

Sequential semi-device-independent quantum randomness certification

Carles Roch i Carceller^{1,*}, Hanwool Lee,² Jonatan Bohr Brask³, Kieran Flatt⁴, and Joonwoo Bae⁴

¹*Physics Department and NanoLund, Lund University, Box 118, 22100 Lund, Sweden*

²*Faculty of Information Technology, University of Jyväskylä, 40100 Jyväskylä, Finland*

³*Center for Macroscopic Quantum States bigQ, Department of Physics, Technical University of Denmark, Fysikvej 307, 2800 Kgs. Lyngby, Denmark*

⁴*School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea*



(Received 29 October 2025; revised 2 February 2026; accepted 25 April 2026; published 19 May 2026)

Quantum measurements under realistic conditions reveal only partial information about a system. Yet, by performing sequential measurements on the same system, additional information can be accessed. We investigate this problem in the context of semi-device-independent randomness certification using sequential maximum-confidence measurements. We develop a general framework and versatile numerical methods to bound the amount of certifiable randomness in such scenarios. We further introduce a technique to compute min-tradeoff functions via semidefinite programming duality, thus making the framework suitable for bounding the certifiable randomness against adaptive attacking strategies through entropy accumulation. Our results establish sufficient criteria showing that maximum-confidence measurements enable the distribution and certification of randomness across a sequential measurement chain in single-party systems.

DOI: [10.1103/vb68-jlr3](https://doi.org/10.1103/vb68-jlr3)

I. INTRODUCTION

The inherent unpredictability of quantum phenomena makes quantum systems a natural source of randomness. This fundamental feature has driven key advances in quantum information, particularly in cryptography, where certified randomness offers the strongest security guarantees [1–3]. Developing protocols for quantum randomness certification, which are both practically useful and secure, remains one of the key questions in quantum information science. Achieving this balance is not trivial.

The strongest security guarantees are provided by device-independent approaches [4–9]. In these schemes, none of the devices involved require precise characterization; security relies solely on the observed correlations in multipartite experiments, typically certified through the violation of a Bell inequality [10,11]. However, the experimental demands associated with violating a Bell inequality are substantial. This has motivated the development of semi-device-independent frameworks, shifting the focus from multipartite scenarios to prepare-and-measure scenarios, and introducing physically motivated assumptions to relax experimental requirements while still retaining strong security guarantees [12–17].

In parallel, sequential scenarios for monogamous correlations, such as Bell nonlocality [18] and state discrimination [19], have been investigated. At first sight, such scenarios appear counterintuitive: Quantum resources are typically not shareable, as nonlocal correlations are monogamous [20] and unknown quantum states cannot be broadcast [21]. Nevertheless, sequential protocols have revealed that a single quantum system can be measured successively by multiple parties while retaining nonclassical features. In the context of sequential Bell violations [22], a single party can share nonlocal correlations with arbitrarily many others [18,23], a feature that has been exploited for sequential device-independent quantum randomness certification [24–31]. Sequential measurement schemes have also been investigated in prepare-and-measure settings, for instance, in sequential quantum state discrimination. In these protocols, each receiver performs a measurement with both conclusive and inconclusive outcomes and forwards the resulting postmeasurement state to the next party, where conclusive outcomes allow the receiver to infer the prepared state [19,32]. Beyond these developments, little is yet known about sequential randomness in semi-device-independent settings, which may balance and enable security-level adjustment in realistic, practical applications.

In this work, we investigate randomness certification in a sequential prepare-and-measure semi-device-independent scenario. In contrast with already existing sequential randomness certification methods based on bipartite schemes, our approach considers sequential measurements of a single-party system by multiple parties. This means that the prepared quantum states are entirely sent to each device, rather distributed among distant parties, bypassing the device-independence requirement of Bell violation. A further advantage of this

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

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) 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](https://www.bibsam.com/).

approach is to make sequential randomness generation more practically accessible, as it is relatively simpler to implement prepare-and-measure schemes than those based on nonlocal correlations.

Throughout this work, we consider adversarial scenarios in which untrusted operations are treated as uncharacterized. Concretely, we consider realistic scenarios where measurements may not function as desired—yielding undetected or inconclusive events—and thus cannot be trusted. Then, we take two approaches. One is a measurement-device-independent scenario, where all states—including postmeasurement states—are characterized and trusted, but measurements are completely uncharacterized. The second approach relaxes the previous by removing all trust from postmeasurement states and only maintaining minimal assumptions on the initial state preparations, such that these are initially pure and a bound on their overlap is provided. We show that sequential randomness can be certified in both cases. These results can be rephrased as the distribution of randomness inherent in a measurement of an ensemble among multiple parties. Randomness may originate from the fact that no measurement can perfectly discriminate nonorthogonal states, hence identified as the indistinguishability of quantum states. The randomness is given to a single party by the sender, and the receiver can distribute the randomness by applying nondestructive measurements and sending remaining states to the next party, and so on. Our results show that randomness distributed in a sequential prepare-and-measure scenario can be certified.

The remainder of this work is organized as follows. In Sec. II, we present the sequential prepare-and-measure scenario with two consecutive measurements that we investigate, and the correlations that arise within. We continue in Sec. III introducing the randomness certification framework. We provide the semidefinite programming tools to compute the bounds on the min- and Shannon entropies in both approaches, i.e., with fully or partially trusted preparations. We deploy the methods to compute bounds on the certifiable randomness in Sec. IV considering the simplest case of two state preparations and two sequential measurements performing maximum-confidence measurements. We observe that in some cases it is possible to simultaneously distribute the certifiable randomness in both sequential measurements, which leads us to finding the necessary condition to be able to certify randomness in N sequential measurements in Sec. V. We end in Sec. VI with an outlook of our methods and discussing the importance of our results.

II. SEQUENTIAL PREPARE-AND-MEASURE SCENARIO

Consider the sequential prepare-and-measure scenario depicted in Fig. 1. With probability p_x , Alice encodes a classical symbol $x \in X$ into a quantum state ρ_x , which is sent to Bob, who performs a measurement $\{M_b\}$ and receives b as a measurement outcome. After doing so, Bob will possess the remaining postmeasurement state

$$\sigma_x := \sum_{i,b} (K_b^i)^\dagger \rho_x K_b^i, \quad (1)$$

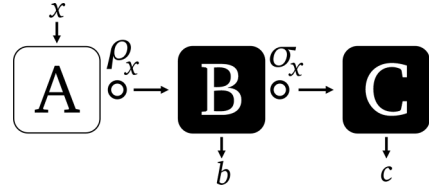


FIG. 1. Sequential prepare-and-measure scenario. Alice (A) encodes a symbol x into a quantum state ρ_x . This is sent to Bob (B), observing a measurement outcome b . Finally, Charlie (C) measures Bob's postmeasurement state σ_x and produces an outcome c .

where K_b^i are the Kraus operators corresponding to Bob's instrument, i.e., $M_b = \sum_i K_b^i (K_b^i)^\dagger$. In general, Bob's measurement may not extract all the information encoded in Alice's states. The remaining quantum state σ_x can thus still contain information about x that can be accessed by a subsequent observer, Charlie, who performs a measurement $\{N_c\}$ with outcomes c . This leads to a natural trade-off: the more information Bob gains about x , the less remains available to Charlie, and vice versa.

We study frameworks with completely untrusted measurements. Specifically, we assume that all measurement devices have been preprogrammed to perform certain unknown measurement strategies labeled by λ according to a distribution $q(\lambda)$. Note that, due to unitary invariance, without loss of generality we can take the states to be independent of λ . Namely, in each prepare-and-measure round, one can rotate to a frame in which Alice's state preparations, say, $\tilde{\rho}_x^\lambda$, are ρ_x , with $U^{(\lambda)} \rho_x U^{(\lambda)\dagger} = \tilde{\rho}_x^\lambda$. Thanks to the cyclic property of the trace, the rotation $U^{(\lambda)}$ can be absorbed by any subsequent operation, such as quantum measurements or channels. In summary then, the observable correlations in this scenario can be written as

$$p(b, c|x) = \sum_i \sum_\lambda q(\lambda) \text{Tr}[\rho_x K_b^{i,(\lambda)} N_c^{(\lambda)} (K_b^{i,(\lambda)})^\dagger]. \quad (2)$$

The correlations gathered individually in each measurement device can be directly obtained through marginalization. At this point, it is important to distinguish between different types of events in state discrimination. We say that a measurement successfully identified a preparation x if the measurement outcome is equal to x . The average rate of occurrence of successful outcomes is denoted by p_s . Similarly, if the measurement outcome is inside the alphabet of preparations X but not equal to x , we say that the measurement performed an error, and we call p_e the error probability. Additionally, measurement devices may lead to inconclusive events either through purposeful design or through experimental imperfections. We label by $b, c = \emptyset$ any measurement outcome that is inconclusive—i.e., is not in the alphabet of preparations X —and $p_\emptyset$ their outcome rate.

