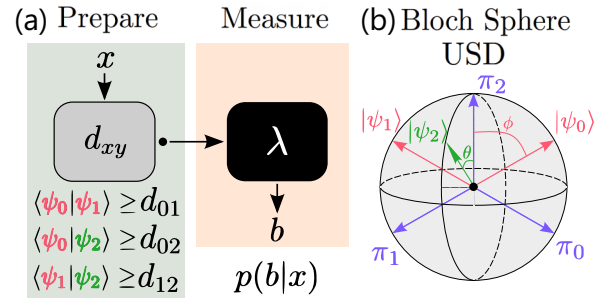


FIG. 1. (a) Sketch of the semi-device-independent prepare-and-measure scenario with three preparations and one untrusted measurement (black box). (b) The USD protocol is illustrated on the Bloch sphere, with Bloch vectors corresponding to the prepared states $|\psi_x\rangle$ (red and green) and POVM elements π_b (blue).

inconclusive events in USD is given by a rank-1 (hence extremal) and unique measurement, which benefits the amount of certifiable randomness on the measurement outcome. While a setup with two preparations ($x = 0, 1$) is sufficient for QRNG, we add a third state preparation ($x = 2$) such that all outcomes are equally distributed when Alice selects $x = 2$. The key idea is then that, to be able to reproduce the observable statistics for inputs $x = 0, 1$, Eve must perform the USD measurement. Therefore, when Alice selects $x = 2$, Eve's chances of guessing the outcome become minimal. Here, we implement a protocol which uses USD during the self-test rounds, allowing us to make use of the additional inconclusive event in two-state discrimination to reach randomness values greater than one bit per round. Then, we choose a third state that yields equiprobable outcomes when involved in the state discrimination scenario.

The remainder of the paper is organized as follows. In Sec. II, we introduce the state discrimination scenario and specify the measurement strategy. Later, we explain how we evaluate the randomness, continue with the main semi-device-independent assumptions we consider, and explain how we deal with finite size effects assuming i.i.d. and non-i.i.d. rounds. We end the section by experimentally implementing the protocol in an optical platform using coherent states of light. In Sec. III we present the results we observe both in the experiment and in simulations. We end the paper with Sec. IV, concluding our work and outlining the main result.

II. METHODS

A. Prepare and measure

In order to illustrate the main idea of the protocol, consider the scenario in Fig. 1(a), where one party (namely, Alice) owns a device that receives inputs $x \in \{0, 1, 2\}$ with prior probabilities p_x and prepares the following pure quantum states:

$$\begin{aligned} |\psi_0\rangle &= \cos \frac{\phi}{2} |0\rangle + \sin \frac{\phi}{2} |1\rangle \\ |\psi_1\rangle &= \cos \frac{\phi}{2} |0\rangle - \sin \frac{\phi}{2} |1\rangle, \end{aligned} \quad (1)$$

and a third qubit state $|\psi_2\rangle$ which shall remain unspecified for now. These states are sent to a second party (namely, Bob)

who owns a device which will perform a measurement described by the positive operator-valued measure (POVM) $\{\pi_b\}$ for $b \in \{0, 1, 2\}$. Over many rounds of the experiment, one can estimate the conditional probability distribution $p(b|x) = \text{Tr}[\rho_x \pi_b]$, for $\rho_x = |\psi_x\rangle\langle\psi_x|$.

Our first task is to find Bob's optimal measurement, according to a particular state discrimination protocol, to identify whether Alice prepared $x = 0$ or $x = 1$, ignoring the third possible input $x = 2$. This will yield correlations reproducible only with extremal and unique POVMs. The idea is to properly design a state $|\psi_2\rangle$ such that, with that optimal measurement, all outcomes are equiprobable whenever that state is prepared [i.e., $p(b|x = 2)$ are equal $\forall b$]. We take optimality to be set by USD, i.e., a measurement that minimizes the rate of inconclusive events (here labeled by $b = 2$) given zero error rate. Correlations drawn from optimal USD measurements are extremal and unique, which means that they cannot be decomposed by any convex combination of other POVMs and no other measurement can reproduce the same probabilities, up to unitary rotations.

B. Unambiguous state discrimination

The task in USD is to identify which state was prepared without making any errors, i.e., $p_{\text{error}} := p_0 p(1|0) + p_1 p(0|1) = 0$ [62–64]. That can be done if one pays the price of having some rounds in which the measurement result turns inconclusive. In the present case, USD targets preparations $x = 0$ and $x = 1$, and the inconclusive events will be labeled with $b = 2$. The goal of USD is to minimize the rate of inconclusive events $p_{\text{inc}} := p_0 p(2|0) + p_1 p(2|1)$. In two-state discrimination, the minimum p_{inc} is proportional to the overlap of the prepared states, which in our scenario is $|\langle\psi_0|\psi_1\rangle| = \cos\phi$, according to (1). In this case, the minimum p_{inc} is lower bounded by [65]

$$p_{\text{inc}} \geq 2\sqrt{p_0 p_1} \cos\phi. \quad (2)$$

The POVM that represents an optimal USD measurement must be given by rank-1 POVM elements, proportional to the projectors onto the orthogonal states of $|\psi_0\rangle$ and $|\psi_1\rangle$. Concretely, for equiprobable preparations $p_0 = p_1 = 1/2$,

$$\begin{aligned} \pi_0 &= \frac{1}{1 + \cos\phi} |\psi_1^\perp\rangle\langle\psi_1^\perp| \\ \pi_1 &= \frac{1}{1 + \cos\phi} |\psi_0^\perp\rangle\langle\psi_0^\perp| \\ \pi_2 &= \mathbb{1} - \pi_0 - \pi_1, \end{aligned} \quad (3)$$

where $\langle\psi_x|\psi_x^\perp\rangle = 0$. Consider now a third preparation $x = 2$. We aim to find a state $|\psi_2\rangle$ which triggers all three outcomes $b = 0, 1, 2$ of the measurement in (3) with the same probability. That means, it must satisfy $\langle\psi_2|\pi_b|\psi_2\rangle = 1/3 \forall b$. As illustrated on the Bloch sphere in Fig. 1(b), a good candidate is the state

$$|\psi_2\rangle = \cos\frac{\theta}{2} |0\rangle + i \sin\frac{\theta}{2} |1\rangle. \quad (4)$$

