

Composable Framework for Device-Independent State Certification

Rutvij Bhavsar^{1,*†‡}, Lewis Woollorton^{2,3,4,*§} and Joonwoo Bae^{1,||}

¹*School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea*

²*Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom*

³*Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1FD, United Kingdom*

⁴*Inria, École normale supérieure (ENS) de Lyon, Laboratoire de l'Informatique du Parallélisme (LIP), 46 Allée d'Italie, 69364 Lyon Cedex 07, France*

 (Received 11 June 2025; revised 4 September 2025; accepted 16 October 2025; published 5 December 2025)

Certifying a quantum state in a device-independent (DI) manner, in which no trust is placed on the internal workings of any physical components, is a fundamental task bearing various applications in quantum information theory. The composability of a state-certification protocol is key to its integration as a subroutine within information-theoretic protocols. In this work, we present a composable certification of quantum states in a DI manner under the assumption that a source prepares a finite sequence of independent quantum states that are not necessarily identical. We show that the security relies on the DI analog of the fidelity, called the *extractability*. We develop methods to compute this quantity under local operations and classical communication in certain Bell scenarios that self-test the singlet state, which may also be of independent interest. Finally, we demonstrate our framework by certifying the singlet state in a composable and DI manner using the Clauser-Horne-Shimony-Holt inequality.

DOI: [10.1103/1j5f-qjhx](https://doi.org/10.1103/1j5f-qjhx)

I. INTRODUCTION

Certifying the nonclassical properties of a source is essential for its use in quantum information processing. This is often achieved by modeling the physical mechanisms which govern either the behavior of the source directly, or the measurements used to characterize it. However, deviations between a realistic implementation and this model are difficult to rule out, and any assumptions which are not met in practice could render the certification invalid. The device-independent (DI) approach [1–5] addresses this issue. Here, certification is obtained through the observation of nonlocal input-output correlations, removing the need to understand the inner workings of the source or perform trusted measurements.

The aim of DI state certification (DISC) is to certify the presence of a certain multipartite “target” state in a state that is stored in the memory of the user(s). Recently, there have been significant advances in DISC [6,7], in which the states and measurements are treated as (separate) black boxes, and tools from robust self-testing [8–10] enable certification when the source is not assumed to be independent and identically distributed (IID), and the collected statistics are finite. A related protocol has also been outlined in Refs. [11,12], where DI lower bounds on the rate of distillable entanglement have been derived for non-IID sources. Such protocols have also been successfully demonstrated experimentally [13–15].

However, when using any protocol as a subroutine in a larger system, a notion of composability is essential. For example, in cryptography [1–4,16–24], composable security statements ensure that the concatenation of two secure protocols results in another secure protocol [25,26]. A composable approach to DISC is therefore crucial if the stored state is intended for many practical purposes.

Here, we address the need for the framework of composable certification and present composable guarantees for DISC protocols, enabling their integration as subroutines in broader information-theoretic tasks, such as cryptography. Furthermore, our protocols only assume that finitely many independent states are emitted by the source, from which a single state is randomly selected and preserved

*These authors contributed equally to this work.

†Contact author: rutvij.bhavsar@kcl.ac.uk

‡Current affiliation: Department of Mathematics, King’s College London, Strand, London, WC2R 2LS, United Kingdom.

§Contact author: lewis.woollorton@ens-lyon.fr

||Contact author: joonwoo.bae@kaist.ac.kr

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.

in a memory for future applications. The remaining states then interact with measurement devices that can have a memory in general, and the statistics are used to certify the preserved state.

We prove the security of our protocol using the *extractability*, a DI variant of the fidelity between each measured state and the target [10,27]. A bound on the extractability follows from observing a Bell inequality violation, and we provide a generic way to compute this quantity in Bell scenarios with binary inputs and binary outputs [28], which may be of independent interest in the context of nonlocality and entanglement theory. Specifically, the standard definition of extractability quantifies how robust a self-test is, by measuring the minimal distance between a “physical” state which produces a given Bell violation and the target state. This distance is typically computed after applying local operations to the physical state, accounting for degrees of freedom undetectable from the statistics alone [29]. However, this notion can be restrictive in the context of state-certification protocols, where the relevant class of *free operations* may depend on both the intended application and the experimental setup. For example, in cryptographic settings, it is natural to consider local operations and classical communication (LOCC) as the allowed free operations. Our security framework can be applied to any chosen class of operations, and we propose a method to compute bounds on the extractability under LOCC for any Bell inequality in the minimal Bell scenario certifying the singlet state. As LOCC extractability is typically greater than that obtained under local operations alone, our protocols benefit from tighter security bounds than those derived using the standard approach.

The paper is structured as follows. In Secs. II and III we provide the necessary background. In Sec. IV we introduce the measurement scenarios considered. Section V then outlines the corresponding DISC protocols. A composable security framework is then presented in Sec. VI, and in Sec. VII we bound the security of the introduced protocols according to this definition. Section VIII discusses the main tool needed to provide security, namely, how to bound the extractability. We then provide an explicit example using the Clauser-Horne-Shimony-Holt (CHSH) inequality in Sec. IX, and conclude with a discussion in Sec. X. Technical details of the protocols and assumptions are provided in the Supplemental Material [30, Secs. 1 and 2], along with the full proofs of all security claims [30, Secs. 3–5]. A detailed derivation of the extractability bounds appears in the Supplemental Material [30, Sec. 6].

II. PRIOR WORK

Certifying properties of entangled states in a device-independent fashion has been extensively studied. Often considered is the amount of private randomness contained in the measurement outcomes, as a function of the

observed Bell violation. This can be estimated in the asymptotic regime [2,31–33], and lifted to the finite-size setting using tools such as the entropy accumulation theorem [34–36] and the quantum probability estimation framework [37], enabling composable secure DI randomness expansion [3,4,21–23], amplification [24,38], and key distribution [1,2,16,17,19,20].