Moreover, postmeasurement states cannot be arbitrarily chosen. For instance, consider that Bob employs a measurement strategy in a two-qubit state discrimination setting such that the error probability p_e is null—also known as unambiguous state discrimination. During the rounds that his device returns conclusive results, i.e., either $b = 0$ or $b = 1$, he will be able to send the original states ρ_x to Charlie. However, if

Bob's device returns an inconclusive event $b = \emptyset$, he will not know what state was produced and thus will have to randomly choose to send either ρ_0 or ρ_1 to Charlie. It turns out that the optimal strategy for Bob and Charlie to optimally discriminate Alice's preparations with unambiguous qubit-state discrimination is to program Bob's instrument to produce two pure states $|\phi_x\rangle$ with an overlap lower bounded by $\langle\psi_0|\psi_1\rangle/p_\emptyset^B$ regardless of his measurement outcome [19], for $p_\emptyset^B$ being the probability of inconclusive events in Bob's device. A generalization with mixed states has also been studied in Ref. [32], where the optimal choice of a measurement that effectively verifies a state corresponds to a maximum-confidence measurement. The confidence C_x that a receiver has in correctly discriminating a particular state is defined as the conditional probability that the state preparation was x given that the observed measurement outcome is also x [33]. It can be expressed through Bayes' rule as

$$C_x := \frac{p_x \text{Tr}[\rho_x M_x]}{\sum_{x'} p_{x'} \text{Tr}[\rho_{x'} M_x]}. \quad (3)$$

Maximum-confidence measurements—i.e., the measurements that yield the maximum value of confidence—have been widely studied in the context of qubit state discrimination (see Refs. [34,35]). Additionally, it has been shown that they reproduce extremal prepare-and-measure correlations making them strong candidates for randomness certification [36]. Maximum-confidence measurements reduce to well-known state discrimination cases in extreme conditions. Concretely, on the one hand, if the probability of inconclusive events is null, maximum-confidence measurements reduce to minimum error state discrimination measurements [37]. On the other hand, if all state preparations are linearly independent, maximum-confidence measurements reduce to unambiguous state discrimination measurements [38–40], with $C_x = 1, \forall x$. Moreover, similarly as in a sequential unambiguous state discrimination scheme, Bob's postmeasurement states cannot contain unlimited information about Alice's inputs x . Namely, as we show in the Supplemental Material [41], if Alice's preparations are qubits and initially contained a pure part with well-defined overlaps $|\langle\psi_0|\psi_1\rangle| = \delta$ and a white noise component weighted by $1 - r$, his postmeasurement states can be chosen to be of the form $\sigma_x = t|\phi_x\rangle\langle\phi_x| + \frac{1-t}{2}\mathbb{1}$ with

$$t = r \sqrt{\frac{1 - \delta^2 + (1 - r^2) \frac{\delta^2}{(p_\emptyset^B)^2}}{1 - r^2 \delta^2}}. \quad (4)$$

and $|\langle\phi_0|\phi_1\rangle| = \frac{r\delta}{p_\emptyset^B t}$. With this configuration, both Bob and Charlie are able to reach the same maximum confidence in discriminating x . In what follows, we investigate the certifiable randomness in specific cases with perfect knowledge of all state preparations, including the postmeasurement states. Later, we generalize our findings to a case where only the overlaps of Alice's pure state preparations are known to be bounded, and Bob's postmeasurement states are completely uncharacterized.

III. SEQUENTIAL RANDOMNESS CERTIFICATION

The goal of Alice, Bob, and Charlie is to be able to produce measurement outcomes that are as unpredictable as possible for an external malicious party. To this end, Bob and Charlie can perform maximum-confidence measurements, each yielding observable confidences C^B and C^C , $\forall x$, and rates of inconclusive events $p_\emptyset^B$ and $p_\emptyset^C$, respectively. To quantify how predictable those measurement outcomes are, we introduce the figure of an eavesdropper, or Eve, who has the goal of guessing those outcomes. We assume that, prior to the prepare-and-measure experiment, Eve has full access to the inner workings of the measurement devices and can preprogram the strategies λ at will. Then, she hands the devices to all participating parties who privately select their respective inputs and observe their outcomes. Thus, the eavesdropping strategies λ cannot depend on the inputs x .

In the most general case, an eavesdropper could exploit quantum correlations by establishing entanglement with the devices. Recent studies have shown that such attacks, based on quantum side information, can enhance the eavesdropper's guessing capabilities, reducing the amount of certifiable randomness in semi-device-independent prepare-and-measure scenarios [42]. Any admissible attack, however, must satisfy the semi-device-independent assumptions imposed on the state preparations. Here, we consider two separate cases: fully characterized preparations or partially characterized pure state preparations constrained by a lower bound on their overlap. Both assumptions ensure that any side information available to the eavesdropper at the level of preparations is necessarily classical, i.e., unentangled with the adversary. The measurement devices, in contrast, are left completely uncharacterized, allowing the eavesdropper to exploit quantum side information only at the measurement stage. As we show in the Supplemental Material [41], this model is equivalent to the standard assumption of globally classical side information and does not offer any additional advantage to the adversary.

To this end, we present the tools based on semidefinite programming to compute bounds on the certifiable randomness. We consider two distinct cases. First, a measurement-device-independent setting where all state preparations—even Bob's postmeasurement states—are completely characterized. Second, we relax the assumption of known state preparations to a more semi-device-independent approach, where all devices are left uncharacterized and we only assume a bound on the overlap of the pure states prepared by Alice.

A. Trusted state preparations

We begin assuming complete knowledge of all state preparations, including Bob's postmeasurement states, as sketched in Fig. 1. While the protocol involves multiple preparations, we certify the randomness in the measurement outcomes only during the rounds when Alice chooses a particular $x = x^*$. We find a bound on Eve's guessing probability p_g , which leads to a bound on the single-round min-entropy as $H_{\min} = -\log_2(p_g)$ [43,44]. Specifically, given a set of n known quantum states $\{\rho_x\}_{x=0}^{n-1}$, we maximize

$$p_g^B := \sum_{\lambda} q(\lambda) \max_b \{\text{Tr}[\rho_{x^*} M_b^{(\lambda)}]\}. \quad (5)$$

The maximization of p_g^B runs over any possible positive operator-valued measure (POVM) $\{M_b^{(\lambda)}\}$ and distributions $q(\lambda)$ such that Bob's confidence C^B and rate of inconclusive events $p_\emptyset^B$ are reproduced. As we show in the Supplemental Material [41], we are able to cast this optimization as a semidefinite program [45]. Moreover, we reformulate the optimization problem using the dual semidefinite program, from which we find

$$p_g^B \leq \min_{g,h,R,H^\lambda} g p_\emptyset^B + h C^B (1 - p_\emptyset^B) + \text{Tr}[R], \quad (6)$$

where g and h are arbitrary scalars restricted by

$$\sum_x \rho_x \left(\delta_{b,\lambda} \delta_{x,x^*} - \frac{g}{n} \delta_{b,\emptyset} - \frac{h}{n} \delta_{b,x} \right) + H^\lambda - \frac{1}{d} \text{Tr}[H^\lambda] \mathbb{1} - R \leq 0, \quad (7)$$

for R and H^λ being arbitrary $d \times d$ Hermitian matrices. Formulating the semidefinite program in its dual form is relevant for computing randomness certification in real-world conditions. In experimental implementations, the observed frequencies of events only approximate the true underlying probability distribution. As a result, the estimated distribution may not correspond to any valid quantum realization, meaning that the associated constraints cannot be exactly satisfied. Since the dual optimal value always yields an upper bound on the primal solution, it will always find a solution even if the specified correlations—in this case in the form of observable confidence and rate of inconclusive events—are not physical.