The three outcomes will be equiprobable when

$$\cos\theta = \frac{1 - 2\cos\phi}{3\cos\phi}. \quad (5)$$

Since $-1 \leq \cos\theta \leq 1$, this condition can only be satisfied for $\cos\phi \geq 1/5$, meaning that equiprobable outcomes in this setting are only achievable in that range. One can then use these equiprobable outcomes, which are only reproducible through a unique and extremal POVM in a qubit space, to improve the randomness certification. Note, though, that this is only true for qubit states. In semi-DI randomness certification, one wants to keep the number of assumptions at a minimum. We will later show how we can get rid of the assumption of a fixed dimension.

C. Randomness certification

We proceed to explain how we certify randomness in the measurement outcomes, relative to a classically correlated adversary Eve. Eve has knowledge of the preparation (x) and measurement device, and can share classical correlations with the measurement according to the distribution $q(\lambda)$. We begin by explaining how we certify single-round randomness using the min-entropy. Then, we bound the Shannon entropy in order to leverage the power of the EAT to accommodate the finite-size effects from experimental data.

Min-entropy: We certify randomness only from rounds where state $|\psi_2\rangle$ is prepared. The rounds where states $|\psi_0\rangle$ and $|\psi_1\rangle$ are prepared can be thought of as self-test rounds. During the rounds where $|\psi_2\rangle$ is prepared, Eve's guessing probability averaged through each round can be written as

$$p_g = \sum_{\lambda} q(\lambda) \max_b \{p(b|x = 2, \lambda)\}, \quad (6)$$

with $p(b|x, \lambda) = \text{Tr}[\rho_x \pi_b^\lambda]$ ($\rho_x = |\psi_x\rangle\langle\psi_x|$) being the probability that the measurement outcome is b given state preparation x and the measurement strategy λ .

We aim to find an upper bound on p_g in (6) over all strategies of Eve, i.e., all distributions $q(\lambda)$ and measurements π_b^λ , subject to reproducing the observed statistics on average $p(b|x) = \sum_{\lambda} q(\lambda) \text{Tr}[\rho_x \pi_b^\lambda]$. This optimization problem can be rendered as a semidefinite program [66]. As we detail in Ref. [67], we can write Eve's guessing probability as

$$p_g = \sum_{\lambda} \text{Tr}[\rho_2 M_{\lambda}^\lambda]. \quad (7)$$

An upper bound $p_g^* \geq p_g$ can be found by maximizing (7) over all positive semidefinite $D \times D$ matrices M_b^λ that fulfill the constraints

$$\sum_b M_b^\lambda = \frac{1}{D} \text{Tr}\left[\sum_b M_b^\lambda\right] \mathbb{1} \quad \forall \lambda, \quad (8)$$

$$p(b|x) = \sum_{\lambda} \text{Tr}[M_b^\lambda \rho_x] \quad \forall b, x, \quad (9)$$

where D is the eavesdropper's dimension. The randomness of the measurement outcomes is quantified through the min-entropy $H_{\text{min}} = -\log_2(p_g)$, which gives the number of (almost) uniformly random bits which can be extracted per round of the protocol [51].

Shannon entropy. Due to the nonlinear nature of the Shannon entropy, it is very difficult to find linear schemes that provide tight numerical bounds in single-party prepare-and-measure scenarios. For example, in Ref. [47] the authors

design a hierarchy of semidefinite programs to bound the Shannon entropy in scenarios with energy-restricted correlations. Here, our correlations are bounded by a constraint on the overlaps and thus, we find the following method more suitable. As shown in Ref. [68], applying the Gauss-Radau quadrature to an integral representation of the logarithm yields a variational upper bound for the quantum relative entropy $D(\rho||\sigma) := \text{Tr}[\rho(\log_2 \rho - \log_2 \sigma)]$. This can be related to the von Neumann entropy, and consequently to the Shannon entropy for classically correlated eavesdroppers. In Ref. [67] we show how to use this technique to derive the bound on the conditional Shannon entropy $H(B|E, x = 2) \geq H^*$ for

$$H^* = c_m + \sum_{i=0}^{m-1} \max_i \left\{ \sum_{b,x} -v_{bx} p(b|x) - \text{Tr}[R] \right\}, \quad (10)$$

where we introduced $c_m := \sum_{i=1}^{m-1} \tau_i$ with $\tau_i := \omega_i/[t_i \log_2(2)]$ for $\{t_i, \omega_i\}$ being the nodes and weights, respectively, corresponding to the Gauss-Radau quadrature. The maximization runs for each iteration of i over the set of scalars v_{bx} and $D \times D$ matrices R that satisfy

$$\sum_a E_b^a = \sum_x \rho_x v_{bx} + R \quad (11)$$

$$F_b^a + F_b^{a\dagger} = 2\tau_i \rho_2 \delta_{a,b} + Q^a - \frac{1}{d} \text{Tr}[Q^a] \mathbb{1} \quad (12)$$

$$L_b^a = \tau_i \rho_x [(1-t_i)\delta_{a,b} + t_i] + P^a - \frac{1}{d} \text{Tr}[P^a] \mathbb{1}, \quad (13)$$

with Q^a and P^a being $D \times D$ matrices and E_b^a , F_b^a , and L_b^a being blocks of $D \times D$ matrices that built the following positive semidefinite matrix:

$$\begin{pmatrix} E_b^a & F_b^a \\ F_b^{a\dagger} & L_b^a \end{pmatrix} \geq 0. \quad (14)$$

Any feasible point that fulfills all constraints specified above represents a valid lower bound on the Shannon entropy.