A stronger characterization of the source is possible by estimating properties of the emitted states directly, rather than the measurements performed on them. For example, various entanglement measures can be quantified as a function of the observed Bell violation in the asymptotic regime [11,39]. In the finite-size regime, Refs. [11,12] certify the largest number of maximally entangled states that can be extracted from an untrusted source under LOCC operations, a quantity known as the one-shot distillable entanglement. This protocol outputs a subset of states (intended for a future task) which the entanglement certification applies to, and does not require an IID assumption on the source.

DISC achieves the strongest type of characterization, namely, that the states emitted by the source are close to (many copies of) a target state. Bancal *et al.* [6] have provided a DI state-verification protocol (in which all states are measured; see Ref. [7] for a detailed comparison between verification and certification) using the CHSH inequality. Notably, this protocol does not require an IID assumption on the source and has been used to verify the successful distribution of entangled states via a quantum network link. Gočanin *et al.* [7] have later developed a general framework for DI state verification based on any robust self-testing result. This approach achieves an optimal sample efficiency in the fully non-IID setting. The authors of Ref. [7] have further proposed a framework for DI state certification, which outputs multiple certified copies with an optimal sample efficiency under the assumption of an independently distributed source.

In the framework of Refs. [6,7], the average extractability of the state ensemble is certified up to a fixed confidence level. This contrasts the definition of composable security adopted in cryptography, such as quantum key distribution (QKD), in which the distinguishability between an idealized version of the protocol and its real implementation is shown to be small [25,26]. Applying such a framework to DISC is one of the new contributions of our work. Inspired by Ref. [7], we present a general framework for DISC based on extractability under the assumption of independent states. The key difference is that we introduce and apply a composable security definition inspired by quantum cryptography. We do however lose the sample efficiency achieved in Ref. [7], a trade-off which is necessary in the case of exact certification (see Sec. V for a discussion of different types of certification) owing to the inherently stronger demand of composable security [40]. As a proof-of-principle demonstration, we also consider

certifying a single copy of the target state. Extending our framework to the certification of multiple copies in a sample-efficient and fully non-IID manor is a promising future direction, which we elaborate on in Sec. X. Additionally, while composability is not directly addressed in Refs. [11,12], we expect that an analysis similar to the one presented here would directly apply to one-shot distillable entanglement certification. However, as aforementioned, certifying the state directly as considered in this work and Refs. [6,7] is a stronger demand than certifying its distillable entanglement.

III. NONLOCALITY AND SELF-TESTING

We now review self-testing, which can be viewed as a form of DI state verification in the asymptotic limit. Consider a bipartite Bell scenario, in which two noncommunicating devices perform local measurements on some unknown shared quantum state. The inputs to each device are uniformly distributed binary random variables, denoted X and Y , respectively. The outputs of each device are binary random variables, denoted A and B , which for a given pair of inputs $X = x, Y = y$ are distributed according to the behavior of the device, $\mathbf{p} = \{p(a, b|x, y)\}$. A behavior is quantum if it can be realized by local quantum measurements on a bipartite state $\rho \in \mathcal{S}(\mathcal{H}_{Q_A} \otimes \mathcal{H}_{Q_B})$, where $\mathcal{S}(\mathcal{H})$ denotes the set of normalized states on a Hilbert space $\mathcal{H}$. Specifically, the probabilities are given by the Born rule, $p(a, b|x, y) = \text{tr}[(M_{a|x} \otimes N_{b|y})\rho]$, where $\{\{M_{a|x}\}_{a \in \{0,1\}}\}_{x \in \{0,1\}}$ and $\{\{N_{b|y}\}_{b \in \{0,1\}}\}_{y \in \{0,1\}}$ are positive operator-valued measures (POVMs) on $\mathcal{H}_{Q_A}$ and $\mathcal{H}_{Q_B}$, respectively.

In certain cases, a given quantum behavior $\mathbf{p}^* = \{p^*(a, b|x, y)\}$ guarantees the presence of a particular state $|\psi^*\rangle$ up to operations which cannot be detected from the behavior, called local isometries. If this is the case, we say that the behavior $\mathbf{p}^*$ *self-tests* $|\psi^*\rangle$ [8,27]. Such statements are the strongest form of verification possible. However, in noisy systems it is often the case that the behavior $\mathbf{p}^*$ cannot be achieved exactly. We say that $\mathbf{p}^*$ *robustly* self-tests $|\psi^*\rangle$ if witnessing a behavior $\mathbf{p}'$ ϵ -close to $\mathbf{p}^*$ guarantees the presence of a state ρ' ϵ -close to $\psi^* = |\psi^*\rangle\langle\psi^*|$, according to a given metric (see, e.g., Ref. [27] for a definition). Robust self-testing can thus be viewed as a form of DI state verification when given access to infinitely many copies of an identical (potentially noisy) state.

Self-testing statements can also be formulated without relying on the full input-output distributions. One approach is to express them in terms of functionals of the behavior, which may be nonlinear in general [41]. However, the most common and often more practical method is to use linear functionals, which correspond to Bell inequalities [42,43].