We move on computing the certifiable randomness produced in Charlie's device. After the first measurement on Alice's states, Bob is left with the postmeasurement state σ_x for which we have a full description. Concretely, let us assume that after Alice chose to prepare the pure state $|\psi_x\rangle\langle\psi_x|$, this was affected by white noise such that, instead, Bob received $\rho_x = r|\psi_x\rangle\langle\psi_x| + (1-r)\frac{\mathbb{1}}{d}$, where d is the Hilbert space dimension, r is a noise parameter, and the pure part of her states have a well-defined overlap $|\langle\psi_x|\psi_{x'}\rangle| = \delta$, $\forall x \neq x'$. Let Bob perform a maximum-confidence measurement. Aligned with the framework from Ref. [32], if we want to maximize Charlie's confidence in the two-qubit state discrimination case, Bob's postmeasurement states averaged over his measurement outcomes b as in Eq. (1) will be given by $\sigma_x = t|\phi_x\rangle\langle\phi_x| + (1-t)\frac{\mathbb{1}}{d}$ with t from Eq. (4) and $|\langle\phi_x|\phi_{x'}\rangle| = \frac{r\delta}{p_\emptyset^B t}$, $\forall x \neq x'$. These states are then sent to Charlie, who will perform a measurement described by the POVM $\{N_c^{(\lambda)}\}$ distributed according to $q(\lambda)$. For the concrete setting x^* , Eve's guessing probability is then given by

$$p_g^C := \sum_\lambda q(\lambda) \max_c \{ \text{Tr}[\sigma_{x^*} N_c^{(\lambda)}] \}. \quad (8)$$

We aim to maximize p_g^C over all possible POMVs implementable in Charlie's device, and over all distributions $q(\lambda)$. This optimization, however, is exactly the same scenario analogous to that from Alice-Bob prepare-and-measure case: Instead of Alice preparing $\{\rho_x\}$ now Bob sends the states $\{\sigma_x\}$, and instead of Bob performing the measurement $\{M_b^{(\lambda)}\}$ now

Charlie measures $\{N_c^{(\lambda)}\}$. We can thus use the exact same formalism and use the analogous form of the bound in Eq. (6), which allows us to find a bound on the probability that Eve guesses Charlie's measurement outcome p_g^C , replacing $\rho_x \leftrightarrow \sigma_x$ and $M_b^{(\lambda)} \leftrightarrow N_c^{(\lambda)}$.

The proposed framework with trusted postmeasurement states allows us to compute bounds on the randomness individually in Bob and Charlie's measurement outcomes using a single semidefinite program for each party. The underlying assumptions, although conveniently practical, are rather strong. For example, although Bob and Charlie's measurements are completely uncharacterized, Bob's postmeasurement states $\{\sigma_x\}$ are assumed to be perfectly known and fixed over each prepare-and-measure round. If that were not true, Charlie's certifiable randomness would be drastically reduced, as Eve would have more freedom available to increase her guessing probability. For example, consider a configuration in which Bob's randomness yield is null. If the postmeasurement states were not independent of λ , Eve could preprogram Bob's device to transmit the knowledge of the measurement outcome b to Charlie through the hidden variable λ during each prepare-and-measure round. That would be possible only if the observable maximum confidence and rate of inconclusive events averaged over λ permit it. Charlie's device would just need to spit the received value of λ as measurement outcome, of which Eve has full knowledge, hence producing no randomness.

More importantly, assuming a fixed form of postmeasurement states over the rounds significantly limits potential adaptive eavesdropping strategies. Using adaptive attacking strategies, Eve can gather knowledge from attacks in Bob's device from previous rounds to improve her guess of b in future rounds. Similarly, Eve can gather statistical information from previous attacks to both Bob and Charlie to improve her guess of c in future rounds. However, if Bob's postmeasurement states remain fixed and constant over the rounds, Eve cannot fully unleash her adaptive potential. That is because, after Bob's device employs a measurement strategy λ , the trusted postmeasurement states will be independent of λ , and thus, any different attack Eve could have performed in Bob will not influence her attack to Charlie. In consequence, the statistical behavior of Charlie's outcome will be independent of any knowledge she could have gathered during her attack in Bob, and thus, Eve cannot employ a fully adaptive attacking strategy. This rules out the applicability of entropy accumulation methods [46], which are becoming the standard approach in quantum cryptography (see, e.g., Refs. [47–49]).

B. Untrusted state preparations

In an attempt to relax the assumption of perfect knowledge in all state preparations, we introduce a more general framework as illustrated in Fig. 2. We remove any assumption on the structure of the postmeasurement states and any intermediate operation between Bob and Charlie. Moreover, we assume that Alice's pure state preparations are only partially characterized through a lower bound on their pairwise overlap, i.e., $|\langle\psi_x|\psi_{x'}\rangle| \geq \delta$.

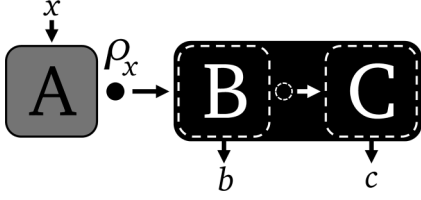


FIG. 2. Semi-device-independent framework. We assume that Alice's preparations are pure with bounded pairwise overlaps. All operations performed after the preparation process are completely uncharacterized.

In order to remove any imposed knowledge on Bob's postmeasurement states, we collect any measurement and state updates he might perform in his device, together with Charlie's measurements, into the operator

$$G_{b,c}^{(\lambda)} := \sum_i K_b^{i,(\lambda)} N_c^{(\lambda)} (K_b^{i,(\lambda)})^\dagger. \quad (9)$$

This new operator constitutes a well-defined POVM. Namely, by definition, it is positive semidefinite $G_{b,c}^{(\lambda)} \geq 0 \forall b, c$ and complete $\sum_{b,c} G_{b,c}^{(\lambda)} = \mathbb{1}$. Moreover, the observable correlations can be retrieved directly through the Born rule $p(b, c|x) = \sum_\lambda q(\lambda) \text{Tr}[\rho_x G_{b,c}^{(\lambda)}]$. It is important to remark that the sequential nature of the events b and c is not imprinted itself into the operators $\{G_{b,c}^{(\lambda)}\}$. It is through the correlations—or more generally in any observable witness such as the confidence—that the sequential nature of the operations embedded in $\{G_{b,c}^{(\lambda)}\}$ must be imposed.

Armed with the new compact definition of all sequential measurements in the operators $\{G_{b,c}^{(\lambda)}\}$, we now present the methods to compute the certifiable randomness. We begin computing bounds on the min-entropy and continue bounding Shannon entropy that we use to certify the randomness in non-independent and identically distributed (non-i.i.d.) prepare-and-measure rounds subject to adaptive attacking strategies.