D. Semi device independence

We consider frameworks with the lowest device characterization possible in a semi-device-independent manner. Concretely, we consider that the measurement device is completely uncharacterized, and assume pure state preparations with known overlaps. For two pure state preparations, this allows using two fixed qubit states in the semidefinite program without loss of generality, because unitary rotations of the state pair will not affect the optimum, and Eve will not gain any extra information by extending the measurements beyond the two-dimensional span of the pair [46]. In our case we consider three pure states, which means that Eve's maximal useful dimensionality will not exceed a qutrit space. Hence, we need to assume that the three prepared states span a three-dimensional space. That is, the third state is

$$|\tilde{\psi}_2\rangle = \sqrt{a}|\psi_2\rangle + \sqrt{1-a}|2\rangle, \quad (15)$$

for $|\psi_2\rangle$ in (4) having support on the bidimensional space spanned by $|\psi_0\rangle$ and $|\psi_1\rangle$ in (1), and $|2\rangle$ having only support on an additional orthogonal dimension, such that $\langle\psi_x|2\rangle = 0 \forall x$. One can see that if both overlaps $|\langle\tilde{\psi}_2|\psi_0\rangle|^2$

and $|\langle\tilde{\psi}_2|\psi_1\rangle|^2$ are simultaneously fixed to be

$$|\langle\tilde{\psi}_2|\psi_0\rangle|^2 = |\langle\tilde{\psi}_2|\psi_1\rangle|^2 = \frac{1}{2}(1 + \cos\phi \cos\theta), \quad (16)$$

then the normalization in (15) imposes $a = 1$, and all three preparations must have support on a qubit space. However, strict equalities can be hard to satisfy in the laboratory. In Ref. [67] we show how one can relax this assumption to lower bounds on the overlaps $|\langle\psi_x|\psi_y\rangle| \geq d_{xy}$. This, in turn, bounds the access of the eavesdropper to an additional third dimension, as a fulfills

$$a \geq \frac{d_{02}^2 + d_{12}^2 - 2d_{01}d_{02}d_{12}}{1 - d_{01}^2}. \quad (17)$$

Also, since $a \leq 1$, one also finds the following relation:

$$1 \geq d_{02}^2 + d_{12}^2 + d_{01}^2 - 2d_{01}d_{02}d_{12}, \quad (18)$$

which must hold true for any dimension. Equation (17) defines the surface of an inflated tetrahedron with curved faces (see Ref. [67]). The amplitude a decreases toward the center of the tetrahedron. Thus, in other words, bounding $|\langle\psi_x|\psi_y\rangle| \geq d_{xy}$ implies that we forbid Eve to access the interior of the tetrahedron.

This semi-DI characterization allows us to compute the certifiable randomness beyond the two-qubit case and avoid direct dimensional constraints. In our implementation, we employ coherent states of light as pure state preparations. We control the pairwise overlaps of the preparation and use (17) to bound their support outside a two-dimensional subspace.

E. Finite-size effects—i.i.d. vs entropy accumulation

In actual experiments, probabilities are estimated from frequencies. Due to the finite number of data points, the observed frequency of events $\text{freq.}(b|x) = n_{bx}/n_x$ for n_{bx} denoting the total number of events b given a state preparation x does not exactly represent the true conditional probability $p(b|x)$. To deal with finite-size effects, we take two different approaches.

First, we assume that all rounds from the experiment are considered to be independent and identically distributed. Under this assumption, we recall the asymptotic equipartition property (AEP). The AEP establishes that the output of a random experiment is certain to come from the typical set, under the limit of large number of repetitions. In Ref. [52] a generalization of the AEP to quantum theory is developed, establishing that the *smooth min-entropy* $H_{\min}^\varepsilon$ (i.e., the maximum min-entropy for any state ε close to a fixed state [69]) converges to the conditional von Neumann entropy up to an error term. Our case simplifies this statement to the Shannon entropy, because only classical side information is considered here. Specifically,

$$\frac{1}{N} H_{\min}^\varepsilon(B^N|E^N, x = 2) \geq H^* - \frac{\delta}{\sqrt{N}}, \quad (19)$$

with $H_{\min}^\varepsilon(B^N|E^N, x = 2)$ being the smooth min-entropy accumulated over a total of N experimental rounds for a particular preparation $x = 2$, and δ a parameter specified in Ref. [67]. By H^* we denoted a lower-bound on the single-round Shannon entropy assuming i.i.d. for a particular set of observable statistics, which can be estimated from (10).

Next, we go beyond the i.i.d. assumption and perform a second characterization of finite size effects. In this case, we use the EAT generalized to prepare-and-measure scenarios [54,55], which allows us to quantify the amount of entropy accumulated per round also when they are not i.i.d.. The EAT places a bound on the conditional smooth min-entropy, which depends only on the von Neumann entropy per round plus a correction term which depends on the total number of rounds in the experiment. Every round of the experiment is described by a channel $\mathcal{M}_i$ which maps Bob's (B_i) and Eve's (E_i) systems to their corresponding systems in the next round (B_{i+1} and E_{i+1} , respectively). To make the EAT applicable in our experiment, we assume a no-signaling constraint between Bob's and Eve's devices which can be straightforwardly justified thanks to the classical nature of side information. The marginal of the new side information E_i without the new output B_i must be reproducible only with past side information E_{i-1} (i.e., any new E_i should depend on past E_{i-1} alone). This forbids that Eve's information E_i is passed along Bob's systems B_{i-1} , which would mean that, in some cases, E_{i-1} holds no information on Bob's outcome but E_i does. It follows from assuming classically correlated eavesdroppers that any state Eve and Bob may share is separable and thus, the nonsignaling condition is ensured by sealing the laboratory during the prepare-and-measure rounds. In Ref. [67] we explain in more detail how we apply the EAT to our results to certify the randomness outside the i.i.d. assumption. Concretely, we are able to bound the smooth min-entropy on the measurement outcome using the single-round Shannon entropy plus a correction term, i.e.,