In the minimal Bell scenario, it will be convenient to work with the expected values $\langle A_x \rangle = \sum_a (-1)^a p(a|x)$, $\langle B_y \rangle = \sum_b (-1)^b p(b|y)$, and $\langle A_x B_y \rangle =$

$\sum_{a,b} (-1)^{a+b} p(a, b|x, y)$. When the behavior is quantum, we define the associated observables $A_x = \sum_a (-1)^a M_{a|x}$ and $B_y = \sum_b (-1)^b N_{b|y}$, which satisfy $\langle A_x B_y \rangle = \text{tr}[(A_x \otimes B_y)\rho]$, $\langle A_x \rangle = \text{tr}[(A_x \otimes \mathbb{I}_{Q_B})\rho]$ and $\langle B_y \rangle = \text{tr}[(\mathbb{I}_{Q_A} \otimes B_y)\rho]$. A Bell expression is then a linear combination of the probabilities $\{p(a, b|x, y)\}$, or equivalently the expectations $\{\langle A_x \rangle, \langle B_y \rangle, \langle A_x B_y \rangle\}$, and for quantum behaviors we consider Bell operators of the form [44]

$$B = \sum_{x,y \in \{-1,0,1\}} c_{xy} A_x \otimes B_y, \quad (1)$$

for some real coefficients c_{xy} , where we have defined $A_{-1} := \mathbb{I}_{Q_A}$ and $B_{-1} := \mathbb{I}_{Q_B}$. The Bell value is given by $\langle B \rangle = \text{tr}[B\rho]$ for a state ρ , and the maximum quantum and classical values of $\langle B \rangle$ are denoted by η^Q and η^L , respectively. A Bell inequality $\langle B \rangle \leq \eta^L$ self-tests a state $|\psi^*\rangle$ if every quantum state which achieves $\langle B \rangle = \eta^Q$ is equivalent to $|\psi^*\rangle$ up to local isometries.

Of particular interest to this work are Bell inequalities which self-test the maximally entangled pair of qubits, $\phi^+ = |\phi^+\rangle\langle\phi^+|$, where $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Such inequalities have been fully characterized in the minimal Bell scenario [45–48]. An important example is that due to Clauser, Horne, Shimony, and Holt [43], which is the only non-trivial facet Bell inequality in this scenario up to relabelings. Its Bell operator takes the form $B_{\text{CHSH}} := A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)$, and has local and quantum bounds of 2 and $2\sqrt{2}$, respectively.

IV. MEASUREMENT SCENARIOS

Real sources emit a finite sequence of non-IID states. Furthermore, a real measurement device may also be non-IID, e.g., through the use of a memory. It is then clear that, on their own, self-testing statements are not enough for state verification or certification in practice. To address this, we consider certifying a source which emits n independent but not necessarily identical states, $\rho = \bigotimes_{i=1}^n \rho_i$, where $\rho_i \in \mathcal{S}(\mathcal{H}_{Q_i^A} \otimes \mathcal{H}_{Q_i^B})$. We also assume that the user has access to a quantum memory in which states can be stored, and treat all measurement devices as black boxes, making no assumptions on their internal workings.

Associated to each index i is a channel, $\mathcal{N}_i^A : I_i^A Q_i^A \rightarrow A_i X_i O_i^A$, shown in Fig. 1. The systems $A_i X_i$ are classical, while I_i^A contains any auxiliary information available to the device prior to measurement (e.g., information from previous rounds), and O_i^A contains auxiliary output information (e.g., information to pass on to future rounds). The channel $\mathcal{N}_i^A$ first samples the input X_i and then performs the corresponding measurement on the (quantum) system held by the measurement device. Thus, while X_i serves as an input to the measurement device, from this perspective it is naturally regarded as an output of the channel $\mathcal{N}_i^A$. We similarly define channels $\mathcal{N}_i^B : I_i^B Q_i^B \rightarrow B_i Y_i O_i^B$. A joint

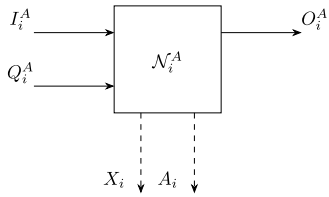


FIG. 1. The channels that represent measurements on Alice's side. The channels on Bob's side have an identical structure. Solid lines indicate quantum systems, while dashed lines represent classical systems. I_i^A and O_i^A represent auxiliary information available to, and generated by, the measurement of Q_i^A , respectively. The generation of Alice's input X_i is absorbed as part of the channel output, while A_i represents the output of a quantum measurement.

channel $\mathcal{N}_i$ is described by performing $\mathcal{N}_i^A$ and $\mathcal{N}_i^B$ in a spacelike separated manner, i.e., $\mathcal{N}_i = \mathcal{N}_i^A \otimes \mathcal{N}_i^B$. Then, the systems $X_i Y_i$ and $A_i B_i$ denote the inputs and outputs to the Bell test, respectively.

We then consider two possible arrangements of the channels $\{\mathcal{N}_i\}_{i=1}^n$, corresponding to parallel and sequential setups. In the parallel setup, $n - 1$ isolated measurement devices M_i each receive ρ_i and implement the channel $\mathcal{N}_i$. Following the isolation of the devices, the auxiliary systems $I_i^A O_i^A$ and $I_i^B O_i^B$ can be omitted, and all measurements occur simultaneously. This can be equivalently viewed as the action of a single memoryless measurement device acting on each system sequentially. We illustrate this scenario in Fig. 2.

In the sequential scenario, we consider a single measurement device M , which performs all channels in sequence.

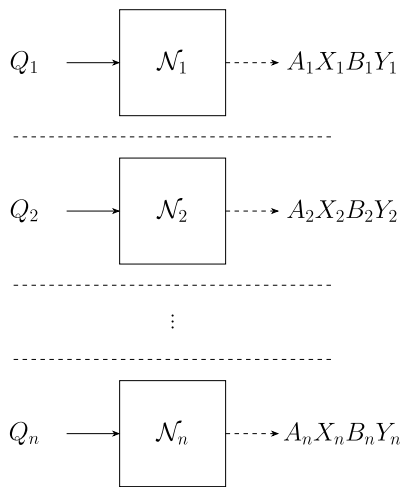


FIG. 2. The parallel setup, in which $n - 1$ devices each perform an isolated measurement on a composite quantum system $Q_i = Q_i^A Q_i^B$. Each measurement is performed in an isolated manner with respect to the AB partition.