1. I.i.d. rounds: min-entropy

With the new operator $\{G_{b,c}^{(\lambda)}\}$ describing any operation performed in Bob and Charlie's devices, we begin computing the min-entropy to quantify the single-shot certifiable randomness in Charlie's device [the certifiable randomness in Bob's device can be directly computed with the bound in Eq. (6)]. To do so, we assume that we are given the observable confidences C^B and C^C and rates of inconclusive events $p_\emptyset^B$ and $p_\emptyset^C$ in Bob and Charlie's devices, respectively. As explained in Sec. III A, a lower bound on the min-entropy can be found directly through upper bounding the probability that Eve guesses the measurement outcome, conditioned on her having access to classical side information. Here, Eve's guessing probability of Charlie's outcome can be written as

$$p_g^C := \sum_b \sum_\lambda q(\lambda) \max_c \{\text{Tr}[\rho_{x^*} G_{b,c}^{(\lambda)}]\}. \quad (10)$$

The maximization of p_g^C can be formulated as a semidefinite program, as shown in the Supplemental Material [41]. We further derive its dual form yielding the bound on Eve's guessing probability,

$$p_g^C \leq \min_{g^B, h^B, F^{\lambda_1, \lambda_2}, g^C, h^C, R} g^B p_\emptyset^B + h^B C^B (1 - p_\emptyset^B) + g^C p_\emptyset^C + h^C C^C (1 - p_\emptyset^C) + \text{Tr}[R], \quad (11)$$

where g^B, g^C, h^B , and h^C are arbitrary scalars restricted by

$$\sum_x \rho_x \left(\delta_{c,\lambda} \delta_{x,x^*} - \frac{g^B}{n} \delta_{b,\emptyset} - \frac{h^B}{n} \delta_{b,x} - \frac{g^C}{n} \delta_{c,\emptyset} - \frac{h^C}{n} \delta_{c,x} \right) + F^\lambda - \frac{1}{2} \text{Tr}[F^\lambda] \mathbb{1} - R \leq 0, \quad (12)$$

with R and F^λ being arbitrary $d \times d$ Hermitian matrices. Note that d denotes the Hilbert space dimension, which we aim to leave unconstrained. To do so, since n pure state preparations can span at most an n -dimensional Hilbert space, it suffices to consider $d \geq n$.

By defining the new operators $\{G_{b,c}^{(\lambda)}\}$ in the semi-device-independent framework, we can now also compute a bound on the certifiable randomness jointly contained in both Bob and Charlie's measurement outcomes. To do so, we first write the probability that Eve guesses both Bob and Charlie's outcomes as

$$p_g^{BC} := \sum_\lambda q(\lambda) \max_{b,c} \{\text{Tr}[\rho_{x^*} G_{b,c}^{(\lambda)}]\}. \quad (13)$$

We maximize p_g^{BC} for any set of pure states $\{\rho_x\}$ with pairwise overlaps lower bounded by δ , and over all possible implementable $\{G_{b,c}^{(\lambda)}\}$, distributed according to $q(\lambda)$, such that the observable confidences C^B and C^C , and rates of inconclusive events $p_\emptyset^B$ and $p_\emptyset^C$ are reproduced. As we show in detail in the Supplemental Material [41], we can cast this optimization problem as a semidefinite program, and subsequently find its dual formulation which will lead to p_g^{BC} be bounded by the exact same bound in Eq. (11), but now g^B, g^C, h^B , and h^C are arbitrary scalars subject to

$$\sum_x \rho_x \left(\delta_{b,\lambda_1} \delta_{c,\lambda_2} \delta_{x,x^*} - \frac{g^B}{n} \delta_{b,\emptyset} - \frac{h^B}{n} \delta_{b,x} - \frac{g^C}{n} \delta_{c,\emptyset} - \frac{h^C}{n} \delta_{c,x} \right) + F^{\lambda_1 \lambda_2} - \frac{1}{2} \text{Tr}[F^{\lambda_1 \lambda_2}] \mathbb{1} - R \leq 0, \quad (14)$$

where now we split the tuple $\lambda = (\lambda_1, \lambda_2)$ for each measuring party, with R and $F^{\lambda_1 \lambda_2}$ being arbitrary $d \times d$ Hermitian matrices.

2. Non-i.i.d. rounds: Shannon entropy

The semi-device-independent approach by compacting all sequential measurements in a single uncharacterized operation is now resilient to non-i.i.d. attacks. Namely, Eve is allowed to adapt the attacking strategy during each round based on accumulated knowledge from previous rounds. This was not conceived in the measurement-device-independent

setting, which had an i.i.d. component because postmeasurement states were fixed on every round of the experiment. The channel connecting Bob and Charlie, however, must remain secured; i.e., we assume that Eve cannot intercept Bob's post-measurement state in each round. This is an assumption that, combined with classical side information, has been considered in the vast majority of previous semi-device-independent approaches [50–53]. Nevertheless, no knowledge on either the channel connecting both measurement devices or the measurements themselves is assumed. This makes the framework applicable for entropy accumulation theorems in prepare-and-measure scenarios [46]. The entropy accumulation theorem establishes that the total amount of entropy per round accumulated after m prepare-and-measure rounds assuming that Eve can perform adaptive attacking strategies over the rounds is bounded by

$$\frac{1}{m} H_{\min}^{\varepsilon}(B^m | E^m) \geq \min f_{\min} - \mathcal{O}\left(\frac{1}{\sqrt{m}}\right). \quad (15)$$

Here, $H_{\min}^{\varepsilon}(B^m | E^m)$ is the so-called *smooth min-entropy* accumulated over m prepare-and-measure rounds [54] and $f_{\min}$ is an affine function that lower bounds the Shannon entropy (also known as *min-tradeoff function*). This quantity is essential to treat finite size effects in non-i.i.d. prepare-and-measure rounds. In what follows, we introduce a method to find valid min-tradeoff functions by lower bounding the Shannon entropy based on the recent works from Refs. [52,53]. Concretely, let us begin considering Bob's system. The Shannon entropy in Bob's system B given a particular choice of preparation $x^* \in X$ and conditioned on Eve's system E and on the classical side information stored in the shared randomness λ can be written as

$$H(B|E) = - \sum_{\lambda} q(\lambda) \sum_b p_{\lambda}(b|x^*) \log_2 p_{\lambda}(b|x^*), \quad (16)$$

for $p_{\lambda}(b|x) = \sum_c \text{Tr}[\rho_x G_{b,c}^{(\lambda)}]$. As we show in the Supplemental Material [41], we are able to compute an affine min-tradeoff function $f_{\min}^B \leq H(B|E)$ by expressing the Shannon entropy through the Gauss-Radau quadrature following the ideas from Ref. [55]. One can then cast the optimization as a semidefinite program relaxation and find the subsequent dual form. This provides us with the min-tradeoff function

$$f_{\min}^B = c_m + \bar{g} p_{\varnothing}^B + \bar{h} C^B (1 - p_{\varnothing}^B) + \text{Tr}[\bar{R}], \quad (17)$$

for $c_m = \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln 2}$, with t_i and w_i being the nodes and weights from the Gauss-Radau quadrature, which can be obtained through a simple algorithm [56]. Here, $\bar{g} = \sum_i g_i$ and $\bar{h} = \sum_i h_i$ are arbitrary scalars and $\bar{R} = \sum_i R_i$ arbitrary $d \times d$ Hermitian matrices subject to

$$\begin{aligned} \sum_j D_b^{ij} &= - \sum_x \rho_x \left(\frac{g_i}{n} \delta_{b,\varnothing} + \frac{h_i}{n} \delta_{b,x} \right) - R_i, \\ F_b^{ij} + F_b^{ij\dagger} &= 2\tau_i \rho_{x^*} \delta_{j,b} + P_1^{ij} - \frac{1}{d} \text{Tr}[P_1^{ij}] \mathbb{1}, \\ L_b^{ij} &= \tau_i \rho_{x^*} [(1 - t_i) \delta_{j,b} + t_i] + P_2^{ij} - \frac{1}{d} \text{Tr}[P_2^{ij}] \mathbb{1}, \end{aligned} \quad (18)$$

where $P_1^{ij}, P_2^{ij}, D_b^{ij}, L_b^{ij}$, and F_b^{ij} are arbitrary $d \times d$ Hermitian matrices, the last three constrained to fulfill the positivity of the following block matrix:

$$\begin{pmatrix} D_{bc}^{ij} & F_b^{ij} \\ F_b^{ij\dagger} & L_b^{ij} \end{pmatrix} \succeq 0. \quad (19)$$

Given a set of variables that fulfill the specified constraints, the min-tradeoff function in Eq. (17) represents a lower bound on the Shannon entropy valid for any observable confidence C^B and rates of inconclusive events $p_{\varnothing}^B$ in Bob's device.