$$\frac{1}{N} H_{\min}^{\varepsilon}(\mathcal{B}^N | E^N, x=2) \geq \min f_{\min}(\text{fq.}(b|x)) - \mathcal{O}\left(\frac{1}{\sqrt{N}}\right), \quad (20)$$

where $f_{\min}[\text{fq.}(b|x)] \leq H^*$ is a so-called *min-trade-off* function, i.e., an affine function on the observable frequencies $\text{fq.}(b|x)$ which lower bounds the minimum Shannon entropy H^* . This function can be directly taken from the objective function of the dual semidefinite program in (10), replacing the ideal probabilities $p(b|x)$ with the observable frequencies, i.e.,

$$f_{\min}[\text{fq.}(b|x)] = c_m - \sum_{i=0}^{m-1} \sum_{b,x} v_{bx}^i \text{fq.}(b|x) + \text{Tr}[R^i], \quad (21)$$

where v_{bx}^i and R^i are the feasible values that maximize the objective function in (10) (see Ref. [67] for details).

Finally, to extract the randomness from the whole sequence of Bob's outcomes, we use a randomness extractor. Here, we shortly introduce the meaning of this function and the main result we use in this work. For a more detailed explanation refer to Ref. [55]. Consider $H_{\min}^{\varepsilon}(\mathcal{B}^N | E^N) \geq h$. A quantum-proof strong $(h, \varepsilon_{\text{EXT}})$ extractor is defined as a function EXT that receives a quantum state $\rho_{BE} \otimes \tau_S$ and acts on the classical systems B and S with dimension equal to $n_B \times n_S$ bits. The l -bit dimensional output $\text{EXT}(\rho_{BE} \otimes \tau_S)$ is $\tilde{\varepsilon}_{\text{EXT}}$ close to $\tau_L \otimes \rho_E \otimes \tau_S$. Here, τ_L and τ_S are maximally mixed states of dimension 2^{n_S} and 2^l , and ρ_{BE} is the classical-quantum state shared by Bob and Eve after the measurement. The input

in system S is called the seed of the extractor. The security parameter of this extractor is given by $\tilde{\varepsilon}_{\text{EXT}} := \varepsilon_{\text{EXT}} + 4\varepsilon$, which can be arbitrarily chosen. Furthermore, there exists a quantum-proof strong $(h, \varepsilon_{\text{EXT}})$ extractor from which we can extract a total of $l \leq h - 2\log_2(1/\varepsilon_{\text{EXT}})$ random bits [69]. In all results from this work we consider $\varepsilon_{\text{EXT}} = 10^{-8}$, which implies an additional correction of $\sim -26/N$ in the extractable randomness per round.

F. Implementation

We implement the protocol using time-bin encoded coherent states and single-photon detection. Our approach is inspired by previous works in similar settings [48,50]. The setup is illustrated in Fig. 2. In the following, we detail its working principle.

Our photon source is a 1550.32-nm continuous-wave laser. We use an electro-optic modulator (EOM) and two acousto-optic modulators (AOMs) to carve the output of the laser into 10-ns-width pulsed coherent states with appropriate amplitude. We alternate the experiment setup between a locking phase and a randomness-generation stage. During the randomness-generation stage, the two AOMs together induce a stable attenuation of 77 dB to bring the laser power down to single-photon level. This attenuation is removed during the locking stage to monitor the transmission power of the EOM and correctly set up its bias voltage. In doing so, we achieve a dark count rate of only $p_{\text{dc}} = (4.5 \pm 2.8) \times 10^{-6}$ per pulse. The EOM, on the other hand, generates the correct amplitudes for the input states during a 10-ns time window, which is chosen as the duration of the time bin. In each round, the pulses can emerge in an early or a late time bin. The two self-testing states for $x=0$ and $x=1$ are prepared using a coherent state with amplitude α in the early and late bins, respectively. We write this as $|\psi_0\rangle = |\alpha 0\rangle$ and $|\psi_1\rangle = |0\alpha\rangle$. On the other hand, the third state, $x=2$, used for randomness extraction is prepared using amplitude β in both early and late bins, $|\tilde{\psi}_2\rangle = |\beta\beta\rangle$. The early and late pulses are separated by 800 ns and the full protocol runs at a 0.526-MHz rate. To ensure high efficiency of the photodetection, we optimize the polarization state of the photons with a fiber polarization controller before the superconducting detector and splice all the fiber connection points in the measurement stage to minimize the photon loss.

The measurement is performed by a superconducting single-photon detector (ID Quantique ID281) with a quantum efficiency of 94% which detects photons from the carved, attenuated laser beam. The values for α and β are calibrated calculating the click rate related to the coherent states. Further, we have introduced a feedback control loop to stabilize the output power of the EOM to stabilize the coherent state amplitudes throughout the experiment. From the measured counting rates, we deduce the coherent state amplitude we sent to be $\alpha_L = 0.401 \pm 0.007$ and $\beta_L = 0.641 \pm 0.006$. Here, the 1σ standard deviations are caused by the residual intensity fluctuations across the data collection time of the entire experiment.