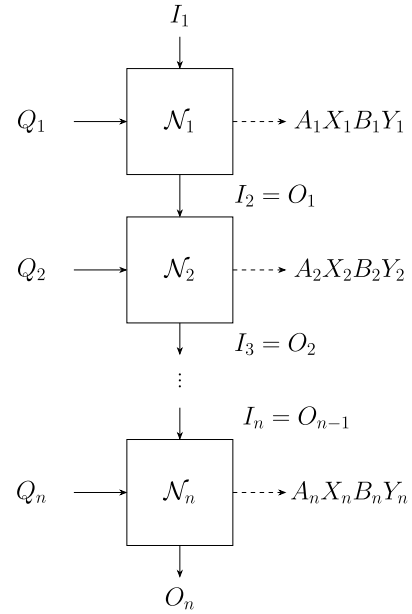


FIG. 3. The sequential setup, in which a single device performs all channels $\mathcal{N}_i$ in a sequence on the systems $Q_i = Q_i^A Q_i^B$. The auxiliary information $O_i = O_i^A O_i^B$ generated by $\mathcal{N}_i$ is fed forward as the input register $I_{i+1} = I_{i+1}^A I_{i+1}^B$ for the subsequent measurement $\mathcal{N}_{i+1}$.

Specifically, the measurement of ρ_i precedes that of ρ_{i+1} , and the auxiliary output O_i^A is sent to the input I_{i+1}^A (and similarly for B). In other words, we associate $I_{i+1}^A = O_i^A$ and $I_{i+1}^B = O_i^B$. Information in O_i^A could, e.g., consist of the inputs and outputs of rounds $i - 1$. Note that systems pertaining to A and B are still assumed to be separated, e.g., O_i^A cannot influence I_{i+1}^B . See Fig. 3 for an illustration.

We also introduce a random variable T , which takes values in $t \in \{1, \dots, n\}$ according to a known distribution $\Pr[T = t] = p_T(t)$, and is sampled prior to all measurements. Specifically, the value of T decides which state is not measured and, instead, held in the quantum memory. Note that the variables T , X , and Y are all sampled from distributions known to the users. While these distributions may also be known to the adversary, the adversary cannot access the actual realized values of T , X , or Y . For a detailed list of the assumptions made in this work, see the Supplemental Material [30, Sec. 1].

V. PROTOCOLS

We consider DISC protocols of the following form. First, the state $\bigotimes_{i=1}^n \rho_i$ is prepared by an untrusted source, and accepted into the secure laboratory. The random variable T is generated, and depending on its value, $T = t$, the state ρ_i is stored in a quantum memory. Next, the remaining states are sent to the measurement device, and either the parallel or sequential measurement setup is performed. The statistics are collected, and if they deviate from an expected

value, the protocol aborts. Specifically, Protocols 1–3 consist of a parallel setup, while Protocols 4 and 5 consist of a sequential setup (see the Supplemental Material [30, Sec. 2] for details).

In the event of not aborting, there are two possible variants of the protocol. In the first, the user applies a predecided channel (from the set of free operations) to the state stored in memory, with the aim of “extracting” a target state (Protocols 1, 2, and 4 in the Supplemental Material [30, Sec. 2]). However, performing this channel in practice may be unrealistic. Thus, in another variant, the user certifies the state held in memory to be equivalent to (i.e., has the potential to be converted to) the target up to the set of free operations (Protocols 3 and 5 in the Supplemental Material [30, Sec. 2]).

We also allow for freedom in the choice of target state. In Protocol 1, we consider extracting the target state ψ^* (e.g., the maximally entangled state) exactly. Due to imperfections such as noise, however, this is out of reach for many practical applications, resulting in an overly stringent security criterion. Instead, the user may wish to relax this, and extract a state ε -close to ψ^* [49], or guarantee that the final state can be converted to any state ε -close to ψ^* under free operations. We allow for this modification in Protocols 2–5 in the Supplemental Material [30, Sec. 2], where the distance of interest is the trace distance.

Additionally, we note that while the protocols outlined thus far are concerned with storing and certifying a single state, the proof techniques can be generalized to multiple states. However, the current bounds scale poorly with the number of states measured, and we leave improvements in sample efficiency, such as that presented in Ref. [7], to future work (see Sec. X for further discussion).

We provide a template for all protocols considered in this work below, followed by a summary of each variant in Table I. All variants are outlined in detail in the Supplemental Material [30, Sec. 2].

TABLE I. A summary of all the protocols provided in this paper. “Setup” denotes the choice of measurement apparatus described in Sec. IV. “Target” indicates whether the final state is assessed to be close to a particular pure entangled state ψ^* , or any state ε -close to ψ^* for some $\varepsilon > 0$. “Extraction channel” indicates whether an extraction channel (within the chosen class of free operations) is applied to the final state or not. In general, such a channel cannot be implemented in a device-independent fashion. Note that the assumptions of the parallel setup can also be satisfied using a single memoryless measurement device.

Protocol	Setup	Target	Extraction channel
1	Parallel	ψ^*	Yes
2	Parallel	ε -close to ψ^*	Yes
3	Parallel	ε -close to ψ^*	No
4	Sequential	ε -close to ψ^*	Yes
5	Sequential	ε -close to ψ^*	No

Example 1 (CHSH-based DISC for the sequential setup). Consider a source that produces n bipartite states $\{\rho_i\}_{i=1}^n$. The goal is to certify that one of these states is ε -close to the maximally entangled pair of qubits $|\phi^+\rangle\langle\phi^+|$, in the sense that it can be converted by LOCC operations to some state τ that is ε -close to $|\phi^+\rangle\langle\phi^+|$. The protocol begins by choosing an index $t \in \{1, \dots, n\}$ at random and storing the corresponding state ρ_t in a memory. The remaining $n - 1$ states are sent one by one to the same pair of noncommunicating measurement devices [50].