We continue computing a bound on the certifiable Shannon entropy in Charlie's device, and in both Bob and Charlie's devices jointly. The Shannon entropy in Charlie's system C and Bob + Charlie's systems BC conditioned on a particular input $x^* \in X$ and conditioned on Eve's system E and on the classical side information stored in the shared randomness λ , respectively, can be written as

$$H(C|E) = - \sum_{\lambda} q(\lambda) \sum_c p_{\lambda}(c|x^*) \log_2 p_{\lambda}(c|x^*), \quad (20)$$

$$H(BC|E) = - \sum_{\lambda} q(\lambda) \sum_{b,c} p_{\lambda}(b, c|x^*) \log_2 p_{\lambda}(b, c|x^*), \quad (21)$$

for $p_{\lambda}(b, c|x) = \text{Tr}[\rho_x G_{b,c}^{(\lambda)}]$ and $p_{\lambda}(c|x) = \sum_b p_{\lambda}(b, c|x)$. Similarly as in Bob's case, in the Supplemental Material [41] we show that we are able to find an affine min-tradeoff function $f_{\min}^C \leq H(C|E)$ and $f_{\min}^{BC} \leq H(BC|E)$ by expressing the optimizations in a semidefinite program and deriving their dual form. This provides us with the exact same bound in both cases $f_{\min}$, i.e.,

$$\begin{aligned} f_{\min} &= c_m + \bar{g}^B p_{\varnothing}^B + \bar{h}^B C^B (1 - p_{\varnothing}^B) \\ &\quad + \bar{g}^C p_{\varnothing}^C + \bar{h}^C C^C (1 - p_{\varnothing}^C) + \text{Tr}[\bar{R}]. \end{aligned} \quad (22)$$

Depending on whether we are interested in bounding the Shannon entropy in solely Charlie's C or the joint BC systems, the scalars $\bar{g}^B = \sum_i g_i^B$, $\bar{g}^C = \sum_i g_i^C$, $\bar{h}^B = \sum_i h_i^B$, and $\bar{h}^C = \sum_i h_i^C$ and $d \times d$ Hermitian matrices $\bar{R} = \sum_i R_i$ will be subject to different restrictions. For $f_{\min} \leq H(C|E)$,

$$\begin{aligned} \sum_j D_{bc}^{ij} &= - \sum_x \rho_x \left(\frac{g_i^B}{n} \delta_{b,\varnothing} + \frac{h_i^B}{n} \delta_{b,x} + \frac{g_i^C}{n} \delta_{c,\varnothing} + \frac{h_i^C}{n} \delta_{c,x} \right) \\ &\quad - R_i, \end{aligned}$$

$$\begin{aligned} F_{bc}^{ij} + F_{bc}^{ij\dagger} &= 2\tau_i \rho_{x^*} \delta_{j,c} + P_1^{ij} - \frac{1}{d} \text{Tr}[P_1^{ij}] \mathbb{1}, \\ L_{bc}^{ij} &= \tau_i \rho_{x^*} [(1 - t_i) \delta_{j,c} + t_i] + P_2^{ij} - \frac{1}{d} \text{Tr}[P_2^{ij}] \mathbb{1}, \end{aligned} \quad (23)$$

where $P_1^{ij}, P_2^{ij}, D_{bc}^{ij}, L_{bc}^{ij}$, and F_{bc}^{ij} are arbitrary $d \times d$ Hermitian matrices satisfying the positivity constraint

$$\begin{pmatrix} D_{bc}^{ij} & F_{bc}^{ij} \\ F_{bc}^{ij\dagger} & L_{bc}^{ij} \end{pmatrix} \succeq 0. \quad (24)$$

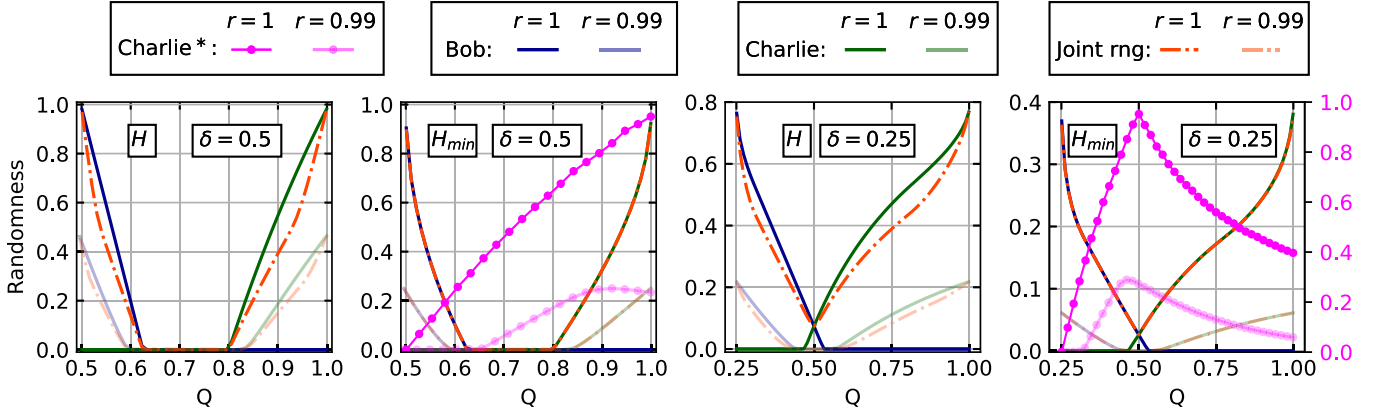


FIG. 3. Shannon and min-entropies certified in two sequential maximum-confidence measurements. Alice prepares two pure states with $|\langle\psi_0|\psi_1\rangle| \geq \delta$. Bob and Charlie perform maximum-confidence measurement with white noise component $1 - r$ and rates of inconclusive outcomes Q and $r\delta/Q$, respectively. We also show the certifiable min-entropy in Charlie's device in the measurement-device-independent setting (Charlie*).

On the other hand, for $f_{\min} \leq H(BC|E)$,

$$\begin{aligned} \sum_j D_{bc}^{ijk} &= -\sum_x \rho_x \left(\frac{g_i^B}{n} \delta_{b,\emptyset} + \frac{h_i^B}{n} \delta_{b,x} + \frac{g_i^C}{n} \delta_{c,\emptyset} + \frac{h_i^C}{n} \delta_{c,x} \right) \\ &\quad - R_i, \\ F_{bc}^{ijk} + F_{bc}^{ijk\dagger} &= 2\tau_i \rho_{x^*} \delta_{j,b} \delta_{k,c} + P_1^{ijk} - \frac{1}{d} \text{Tr}[P_1^{ijk}] \mathbb{1}, \\ L_{bc}^{ijk} &= \tau_i \rho_{x^*} [(1 - t_i) \delta_{j,b} \delta_{k,c} + t_i] + P_2^{ijk} \\ &\quad - \frac{1}{d} \text{Tr}[P_2^{ijk}] \mathbb{1}. \end{aligned} \quad (25)$$

Here, P_1^{ijk} , P_2^{ijk} , D_{bc}^{ijk} , L_{bc}^{ijk} , and F_{bc}^{ijk} are arbitrary $d \times d$ Hermitian matrices, the last three constrained to fulfill the positivity of the block matrix

$$\begin{pmatrix} D_{bc}^{ijk} & F_{bc}^{ijk} \\ F_{bc}^{ijk\dagger} & L_{bc}^{ijk} \end{pmatrix} \geq 0. \quad (26)$$

Given a set of variables that fulfill the specified constraints, the min-tradeoff function in Eq. (22) represents an affine lower bound on the Shannon entropy valid for any observable confidences C^B , C^C and rates of inconclusive events $p_{\emptyset}^B$, $p_{\emptyset}^C$ in Bob and Charlie's devices, respectively.

IV. RESULTS

To illustrate our methods, we consider a simple two-state discrimination scenario with two measurements (Bob and Charlie) performed sequentially. We test our approach when Bob and Charlie perform maximum-confidence measurements, and Bob's performance is dictated by a limit in his rate of inconclusive events.