The outcome b is determined by in which time bin the detector clicks. We label events with clicks in only the early time bin by $b=0$, events with clicks only in the late time bin by $b=1$, events with no clicks in either bin by $b=2$, and

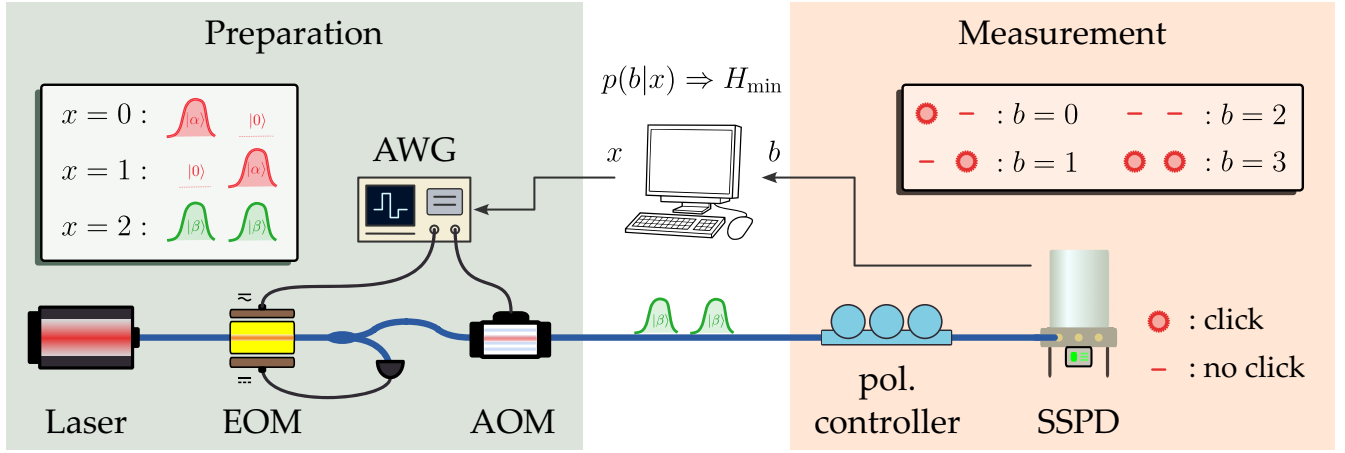


FIG. 2. Experimental implementation. The time-bin-encoded input states are generated by an EOM and a pair of AOMs (only one shown in the figure). The feedback control at the EOM stabilizes the amplitude of the pulsed weak coherent states. After optimizing the polarization (pol. controller), the pulses are sent to the superconducting single-photon detector (SSPD). From the statistics of preparations and detector counts, randomness is extracted and certified.

events with clicks in both bins by $b = 3$. The fourth outcome does not trigger during the self-test rounds and thus is not relevant in our framework. Therefore, as discussed in Ref. [67], the outcome $b = 3$ is binned with the first two, leaving the measurement effectively with three outcomes. Using the measurement setup, in a calibration step, we also determine the AOM and EOM voltages required to prepare coherent states $|\alpha\rangle$ and $|\beta\rangle$ with the desired overlap.

In order to reduce finite size effects, we take around 10^7 rounds of measurements over 11 distinct iterations. After gathering every 10^7 round of data on each iteration, we perform a calibration measurement before taking the data again. The fluctuation of the count rate, measured by the standard deviation across all experiment runs, is only 1.52% relative to the average value, certifying the consistency between the states prepared at different times.

III. RESULTS

In order to find optimal experimental settings, we first simulate the system, computing the randomness for varying coherent-state amplitudes. In Fig. 3 we show the min-entropy under realistic conditions (including loss and detector dark counts). The results show maximal min-entropy around the amplitudes $\alpha_T = 0.4$ and $\beta_T = 0.66$, which we therefore target in the experiment. This corresponds to states $|\psi_x\rangle$ with overlaps $|\langle\psi_0|\psi_1\rangle| = 0.84$ and $|\langle\psi_0|\tilde{\psi}_2\rangle| = |\langle\psi_1|\tilde{\psi}_2\rangle| = 0.78$. We note that these fulfill the criterion $|\langle\psi_0|\psi_1\rangle| \geq 1/5$ deduced from (5) for the possibility of equiprobable outcomes. These preparations should thus allow correlations yielding high values of randomness. We additionally run the semidefinite program optimization method to efficiently compute direct bounds on the Shannon entropy using the exact same realistic settings. Comparing with the min-entropy results, we find a marked increase in the certifiable randomness, as well as a vast expansion of the usable parameter region. Although the optimal randomness in this case is not exactly given by the targeted amplitudes α_T and β_T , we keep them

to directly compare the best possible certifiable randomness using the min-entropy vs the Shannon entropy.

The overlaps constrain support outside the span of $|\psi_0\rangle$ and $|\psi_1\rangle$ but do not eliminate it. Specifically, the minimal amplitude introduced in (15) is $a \geq 0.66$ on the targeted coherent amplitudes. Moreover, the conditional probability $p(b|2)$ does not depend on α . However, we do see some dependency on α in the randomness in Fig. 3, which becomes more evident for higher values of β . The fact that $a < 1$ for our amplitudes is mainly due to that dependency and also implies that the correlations are not reproducible only by unique and extremal POVMs. This reduces the secrecy of the outcome, decreasing the certifiable randomness. Nevertheless, we are able to find a set of amplitudes where, although Eve has unbounded dimensionality, her guessing probability is lower than $1/2$, i.e., more than one bit of randomness is certified using the min-entropy and even more with the Shannon entropy.