In every round $i \neq t$, each device receives a binary input x_i (respectively, y_i) chosen at random, and performs an unknown measurement on their share of the state ρ_i , producing a binary output a_i (respectively, b_i). A CHSH game is won in round i if the outputs satisfy $a_i \oplus b_i = x_i \cdot y_i$, and is lost otherwise. From the $n - 1$ measurement rounds, the empirical CHSH value is then computed, i.e., a value proportional to the number of rounds in which the CHSH game was won divided by $n - 1$.

Depending on the desired security requirement—namely, the soundness and completeness parameters introduced in Sec. VI—an abort threshold for the CHSH value is chosen. If the empirical value does not exceed this value, the protocol aborts. Otherwise, the protocol accepts, and the stored state ρ_t is certified to be ε -close to $|\phi^+\rangle\langle\phi^+|$ under LOCC operations and up to the chosen security requirement. Intuitively, a smaller ε corresponds to a stricter acceptance condition: e.g., exact certification of the target state requires the observed CHSH value to be very close to the maximal quantum value $2\sqrt{2}$.

Template protocol

Parameters:

$n \in \mathbb{N}^+$ —number of rounds.

p_T —probability distribution of T .

$\omega_{\sharp}$ —expected value of the Bell functional.

$\kappa > 0$ —parameter to set completeness error (see Definition 2).

$\varepsilon \geq 0$ —closeness parameter (see Table I).

- (1) Generate a random number T according to p_T . If $T = t$, then store the state ρ_t in the memory.
- (2) Generate the input strings $\mathbf{X} = (X_1, \dots, X_n)$ and $\mathbf{Y} = (Y_1, \dots, Y_n)$ uniformly.
- (3) Depending upon the setup (see Table I and Sec. IV), perform the Bell tests using the generated input strings.
- (4) Estimate the Bell parameter ω_{exp} using the input-output statistics. If $\omega_{\text{exp}} \leq \omega_{\sharp} - \kappa$, then abort the protocol.

- (5) (Optional). From ρ_t , extract a state $\tilde{\rho}$ that is ε -close to the target state ψ^* .

VI. COMPOSABLE FRAMEWORK FOR DEVICE-INDEPENDENT STATE CERTIFICATION

Having outlined the protocol structure, here we introduce a composable security definition for DISC. The security of any protocol must be rigorously defined, and the desired definition depends on its intended application. In cryptographic scenarios, the *composable security definition* [18,25,26,51–54] has been adopted as the gold standard. This definition is particularly valuable since it enables a protocol to be securely integrated into a larger, composite system as a subroutine, and typically consists of two error parameters: ϵ_s , known as the *soundness error* (see Definition 1), and ϵ_c , known as the *completeness error* (see Definition 2).

To illustrate the importance of composability in a state-certification context, consider one of the DISC protocols described in Sec. V. A possible application is to use the certified state to generate a bit of secret key. This key might subsequently serve as input to another cryptographic protocol. Thus, proving the security of the DISC protocol in isolation is insufficient; we require a security definition that is robust enough to guarantee security when the protocol is used as a building block within a larger system.

In noncryptographic contexts, security proofs often involve statements such as: *If the protocol does not abort, it outputs the desired state with a small failure probability*. However, such statements are generally not composable. For instance, consider an extreme adversarial strategy where the adversary sends copies of separable states in each round. By sheer luck, this strategy may achieve a large observed Bell value, despite being exceedingly unlikely. In this case, while the protocol mostly aborts, there remains a nonzero probability that it succeeds with an insecure output. If this output is then used in subsequent protocols (such as QKD) security guarantees break down, since conditioned on not aborting, the output state is always separable. By defining security conditioned on not aborting, the negligibly small probability that this attack succeeds has not been accounted for. In fact, the overall protocol is trivially secure under this attack since it almost always aborts.

Another example of insecurity arises from abort-based attacks. An adversary could manipulate the protocol to abort selectively in ways that are advantageous to them. For instance, consider a scenario in which the adversary supplies the state

$$\rho = \sigma_1 \otimes \psi^* \otimes \psi^* \otimes \cdots \otimes \psi^*,$$

where σ_1 is a separable state and the remaining states are target states (ψ^*). The adversary could further instruct the devices to perform optimal measurements on ψ^* whenever a specific setting (e.g., $t = 1$) is chosen. For all other settings, the adversary forces suboptimal measurements, ensuring the protocol aborts. In such a scenario, whenever the protocol does not abort, the user is left with a separable state. Consequently, any future protocol relying on the nonaborting behavior of the DISC protocol is rendered insecure.

Adaptive adversarial strategies such as exploiting rare successful outcomes with separable states or leveraging abort-based attacks illustrate the inadequacy of non-composable security definitions. Specifically, while such attacks can never be ruled out, they can be tolerated using a composable definition, as we illustrate below. This is essential to ensure that security guarantees remain even when the protocol is integrated into a larger protocol.

To prove that a protocol is composable secure, it is necessary to define an *ideal protocol* (see, e.g., Refs. [26, 55,56]), which aborts with the same probability as the real protocol, and produces a perfect output whenever it does not abort. Importantly, the ideal case is a hypothetical construct that cannot be implemented in practice—it represents a theoretically perfect protocol. A real protocol is then deemed secure if it is virtually indistinguishable from this ideal. Specifically, security is quantified via a hypothetical game, in which the user performs either the real or ideal protocol. A third party, referred to as the *distinguisher*, is then tasked with identifying which protocol the user is running, with their success probability measuring security. Since the success probability of distinguishing two quantum states can be quantified using the trace distance, we define the following soundness criteria.