First, we begin bounding the certifiable confidence that has been recently studied in the context of sequential state discrimination [32]. We assume that Alice is able to prepare a pair of pure states $\rho_x = |\psi_x\rangle\langle\psi_x|$ for $x = \{0, 1\}$, which have an overlap that satisfies the bound $|\langle\psi_0|\psi_1\rangle| \geq \delta$. After being prepared, these states are subjected to white noise and become mixed states of the form $\rho_x = r|\psi_x\rangle\langle\psi_x| + \frac{1-r}{d}\mathbb{1}$. Next, Bob

performs a measurement. His performance is parametrized through a bound on his rate of inconclusive events $p_{\emptyset}^B \geq Q$, which we range from the minimum value allowed by noiseless maximum-confidence measurements (i.e., unambiguous state discrimination) and the algebraic maximum, i.e., $\delta \leq Q \leq 1$. We compute a bound on the certifiable confidence in Bob's side C^B accounting for the white noise. Following up, Charlie measures Bob's postmeasurement states. We compute a bound on Charlie's maximum confidence considering that Bob's device reproduces the named bound on the inconclusive rate Q and observed confidence C^B . We fix Charlie's rate of inconclusive events to reach the optimal value $p_{\emptyset}^C = \frac{r\delta}{Q}$, i.e., the minimum allowed by optimal maximum-confidence measurements. This follows from the fact that we assume both parties attain the maximum confidence, which will be equal as shown earlier.

Moving on, we use the observable confidences and resulting rates of inconclusive events to bound the certifiable randomness in Bob and Charlie's measurement outcomes when $\delta = 0.5$ and $\delta = 0.25$, and we show them in Fig. 3. Concretely, we consider the approach in which all state preparations, including the postmeasurement states, are fully characterized and compute a bound on the min-entropy ($H_{\min}$) in Bob and Charlie's devices through the guessing probabilities in Eq. (5) (blue line labeled Bob) and Eq. (8) (pink-dotted line labeled Charlie*), respectively. We then move on with the second approach, with uncharacterized postmeasurement states, and compute a bound on the i.i.d. randomness with the min-entropies computed through the guessing probabilities in Eq. (8) (green line labeled Charlie) and Eq. (13) (red line labeled Joint rng) in Charlie's and Bob + Charlie's systems, respectively (Bob's randomness in this case is equivalent to the blue line labeled Bob). Finally, we consider the non-i.i.d. case and compute a bound on the Shannon entropy (H) in Bob's system from Eq. (16), in Charlie's system from Eq. (20), and in the joint Bob + Charlie's systems through Eq. (21).

Looking at the first approach with fully trusted preparations, we see that Charlie's certifiable randomness peaks at inconclusive rates $Q = 2r\delta$. This happens because we are

imposing a highly restrictive assumption in the form of Bob's postmeasurement states. Namely, these are constrained to be of the form $\sigma_x = t|\phi_x\rangle\langle\phi_x| + (1-t)\frac{\mathbb{1}}{d}$ with t from Eq. (4) and $|\langle\phi_x|\phi_{x'}\rangle| = \frac{r\delta}{p_{\varnothing}^B t}$. Then, Charlie's maximum-confidence measurement with an optimal rate of inconclusive events $p_{\varnothing}^C = \frac{r\delta}{Q}$ yields maximal randomness in the measurement outcome for $p_{\varnothing}^C = \frac{1}{2}$. This high randomness yield reflects the strength of the assumptions placed in our first approach, i.e., assuming perfect knowledge on Bob's postmeasurement states.

Through the second approach (untrusted postmeasurement states), we observe that the certifiable randomness in Bob's device dies out when the rate of inconclusive outcomes reaches the critical value

$$Q_{\text{crit}}^B = \frac{(1+\delta^2)(r - \sqrt{1-\delta^2}\sqrt{1-r^2\delta^2})}{(1+\delta^2)r - \sqrt{1-\delta^2}\sqrt{1-r^2\delta^2}}, \quad (27)$$

for $\delta^2 \geq \frac{1+r^2-\sqrt{1-2r^2+5r^4}}{2r^2}$, and $Q_{\text{crit}}^B = 0$ otherwise. The fact that for certain rates Q there exist no certifiable randomness indicates that the observable confidence C^B and inconclusive rate $p_{\varnothing}^B$ can be reproduced through predefined deterministic measurement schemes. This is indeed what is happening here. In our model, the confidence in Bob's device is kept at maximum, while its rate of inconclusive events is bounded by $p_{\varnothing}^B \geq Q$. With that, we can then bound the state discrimination success probability as $p_s^B \leq C(1-Q)$. As shown in Ref. [36], the maximum success probability attainable by a deterministic model is given by $p_s^{\text{det}} = 1 - \frac{\delta^2}{2} - \frac{Q}{1+\delta^2}$. If Q grows too large, Bob's success probability will fall below the deterministic threshold, at which point he will not be able to certify any randomness from his measurement outcomes. This limit is indeed Eq. (27), at which $C(1-Q_{\text{crit}}^B) = p_s^{\text{det}}$. Similarly for Charlie, his certifiable randomness is null until Bob's rate of inconclusive events reaches a second critical value $Q_{\text{crit}}^C = \frac{r\delta}{Q_{\text{crit}}^B}$. With maximum-confidence discrimination therefore, no randomness can be sequentially certified simultaneously in Bob and Charlie's devices if Alice's pure state preparations have an overlap $|\langle\psi_0|\psi_1\rangle| \geq \delta$ such that $\delta > \Delta$, for $\Delta = \frac{1}{3}(\tau - 8\tau^{-1} - 1) \simeq 0.2956$, with $\tau = \sqrt[3]{2(13 + 3\sqrt{33})}$ (i.e., when $Q_{\text{crit}}^B \leq Q_{\text{crit}}^C$ for $r = 1$). Otherwise, randomness can be simultaneously certified in both devices if $Q_{\text{crit}}^C \leq Q \leq Q_{\text{crit}}^B$. This insight indicates that there are some cases in which randomness can be simultaneously certified in two sequential measurements. In the following, we complete this analysis by extending these findings to an arbitrary number of sequential maximum-confidence measurements.

V. EXTENSION TO N SEQUENTIAL MEASUREMENTS

For now, we only considered the simplest case of two sequential maximum-confidence measurements. Here, extend this scenario to an arbitrary number N of sequential maximum-confidence measurements. Let $\{S_1, S_2, \dots, S_N\}$ label the systems of each measurement and let $p_{\varnothing}^{S_i} \geq Q_i$ be the rate of inconclusive events in each individual system. Again, consider that all the observable statistics are compatible with those reproduced by maximum-confidence measurements on two pure state preparations $\rho_x = |\psi_x\rangle\langle\psi_x|$ with $|\langle\psi_0|\psi_1\rangle| \geq \delta$.

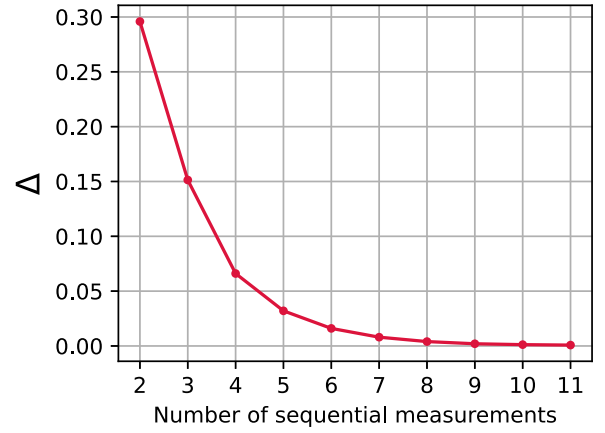


FIG. 4. Numerical search of the bound $\delta \leq \Delta$ at which randomness can be simultaneously certified in all N sequential maximum-confidence measurements.