We run the experiment through the proposed implementation and evaluate the randomness for a single configuration of targeted amplitudes. We show the obtained results in Fig. 3 (right-side plots). The experimental data we collected indicate that the actual amplitudes used in the laboratory were $\alpha_L = 0.401 \pm 0.007$ and $\beta_L = 0.641 \pm 0.006$. Our observations agree well with the predictions from the simulations, and show a randomness extraction rate of 1.304 ± 0.002 and 1.299 ± 0.002 bits per round after 10^7 runs of the experiment, when analyzed assuming i.i.d. experiment rounds using the AEP and without i.i.d. rounds using the EAT, respectively. Additionally, we compute the raw min-entropy per round without taking into account finite size effects and, using the experimental data, we obtain 1.11 ± 0.02 bits of randomness per round. All error bars (also shown in Fig. 3) are the standard deviation obtained over running the experiment 11 different times. We observe approx. 19% improvement in the certifiable randomness by using the Shannon entropy (which is computed in the AEP and EAT approaches) compared to the min-entropy. Also, the estimated errors using the AEP and EAT approaches are lower than the min-entropy approach by one order of magnitude. This is mainly because the Shannon

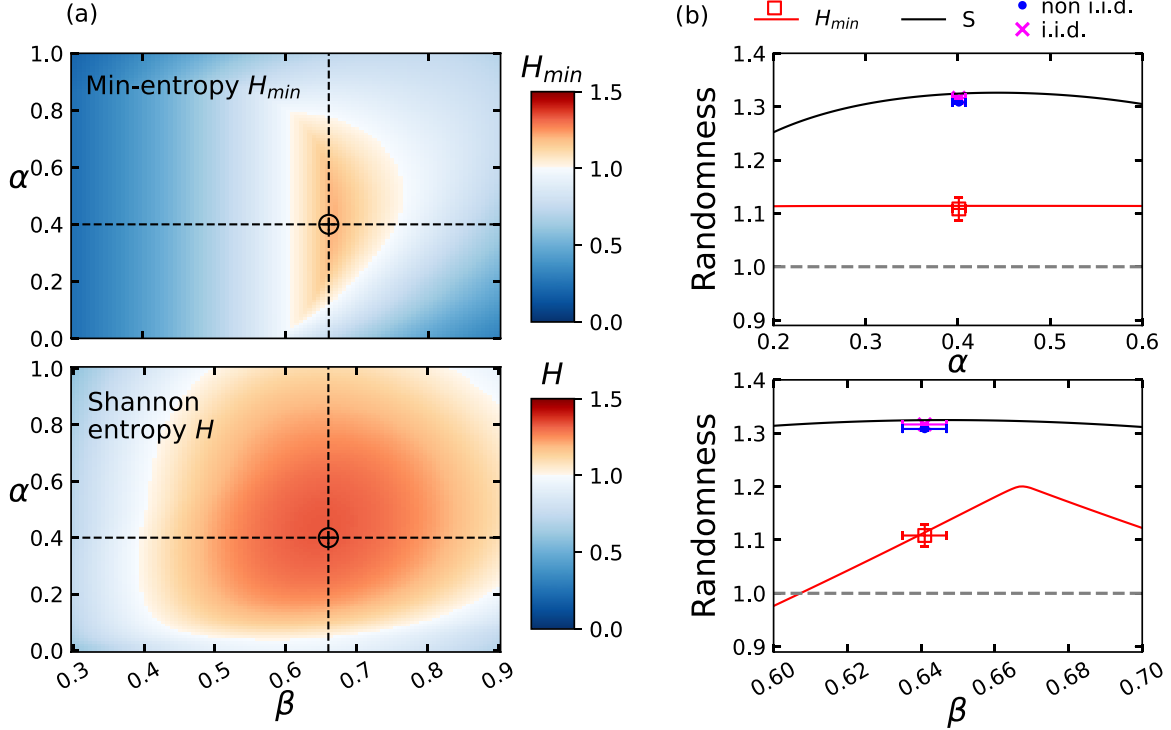


FIG. 3. (a) Bound on the raw min and Shannon entropies (i.e., without accounting for finite size effects) as a result of the semidefinite programs presented in Sec. II C for a limited range of coherent amplitudes. Red regions denote more than one bit of randomness per round. The targeted amplitudes $\alpha_T = 0.4$ and $\beta_T = 0.66$ are denoted with black-dashed lines. (b) Slice of the color plots at the chosen amplitudes. We compare the raw min-entropy, the Shannon entropy, and the certifiable randomness through the AEP (i.i.d.) and generalized EAT (non-i.i.d.). The results of the experiment are shown in a cross/circle/square with their corresponding error bars. The chosen parameters are $m = 8$, $\varepsilon = 10^{-8}$ with photon loss $1 - \eta = 0.06$, dark count probability of $p_{dc} = 10^{-6}$, and total number of samples $N = 10^7$ over 11 distinct repetitions.

entropy is more stable than the min-entropy against fluctuations on the coherent amplitudes. Furthermore, the reason behind the almost-equivalence between the i.i.d. and non-i.i.d. value is the high amount of samples gathered in the experiment (around 10^7), which foresees the convergence of the EAT to the AEP in the limit of infinite number of experimental rounds. In Fig. 4 we additionally collected random subsets between 10^3 and 10^7 data points from the 11 different gathered experimental data sets and computed the randomness using the raw min-entropy, i.i.d. (AEP), and non-i.i.d. (EAT) approaches. Observe that the total of 10^7 experimental rounds lies close to the asymptotic limit. Nevertheless, note that the non-i.i.d. approach is still able to certify more randomness than the raw min-entropy down to approximately 3.8×10^4 samples.

IV. CONCLUSION

We have realized a semi-DI randomness generation protocol implemented in an optical platform, as shown in Fig. 2. By exploiting the entropy accumulation theorem generalized to prepare-and-measure scenarios, we bound the certifiable randomness in terms of the single-round Shannon entropy without assuming that experimental rounds are independent and identically distributed and including finite-size effects. We proposed a method for bounding the Shannon entropy in our semi-DI framework based on overlap assumptions. This

consists in expanding the logarithm function on its integral form using the Gauss-Radau quadrature, i.e., employing the methods from Ref. [68] to derive bounds on the von Neumann entropy and imposing classical side information. We show that this allows certifying more randomness than a standard approach bounding the single-round min-entropy under an i.i.d.