Definition 1 (Soundness). A DISC protocol is ϵ_s -sound if

$$\frac{1}{2} \|\rho_{\text{real}} - \rho_{\text{ideal}}\|_1 \leq \epsilon_s, \quad (2)$$

where ρ_{real} and ρ_{ideal} are the real and ideal protocol outputs, respectively, and $\|M\|_1 = \text{tr}\sqrt{M^\dagger M}$ is the trace norm of an operator M .

Note that when computing the distinguishing probability, the distinguisher is assumed to have access to all available side information, along with the output of the real protocol. However, they cannot access any private data generated during the execution of the protocol.

Appropriately defining an ideal protocol can be challenging in general, since one must demonstrate indistinguishability under all possible circumstances. For DISC, however, the choice is relatively straightforward, and is inspired by existing definitions in QKD. We consider an

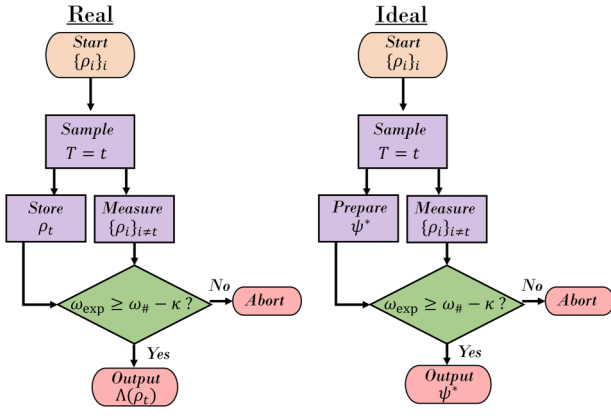


FIG. 4. A flow diagram describing the structure of the real and ideal DISC protocols. Here, $\{\rho_i\}_{i=1}^n$ denotes a sequence of independent states emitted by the source, T is a uniform random variable which takes values $t \in \{1, \dots, n\}$, and $\{\rho_i\}_{i \neq t}$ is shorthand for $\{\rho_i : i \in \{1, \dots, n\} \setminus t\}$. The empirical Bell value obtained by measuring $\{\rho_i\}_{i \neq t}$ is denoted ω_{exp} , while $\omega_{\#} - \kappa$ is the threshold Bell value below which the protocol aborts. For simplicity, we illustrate the variant in which the user outputs the extracted state $\Lambda(\rho_t)$.

ideal DISC protocol which outputs the target state (or an equivalent state up to free operations if the final extraction step is omitted) whenever the protocol does not abort. Furthermore, the ideal protocol aborts with the same probability as the real protocol. Note, however, that this abort probability is not revealed to the user. Similarly, if the goal is to certify a state that is ε -close (in trace distance) to the target state, the ideal protocol outputs any state ρ which is ε -close to ψ^* . A flow diagram comparing the real and ideal DISC protocol can be found in Fig. 4, and we provide technical details for all protocol variants in the Supplemental Material [30, Secs. 3 and 4].

The soundness definition given above ensures that the real protocol is virtually indistinguishable from an ideal one, even under arbitrary adversarial strategies. This includes the aforementioned extreme cases in which the protocol frequently aborts. In such situations, both the real and ideal protocols abort with high probability and are therefore nearly indistinguishable, and hence secure. Specifically, an ε_s -sound DISC protocol ensures that an abort based attack can only succeed with probability no larger than ε_s .

However, if soundness is used as the sole criterion for security, a critical issue arises: a protocol that always aborts would trivially be considered secure, despite being of no practical use. To rule out such degenerate cases, we additionally require that there exists an honest implementation of the protocol that succeeds with high probability. This is captured by the notion of completeness error.

Definition 2 (Completeness). A DISC protocol is said to be ε_c -complete if there exists an honest implementation that aborts with probability at most ε_c .

An honest implementation of the protocol is a source and set of measurement devices that model the expected behavior of an experimental implementation.

Example 2 (Honest implementation of a CHSH-based DISC protocol). As a concrete example, recall the CHSH-based protocol discussed in the previous section (Example 1). An example of an honest implementation in this context is a source $\mathbf{S}$ and measurement devices $\mathbf{M}$ with the following description. The source prepares n identical states $\{\rho_i\}_{i=1}^n$ of the form

$$\rho_i = (1 - \mu)|\phi^+\rangle\langle\phi^+| + \mu\frac{\mathbb{I}_4}{4},$$

where $\mu \in [0, 1]$ (e.g., one may take $\mu = (4/3)\varepsilon$ to match a desired robustness parameter $\frac{1}{2}\|\rho_i - \phi^+\|_1 = \varepsilon$) and $\mathbb{I}_4$ is the identity operator in dimension 4. The measurement devices perform the CHSH projective measurements with observables [57]

$$A_0 = \sigma_x, \quad A_1 = \sigma_z, \\ B_0 = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x), \quad B_1 = \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x),$$

where σ_x , σ_y , and σ_z are the Pauli operators. Under these settings, the expected value of the CHSH functional for the honest implementation $(\mathbf{S}, \mathbf{M})$ is

$$\omega(\mathbf{S}, \mathbf{M}) = \text{tr}[\rho_i B_{\text{CHSH}}] = (1 - \mu)2\sqrt{2}.$$

To achieve an ε_c -complete protocol, one should compute a small deviation $\kappa > 0$ in the observed empirical value ω_{exp} such that

$$\Pr[\omega_{\text{exp}} \geq \omega(\mathbf{S}, \mathbf{M}) - \kappa] \geq 1 - \varepsilon_c.$$

We refer the reader to the Supplemental Material [30, Sec. 3] for an example of this calculation.