Let the postmeasurement states after the i th measurement be $\phi_x^i = |\phi_x^i\rangle\langle\phi_x^i|$, with $|\langle\phi_0^i|\phi_1^i\rangle| = s_i$. To determine the criteria at which randomness can be simultaneously certified in all sequential measurements, we generalize the argument we employed in the two sequential measurement case to the N case. That is, each measurement needs to reproduce a rate of inconclusive events below the threshold, which can be reproduced by deterministic strategies. Thus, to certify randomness during the i th sequential measurement that receives pure states with overlap s_{i-1} , the condition

$$Q_i \leq \frac{1 + s_{i-1}^2}{2} = \frac{1}{2} \left(1 + \frac{\delta^2}{\prod_{j=0}^{i-1} Q_j^2} \right) \quad (28)$$

needs to be satisfied. In the equality, we used the fact that if maximum-confidence measurements are performed, the relation $s_i = \frac{s_{i-1}}{Q_i}$ has to hold, with $s_0 = \delta$ corresponding to the initial state preparations and $Q_0 = 1$. Therefore, if the condition in Eq. (28) holds $\forall i$, randomness can be simultaneously certified in all outcomes of the sequential measurements. In analogy with the example shown in Fig. 3, we take the case that the last measurement yields the minimum rate of inconclusive events compatible with a maximum-confidence measurement, this way consuming all certifiable randomness left after all posterior measurements, i.e., $Q_N = \frac{\delta}{\prod_{j=0}^{N-1} Q_j}$. In order to be able to certify randomness in all devices, the parameter δ needs to be the one that satisfies the condition $Q_N \geq Q_i$, $\forall i$, given that $Q_i \leq Q_{i+1}$ according to Eq. (28). We performed a numerical search for all δ that satisfy that condition. In Fig. 4, we show the bound $\delta \leq \Delta$ that needs to be satisfied in order to be able to sequentially certify randomness in N consecutive maximum-confidence measurements. In a nutshell, if the pure state preparations have an overlap lower bounded by δ , a set of n sequential measurements will be able to certify randomness if the value of δ is below the n th point in Fig. 4. As the number of parties increases, the bound Δ rapidly decreases, to a point that it is practically impossible to certify randomness in all sequential measurements, making it pointless to add subsequent measurements.

VI. DISCUSSION

We investigated the certification of randomness in sequential prepare-and-measure scenarios through maximum-confidence state discrimination. Our approach is semi-device-independent, where assumptions on devices can be significantly relaxed compared to more stringent device-independent approaches based on Bell scenarios. Centrally, we showed that quantum randomness, originating from the fundamental indistinguishability of nonorthogonal states, can be distributed and certified among multiple observers through maximum-confidence measurements.

From a technical point of view, we introduced rigorous methods to quantify randomness in sequential prepare-and-measure scenarios with trusted state preparation (including postmeasurement states) and uncharacterized measurements. By leveraging semidefinite programming techniques, we derived tight bounds on Eve's guessing probability, which directly translate into lower bounds on the certifiable min-entropy. Second, we generalized the sequential randomness certification framework to a setting where only the overlap of the (pure) state preparations is trusted. Here, the sequential structure was compactly encoded into effective operators, which allowed us to extend the certification methods to adaptive attack strategies and non-i.i.d. scenarios, and enabled the use of entropy accumulation methods. Our methods rely on semidefinite programming duality, ensuring their feasibility even in the presence of experimental imperfections that may render the observable frequencies with no physical realization. This makes the approach immediately applicable to realistic scenarios, where noise and limited control over devices are unavoidable.

From a foundational perspective, our analysis clarifies the subtle connection between quantum state discrimination and the distribution of randomness in sequential processes. Maximum-confidence measurements, in particular, emerge as strong candidates for certifying randomness, as they interpolate between well-known state discrimination strategies—in one extreme minimum error state discrimination and in the other unambiguous state discrimination—while reproducing extremal prepare-and-measure correlations. Deploying maximum-confidence measurements in the sequential scenario reveals that randomness is not an isolated property of a single measurement but can be shared among multiple parties. In light of previous approaches for sequential randomness certification, our work is the first that moves the bipartite framework to single-party measurements. This can be thought as translating the device-independent treatment in sequential schemes to semi-device-independent, in which the assumptions placed on the source play an important role. Namely, our analysis provided a sufficient criterion for simultaneously extracting randomness from a given number of sequential measurements, which only depends on the distinguishability of the initial state preparations. Furthermore, our results fit well with the unbounded-randomness certification scheme with sequential measurements in bipartite scenarios

from Ref. [24]. The key for having unbounded randomness stems from allowing the measurement in one particle from a bipartite state to admit twice as many measurement settings as sequential measurements on the other particle. Translated to our semi-device-independent framework, one can allow Alice to prepare twice as many distinct preparations as the number of sequential measurements, which effectively translates to a prepare-and-measure scenario with an arbitrarily large number of preparations and measurement outcomes, leading to arbitrarily large values of certified randomness [57].

The relevance of these findings extends well beyond the theoretical domain. Sequential prepare-and-measure implementations can be realized with relatively modest experimental resources, e.g., on integrated photonic platforms supporting nondestructive quantum measurements [58–60]. Likewise, optical systems provide a natural setting for the implementation of maximum-confidence measurements [61–64]. In photonic platforms, energy-related observables such as photon-number correlations or constraints on the vacuum component arise naturally as measurable quantities, and there is a growing body of research proposing semi-device-independent frameworks based on energetic constraints [65–68]. The approach introduced here is not confined to the specific scenario analyzed in this work. It can be extended to semi-device-independent frameworks defined by energy constraints, by reformulating the corresponding entropy optimization problem through appropriate semidefinite programming relaxations [69].

Finally, our results demonstrate that quantum unpredictability can be sequentially distributed, even under partial trust assumptions. This naturally raises the question of whether such distributed unpredictability can be harnessed beyond randomness certification, e.g., in semi-device-independent quantum key distribution. A particularly intriguing direction is the exploration of multipartite cryptographic schemes, such as quantum secret sharing and third-man quantum cryptography protocols [70,71], or sequential variants of the BB84 protocol [72], where additional collaborative measurements performed after the first receiver could enhance key generation rates, or even enable secure key distribution among multiple parties.

ACKNOWLEDGMENTS

C.R.C. was supported by the Wenner-Gren Foundations. J.B.B. acknowledges the Danish National Research Foundation grant bigQ (DNRF 142). H.L. acknowledges the financial support from the Business Finland project BEQAH. K.F. and J.B. were supported by NRF Korea (2021R1A2C2006309, 2022M1A3C2069728) and the IITP (RS-2023-00229524, RS-2025-02304540).

DATA AVAILABILITY

The data that support the findings of this article are openly available [73].

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C.

- Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
- [3] V. Mannalatha, S. Mishra, and A. Pathak, A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness, *Quantum Inf. Proc.* **22**, 439 (2023).
- [4] J. Barrett, L. Hardy, and A. Kent, No signaling and quantum key distribution, *Phys. Rev. Lett.* **95**, 010503 (2005).
- [5] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [6] U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, *Phys. Rev. Lett.* **113**, 140501 (2014).
- [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 C. Monroe, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
- [8] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, *J. ACM* **63**, 1 (2016).
- [9] A. Acín and L. Masanes, Certified randomness in quantum physics, *Nature (London)* **540**, 213 (2016).
- [10] J. S. Bell, On the einstein podolsky rosen paradox, *Phys. Phys. Fiz.* **1**, 195 (1964).
- [11] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [12] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, *Phys. Rev. A* **84**, 010302 (2011).
- [13] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes, *Phys. Rev. A* **85**, 052308 (2012).
- [14] Y.-Q. Zhou, F. Gao, D.-D. Li, X.-H. Li, and Q.-Y. Wen, Semi-device-independent randomness expansion with partially free random sources using $3 \rightarrow 1$ quantum random access code, *Phys. Rev. A* **94**, 032318 (2016).
- [15] M. Pivoluska, M. Plesch, M. Farkas, N. Ružicková, 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).
- [16] V. Mannalath and A. Pathak, Bounds on semi-device-independent quantum random-number expansion capabilities, *Phys. Rev. A* **105**, 022435 (2022).
- [17] 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).
- [18] R. Silva, N. Gisin, Y. Guryanova, and S. Popescu, Multiple observers can share the nonlocality of half of an entangled pair by using optimal weak measurements, *Phys. Rev. Lett.* **114**, 250401 (2015).
- [19] J. Bergou, E. Feldman, and M. Hillery, Extracting information from a qubit by multiple observers: Toward a theory of sequential state discrimination, *Phys. Rev. Lett.* **111**, 100501 (2013).
- [20] L. Masanes, A. Acín, and N. Gisin, General properties of nonsignaling theories, *Phys. Rev. A* **73**, 012112 (2006).
- [21] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Noncommuting mixed states cannot be broadcast, *Phys. Rev. Lett.* **76**, 2818 (1996).
- [22] R. Gallego, L. E. Würflinger, R. Chaves, A. Acín, and M. Navascués, Nonlocality in sequential correlation scenarios, *New J. Phys.* **16**, 033037 (2014).
- [23] P. J. Brown and R. Colbeck, Arbitrarily many independent observers can share the nonlocality of a single maximally entangled qubit pair, *Phys. Rev. Lett.* **125**, 090401 (2020).
- [24] 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).
- [25] B. Coyle, M. J. Hoban, and E. Kashefi, One-sided device-independent certification of unbounded random numbers, *Electron. Proc. Theor. Comput. Sci.* **273**, 14 (2018).
- [26] B. Coyle, E. Kashefi, and M. J. Hoban, Certified randomness from steering using sequential measurements, *Cryptography* **3**, 27 (2019).
- [27] J. Bowles, F. Baccari, and A. Salavrakos, Bounding sets of sequential quantum correlations and device-independent randomness certification, *Quantum* **4**, 344 (2020).
- [28] G. Foletto, M. Padovan, M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Experimental test of sequential weak measurements for certified quantum randomness extraction, *Phys. Rev. A* **103**, 062206 (2021).
- [29] X. Liu, Y. Wang, Y. Han, and X. Wu, Quantifying the intrinsic randomness in sequential measurements, *New J. Phys.* **26**, 013026 (2024).
- [30] M. Padovan, G. Foletto, L. Coccia, M. Avesani, P. Villoresi, and G. Vallone, Secure and robust randomness with sequential quantum measurements, *npj Quantum Inf.* **10**, 94 (2024).
- [31] S. Sarkar, Certification of unbounded randomness with arbitrary noise, *Phys. Rev. A* **111**, L010201 (2025).
- [32] H. Lee, K. Flatt, and J. Bae, Sequential quantum maximum-confidence discrimination, *Phys. Rev. A* **112**, 052206 (2025).
- [33] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, and J. Jeffers, Maximum confidence quantum measurements, *Phys. Rev. Lett.* **96**, 070401 (2006).
- [34] S. M. Barnett and S. Croke, Quantum state discrimination, *Adv. Opt. Photon.* **1**, 238 (2009).
- [35] H. Lee, K. Flatt, C. Roch i Carceller, J. B. Brask, and J. Bae, Maximum-confidence measurement for qubit states, *Phys. Rev. A* **106**, 032422 (2022).
- [36] C. Roch i Carceller and J. B. Brask, Contextuality witness inspired by optimal state discrimination, *Phys. Rev. A* **109**, 032202 (2024).
- [37] J. Bae, Structure of minimum-error quantum state discrimination, *New J. Phys.* **15**, 073037 (2013).
- [38] I. Ivanovic, How to differentiate between non-orthogonal states, *Phys. Lett. A* **123**, 257 (1987).
- [39] D. Dieks, Overlap and distinguishability of quantum states, *Phys. Lett. A* **126**, 303 (1988).
- [40] A. Peres, How to differentiate between non-orthogonal states, *Phys. Lett. A* **128**, 19 (1988).
- [41] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/vb68-jlr3> for a summary of sequential maximum confidence state discrimination and a derivation of the SDPs presented in the main text.

- [42] C. Roch i Carceller and A. Tavakoli, The role of entanglement in energy-restricted communication and randomness generation, *Quantum Sci. Technol.* **11**, 025020 (2026).
- [43] R. König, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, *IEEE Trans. Inf. Theory* **55**, 4337 (2009).
- [44] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, *Quantum* **1**, 14 (2017).
- [45] L. Vandenberghe and S. Boyd, Semidefinite programming, *SIAM Rev.* **38**, 49 (1996).
- [46] T. Metger, O. Fawzi, D. Sutter, and R. Renner, Generalised entropy accumulation, *Commun. Math. Phys.* **405**, 261 (2024).
- [47] 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).
- [48] R. Bhavsar, S. Ragy, and R. Colbeck, Improved device-independent randomness expansion rates using two sided randomness, *New J. Phys.* **25**, 093035 (2023).
- [49] L. Kamin, A. Arqand, I. George, N. Lütkenhaus, and E. Y.-Z. Tan, Finite-size analysis of prepare-and-measure and decoy-state quantum key distribution via entropy accumulation, *PRX Quantum* **6**, 020342 (2025).
- [50] T. V. Himbeek and S. Pironio, Correlations and randomness generation based on energy constraints, *arXiv:1905.09117*.
- [51] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Semi-device-independent heterodyne-based quantum random-number generator, *Phys. Rev. Appl.* **15**, 034034 (2021).
- [52] C. Roch i Carceller, J. Pauwels, S. Pironio, and A. Tavakoli, Prepare-and-measure scenarios with photon-number constraints, *Phys. Rev. Lett.* **135**, 140802 (2025).
- [53] C. R. Carceller, L. N. Faria, Z.-H. Liu, N. Sguerso, U. L. Andersen, J. S. Neergaard-Nielsen, and J. B. Brask, Improving semi-device-independent randomness certification by entropy accumulation, *Phys. Rev. A* **112**, 022430 (2025).
- [54] R. Renner, Security of quantum key distribution, *Int. J. Quantum Inf.* **06**, 1 (2008).
- [55] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, *Quantum* **8**, 1445 (2024).
- [56] G. H. Golub, Some modified matrix eigenvalue problems, *SIAM Rev.* **15**, 318 (1973).
- [57] 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).
- [58] M. A. Solís-Prosser, P. González, J. Fuenzalida, S. Gómez, G. B. Xavier, A. Delgado, and G. Lima, Experimental multi-party sequential state discrimination, *Phys. Rev. A* **94**, 042309 (2016).
- [59] M. Namkung and Y. Kwon, Sequential state discrimination of coherent states, *Sci. Rep.* **8**, 16915 (2018).
- [60] H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, Experimental characterization of unsharp qubit observables and sequential measurement incompatibility via quantum random access codes, *Phys. Rev. Lett.* **125**, 080403 (2020).
- [61] P. J. Mosley, S. Croke, I. A. Walmsley, and S. M. Barnett, Experimental realization of maximum confidence quantum state discrimination for the extraction of quantum information, *Phys. Rev. Lett.* **97**, 193601 (2006).
- [62] G. A. Steudle, S. Knauer, U. Herzog, E. Stock, V. A. Haisler, D. Bimberg, and O. Benson, Experimental optimal maximum-confidence discrimination and optimal unambiguous discrimination of two mixed single-photon states, *Phys. Rev. A* **83**, 050304 (2011).
- [63] S. Gómez, E. S. Gómez, O. Jiménez, A. Delgado, S. P. Walborn, and G. Lima, Experimental quantum state discrimination using the optimal fixed rate of inconclusive outcomes strategy, *Sci. Rep.* **12**, 17312 (2022).
- [64] L. F. Melo, M. A. Solís-Prosser, O. Jiménez, A. Delgado, and L. Neves, Experimental optimal discrimination of N states of a qubit with fixed rates of inconclusive outcomes, *Phys. Rev. Res.* **5**, 043149 (2023).
- [65] 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).
- [66] 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).
- [67] H. Tebyanian, M. Avesani, G. Vallone, and P. Villoresi, Semi-device-independent randomness from d -outcome continuous-variable detection, *Phys. Rev. A* **104**, 062424 (2021).
- [68] C. Roch i Carceller, Entanglement structure certification based on energy-restricted state discrimination, *New J. Phys.* **28**, 024509 (2026).
- [69] A. Tavakoli, A. Pozas-Kerstjens, P. Brown, and M. Araújo, Semidefinite programming relaxations for quantum correlations, *Rev. Mod. Phys.* **96**, 045006 (2024).
- [70] M. Żukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter, Quest for GHZ states, *Acta Phys. Pol. A* **93**, 187 (1998).
- [71] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Experimental quantum secret sharing and third-man quantum cryptography, *Phys. Rev. Lett.* **95**, 200502 (2005).
- [72] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [73] C. Roch i Carceller, Sequential-QRNG-with-MCM, 2025, <https://github.com/chalswater/Sequential-QRNG-with-MCM>.