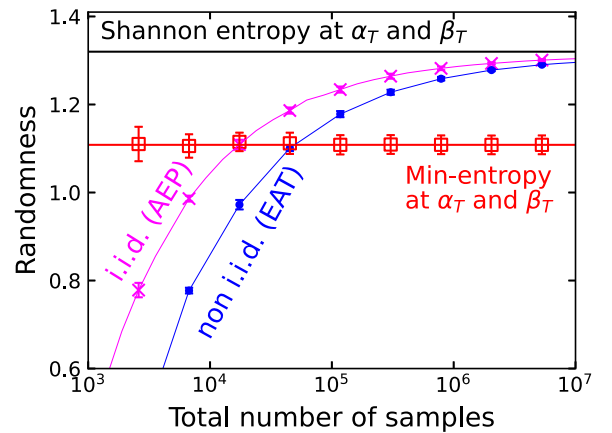


FIG. 4. Scaling of i.i.d. and non-i.i.d. bounds with the number of rounds in the experiment. In our experiment we took $\sim 10^7$ samples, which explains the almost-equivalency between both approaches in our results.

assumption and neglecting finite-size effects. Thus, we certify more randomness under much less restrictive assumptions.

ACKNOWLEDGMENTS

C.R.C. is supported by the Wenner-Gren Foundation. We gratefully acknowledge support from the Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNR142), VILLUM FONDEN (Research Grant No.

40864), the Carlsberg Foundation CF19-0313, Innovation Fund Denmark (PhotoQ project, Grant No. 1063-00046A), the Horizon Europe MSCA (Project GTGBS [70], Grant No. 101106833), and a DTU-KAIST Alliance Stipend.

DATA AVAILABILITY

The data that support the findings of this article are openly available [71].

-
- [1] B. Hayes, Randomness as a resource, *Am. Sci.* **89**, 300 (2001).
 - [2] C. E. Shannon, Communication theory of secrecy systems, *Bell Syst. Tech. J.* **28**, 656 (1949).
 - [3] B. S. Niels Ferguson and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, New York, 2011).
 - [4] N. Metropolis and S. Ulam, The Monte Carlo method, *J. Am. Stat. Assoc.* **44**, 335 (1949).
 - [5] N. Metropolis, A. W. Rosenbluth, M. N. Rosenbluth, A. H. Teller, and E. Teller, Equation of state calculations by fast computing machines, *J. Chem. Phys.* **21**, 1087 (1953).
 - [6] A. Montanaro, Quantum speedup of Monte Carlo methods, *Proc. R. Soc. A.* **471**, 20150301 (2015).
 - [7] D. Gherzi, A. Parakh, and M. Mezei, Comparison of a quantum random number generator with pseudorandom number generators for their use in molecular Monte Carlo simulations, *J. Comput. Chem.* **38**, 2713 (2017).
 - [8] K. Miyamoto and K. Shiohara, Reduction of qubits in a quantum algorithm for Monte Carlo simulation by a pseudorandom-number generator, *Phys. Rev. A* **102**, 022424 (2020).
 - [9] F. James, A review of pseudorandom number generators, *Comput. Phys. Commun.* **60**, 329 (1990).
 - [10] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, *npj Quantum Inf.* **2**, 16021 (2016).
 - [11] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
 - [12] M. N. Bera, A. Acín, M. Kuš, M. W. Mitchell, and M. Lewenstein, Randomness in quantum mechanics: Philosophy, physics and technology, *Rep. Prog. Phys.* **80**, 124001 (2017).
 - [13] P. Grangier and A. Auffèves, What is quantum in quantum randomness?, *Phil. Trans. R. Soc. A* **376**, 20170322 (2018).
 - [14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
 - [15] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2009.
 - [16] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
 - [17] A. Acín and L. Masanes, Certified randomness in quantum physics, *Nature (London)* **540**, 213 (2016).
 - [18] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Detection-loophole-free test of quantum nonlocality, and applications, *Phys. Rev. Lett.* **111**, 130406 (2013).
 - [19] 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 (London)* **562**, 548 (2018).
 - [20] 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 (London)* **556**, 223 (2018).
 - [21] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill, Device-independent randomness expansion with entangled photons, *Nat. Phys.* **17**, 452 (2021).
 - [22] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent randomness expansion against quantum side information, *Nat. Phys.* **17**, 448 (2021).
 - [23] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Quantum randomness certified by the uncertainty principle, *Phys. Rev. A* **90**, 052327 (2014).
 - [24] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-independent quantum random number generation, *Phys. Rev. X* **6**, 011020 (2016).
 - [25] F. Xu, J. H. Shapiro, and F. N. C. Wong, Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring, *Optica* **3**, 1266 (2016).
 - [26] D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent ultrafast quantum random number generation, *Phys. Rev. Lett.* **118**, 060503 (2017).
 - [27] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, *Nat. Commun.* **9**, 5365 (2018).
 - [28] T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, Real-time source-independent quantum random-number generator with squeezed states, *Phys. Rev. Appl.* **12**, 034017 (2019).
 - [29] D. Drahí, N. Walk, M. J. Hoban, A. K. Fedorov, R. Shakhovoy, A. Feimov, Y. Kurochkin, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, Certified quantum random numbers from untrusted light, *Phys. Rev. X* **10**, 041048 (2020).
 - [30] X. Lin, S. Wang, Z.-Q. Yin, G.-J. Fan-Yuan, R. Wang, W. Chen, D.-Y. He, Z. Zhou, G.-C. Guo, and Z.-F. Han, Security analysis and improvement of source independent quantum random number generators with imperfect devices, *npj Quantum Inf.* **6**, 100 (2020).