Remark 1. An honest implementation is one concrete intended realization of the protocol (honest source and devices) that could be implemented in the laboratory; it serves as a guarantee that acceptance occurs with high probability for well-behaved devices. This is not to be confused with the ideal protocol in the definition of soundness (Definition 1): when proving soundness, we do not assume that the devices behave honestly.

Combining both completeness and soundness yields a complete notion of security within the composable framework.

Definition 3 (Security). A DISC protocol is (ϵ_s, ϵ_c) -secure if it is both ϵ_s -sound and ϵ_c -complete.

Specifically, this definition ensures that security is preserved when the protocol is composed with other information-theoretic tasks. In particular, if a subsequent protocol is ϵ'_s -sound, then the combined protocol that includes both the DISC protocol and the subsequent protocol will be $(\epsilon_s + \epsilon'_s)$ -sound.

More concretely, consider a sequence of states $\rho_{\text{init}} = \bigotimes_{i=1}^n \rho_i$ which are certified by a DISC protocol $\mathcal{P}_1$, the output of which is given by $\mathcal{P}_1(\rho_{\text{init}}) = \rho_{\text{real}}$, where $\mathcal{P}_1(\cdot)$ is a quantum channel describing the action of the protocol. Let ρ_{ideal} denote the ideal output state of $\mathcal{P}_1$, and suppose that $\mathcal{P}_1$ is ϵ_1 -sound according to Definition 1, i.e.,

$$\frac{1}{2} \|\rho_{\text{real}} - \rho_{\text{ideal}}\|_1 \leq \epsilon_1.$$

Let $\mathcal{P}_2$ be a quantum channel describing the action of a subsequent protocol, which is ϵ_2 -sound. In particular, $\mathcal{P}_2$ satisfies

$$\frac{1}{2} \|\mathcal{P}_2(\rho_{\text{ideal}}) - \sigma_{\text{ideal}}\|_1 \leq \epsilon_2,$$

where σ_{ideal} is the ideal output state of $\mathcal{P}_2$. What can we say about the composition $\mathcal{P}_2 \circ \mathcal{P}_1$ when acting on ρ_{init} ? Using the triangle inequality and the soundness of $\mathcal{P}_2$,

$$\begin{aligned} & \frac{1}{2} \|\mathcal{P}_2 \circ \mathcal{P}_1(\rho_{\text{init}}) - \sigma_{\text{ideal}}\|_1 \\ & \leq \frac{1}{2} \|\mathcal{P}_2 \circ \mathcal{P}_1(\rho_{\text{init}}) - \mathcal{P}_2(\rho_{\text{ideal}})\|_1 + \epsilon_2. \end{aligned}$$

By the contractivity of the trace distance under quantum channels (see, e.g., [58, Exercise 9.1.9]),

$$\begin{aligned} & \frac{1}{2} \|\mathcal{P}_2 \circ \mathcal{P}_1(\rho_{\text{init}}) - \mathcal{P}_2(\rho_{\text{ideal}})\|_1 \\ & \leq \frac{1}{2} \|\mathcal{P}_1(\rho_{\text{init}}) - \rho_{\text{ideal}}\|_1 \leq \epsilon_1, \end{aligned}$$

where the second equality follows from the soundness of $\mathcal{P}_1$. Combining these facts,

$$\frac{1}{2} \|\mathcal{P}_2 \circ \mathcal{P}_1(\rho_{\text{init}}) - \sigma_{\text{ideal}}\|_1 \leq \epsilon_1 + \epsilon_2.$$

Thus, the protocol formed by composing $\mathcal{P}_1$ and $\mathcal{P}_2$ remains (at least) additively secure. A high level of security for the composite protocol can therefore be achieved whenever the individual protocols are themselves highly secure.

VII. SECURITY PROOF

We are now ready to present our main result: proving that the DISC protocol described in Sec. V is secure, according to the composable definition given in Sec. VI. For simplicity, we choose the target state to be the maximally entangled state $|\psi^*\rangle = |\phi^+\rangle$. However, the proof technique is general enough to replace $|\phi^+\rangle$ with any pure state which can be robustly self-tested, in the sense discussed in Sec. VIII. Furthermore, we restrict our analysis to the case in which the abort condition is defined via a single linear function of the statistics. Specifically, we consider Bell functionals of the form

$$\omega := \sum_{x,y \in \{0,1\}} \gamma_{xy} \langle A_x B_y \rangle, \quad (3)$$

for $\gamma_{xy} \in \mathbb{R}$, and the protocol aborts if the observed value ω_{exp} is below a threshold value $\omega_{\#} - \kappa$, where $\kappa > 0$ is chosen to achieve the desired completeness error. The associated Bell operator is given by B in Eq. (1), and we define the maximum Bell coefficient $\gamma^* := \max_{x,y} |\gamma_{xy}|$. When dealing with the sequential setup, we present our results for the CHSH functional, i.e., the case $\gamma_{00} = \gamma_{01} = \gamma_{10} = -\gamma_{11} = 1$, and leave generalizations to future work. For the parallel setup, however, the protocol allows for the use of any Bell functional of the form given in Eq. (3), such as the family [48, Proposition 1]. The security proofs of all parallel protocols (Protocols 1–3) are given in the Supplemental Material [30, Sec. 3]. For the sequential protocols (Protocols 4 and 5), security is proven in the Supplemental Material [30, Sec. 4].