- [31] X. Lin, R. Wang, S. Wang, Z.-Q. Yin, W. Chen, G.-C. Guo, and Z.-F. Han, Certified randomness from untrusted sources and uncharacterized measurements, *Phys. Rev. Lett.* **129**, 050506 (2022).
- [32] X. Lin, R. Wang, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, Z. Zhou, G.-C. Guo, and Z.-F. Han, Imperfection-insensitivity quantum random number generator with untrusted daily illumination, *Opt. Express* **30**, 25474 (2022).
- [33] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, Optimal randomness certification in the quantum steering and prepare-and-measure scenarios, *New J. Phys.* **17**, 113010 (2015).
- [34] A. Chaturvedi and M. Banik, Measurement-device-independent randomness from local entangled states, *Europhys. Lett.* **112**, 30003 (2015).
- [35] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, *New J. Phys.* **17**, 125011 (2015).
- [36] 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(R) (2016).
- [37] F. Bischof, H. Kampermann, and D. Bruß, Measurement-device-independent randomness generation with arbitrary quantum states, *Phys. Rev. A* **95**, 062305 (2017).
- [38] M. Pivoluska, M. Plesch, M. Farkas, N. Ružičková, C. Flegel, N. H. Valencia, W. McCutcheon, M. Malik, and E. A. Aguilar, Semi-device-independent random number generation with flexible assumptions, *npj Quantum Inf.* **7**, 50 (2021).
- [39] C. Wang, I. W. Primaatmaja, H. J. Ng, J. Y. Haw, R. Ho, J. Zhang, G. Zhang, and C. Lim, Provably-secure quantum randomness expansion with uncharacterised homodyne detection, *Nat. Commun.* **14**, 316 (2023).
- [40] J. Argillander, A. Alarcón, C. Bao, C. Kuang, G. Lima, F. Gao, and G. B. Xavier, Quantum random number generation based on a perovskite light emitting diode, *Commun. Phys.* **6**, 157 (2023).
- [41] X. Lin and R. Wang, Quantum random number generation with partial source assumptions, [arXiv:2312.03333](https://arxiv.org/abs/2312.03333).
- [42] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, *Phys. Rev. A* **84**, 034301 (2011).
- [43] 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).
- [44] P. Mironowicz, G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, Quantum randomness protected against detection loophole attacks, *Quantum Inf. Process.* **20**, 39 (2021).
- [45] T. Van Himbeek, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, *Quantum* **1**, 33 (2017).
- [46] D. Rusca, T. van Himbeek, 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).
- [47] T. V. Himbeek and S. Pironio, Correlations and randomness generation based on energy constraints, [arXiv:1905.09117](https://arxiv.org/abs/1905.09117).
- [48] H. Tebyanian, M. Zahidy, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, Semi-device independent randomness generation based on quantum state's indistinguishability, *Quantum Sci. Technol.* **6**, 045026 (2021).
- [49] C. Roch i Carceller, K. Flatt, H. Lee, J. Bae, and J. B. Brask, Quantum vs noncontextual semi-device-independent randomness certification, *Phys. Rev. Lett.* **129**, 050501 (2022).
- [50] 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, *Phys. Rev. Appl.* **7**, 054018 (2017).
- [51] R. König, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, *IEEE Trans. Inf. Theory* **55**, 4337 (2009).
- [52] M. Tomamichel, R. Colbeck, and R. Renner, A fully quantum asymptotic equipartition property, *IEEE Trans. Inf. Theory* **55**, 5840 (2009).
- [53] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, *Nat. Commun.* **9**, 459 (2018).
- [54] T. Metger, O. Fawzi, D. Sutter, and R. Renner, Generalised entropy accumulation, in *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Piscataway, NJ, 2022), pp. 844–850.
- [55] T. Metger and R. Renner, Security of quantum key distribution from generalised entropy accumulation, *Nat. Commun.* **14**, 5272 (2023).
- [56] H. Zhou, Numerical framework for semi-device-independent quantum random-number generators, *Phys. Rev. A* **107**, 052402 (2023).
- [57] P. Brown, H. Fawzi, and O. Fawzi, Computing conditional entropies for quantum correlations, *Nat. Commun.* **12**, 575 (2021).
- [58] E. Knill, Y. Zhang, and P. Bierhorst, Generation of quantum randomness by probability estimation with classical side information, *Phys. Rev. Res.* **2**, 033465 (2020).
- [59] J. A. Bergou, Quantum state discrimination and selected applications, *J. Phys.: Conf. Ser.* **84**, 012001 (2007).
- [60] S. M. Barnett and S. Croke, Quantum state discrimination, *Adv. Opt. Photon.* **1**, 238 (2009).
- [61] J. Bae and L.-C. Kwek, Quantum state discrimination and its applications, *J. Phys. A: Math. Theor.* **48**, 083001 (2015).
- [62] I. D. Ivanovic, How to differentiate between non-orthogonal states, *Phys. Lett. A* **123**, 257 (1987).
- [63] D. Dieks, Overlap and distinguishability of quantum states, *Phys. Lett. A* **126**, 303 (1988).
- [64] A. Peres, How to differentiate between non-orthogonal states, *Phys. Lett. A* **128**, 19 (1988).
- [65] C. Roch i Carceller, Quantum state discrimination with applications in contextuality and randomness certification, Ph.D. thesis, Technical University of Denmark, 2023.
- [66] P. Skrzypczyk and D. Cavalcanti, *Semidefinite Programming in Quantum Information Science* (IOP Publishing, Philadelphia, 2023), pp. 2053–2563.
- [67] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/dwdv-89bj> for a detailed derivation of the semidefinite programs presented in the main text, specific details of the implementation, and finite-size effects treatment.

- [68] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, *Quantum* **8**, 1445 (2024).
- [69] R. Renner, Security of quantum key distribution, [arXiv:quant-ph/0512258](https://arxiv.org/abs/quant-ph/0512258).
- [70] <https://doi.org/10.3030/101106833>.
- [71] https://github.com/chalswater/QRNG_entropy_accumulation.
- Correction:* The first author's name was presented incorrectly and has been fixed.