In the remainder of this section, we present the security proof of one of the aforementioned protocols in detail. All other cases follow a similar structure, and details can be found in the Supplemental Material [30]. Specifically, below we consider the parallel protocol when the objective is to certify a state ϵ -close to the target state, corresponding to Protocol 2 in the Supplemental Material [30, Sec. 2A].

Theorem 1. The DISC protocol 2 is ϵ_s -sound with ϵ_s equal to the following:

$$\inf_{\delta > 0} \max \left\{ \exp \left(-\frac{n-1}{\gamma^*} \delta^2 \right), G_{\epsilon} \left(\frac{n-1}{n} [\omega_{\#} - \kappa - \delta] + \frac{\eta_{\min}^Q}{n} \right) \right\},$$

where $G_{\epsilon}(\omega)$ is any nonincreasing concave function that upper bounds the function

$$\Theta(\sqrt{1 - \Xi_B(\omega)} - \epsilon) \cdot (\sqrt{1 - \Xi_B(\omega)} - \epsilon).$$

Here, Θ is the Heaviside step function, n is the total number of independent states generated by the source, the Bell

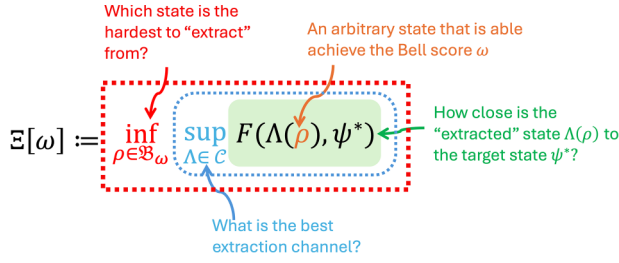


FIG. 5. The definition of the extractability function. Extractability quantifies how close a state can be to a target state (or to one that can be converted to the target under a chosen set of channels). It is defined via a min-max optimization, which is generally difficult to compute or bound.

value ω is given by Eq. (3), which has a minimum quantum value $\eta_{\min}^Q$, $\omega_{\#} - \kappa$ is the value that defines the abort condition, where $\kappa > 0$ chosen to achieve the desired completeness error, and $\Xi_B(\omega)$ is the extractability function given in Definition 4 (see also Fig. 5).

The proof can be found in Supplemental Material [30, Sec. 3B]. For this work, we choose $G_\varepsilon(\cdot)$ to be the function

$$G_\varepsilon(\omega) := -\text{convex}(-\xi_B(\omega, \varepsilon) \cdot \Theta(\xi_B(\omega, \varepsilon))), \quad (4)$$

where $\xi_B(\omega, \varepsilon) := \sqrt{1 - \Xi_B(\omega)} - \varepsilon$, and $\text{convex}(\cdot)$ denotes the convex envelope, i.e., the tightest convex lower bound of a given function (see the Supplemental Material [30, Remark 5] for details on its computation). This choice ensures that $G_\varepsilon(\omega)$ is the optimal concave function required in Theorem 1. Moreover, while Theorem 1 is concerned with soundness, we also provide a proof of completeness in the Supplemental Material [30, Lemma 2].

The soundness parameter ε_s depends on two terms: $\exp(-((n-1)/\gamma^*)\delta^2)$ and $G_\varepsilon(((n-1)/n)[\omega_{\#} - \kappa - \delta])$. Both need to be sufficiently small to guarantee security, and each can be understood as a distinct type of penalty. The former penalty increases when the number of copies used for testing is small. Finite-statistics effects are prominent in this case, resulting in low statistical confidence of the observed Bell value and weaker security. The second penalty is defined in terms of the so-called *extractability* [10, 59, 60], which is a function that indicates how close a state achieving a given Bell violation is to any state in the equivalence class (i.e., any state that can be transformed into the target state using the allowed class of operations) of the target state. Bounding this quantity then becomes the central task in proving security.

VIII. EXTRACTABILITY

Here, let us elaborate on the extractability, $\Xi_B(\omega)$, a robustness measure in the context of the security proof. The extractability represents the worst-case fidelity

between the target state and any state achieving a given Bell violation, following the application of an extraction channel from a set of free operations. Typically, these are taken to be local operations (LO), which originate from the notion of local isometries discussed in Sec. III (see Ref. [29] for the precise connection). This quantity has played a central role in previous works on DISC [7, 13].

Throughout, we consider the extractability under a general class of operations, denoted by $\mathcal{C}$. The choice of $\mathcal{C}$ can be tailored to specific setups, particularly with future protocols in mind. In tasks such as QKD and entanglement distillation, LOCC can be chosen as the class of free operations. The LOCC class includes the LO class, and its use is beneficial since it provides tighter security. Specifically, computing tight lower bounds on the LO extractability for even the simplest case of the CHSH inequality is currently an open question. It is further known that for any CHSH violation up to approximately 2.05 [29, 61], a nontrivial LO extractability is not possible [62]. In contrast, tight bounds on the LOCC extractability for the CHSH inequality are known to be nontrivial for any nonzero violation [59].

We emphasize here that permitting LOCC extraction channels does not enable classical communication between the devices during the Bell test. Indeed, if this were the case, DI certification would become impossible. In our protocol, all classical communication happens strictly after the devices have performed their measurements, during which the user can enforce spacelike separation. We also remark that when the target state is the singlet $|\phi^+\rangle$, extractability under LOCC is closely related to the one-shot distillable entanglement defined in [11].

Definition 4 (Extractability). Let $\mathcal{C}$ be a class of free operations between a physical system $Q_A Q_B$ and a target system $\hat{Q}_A \hat{Q}_B$, let B be a Bell operator, and let $\mathcal{B}_\omega \subset \mathcal{S}(\mathcal{H}_{Q_A} \otimes \mathcal{H}_{Q_B})$ be the set of states in $Q_A Q_B$ that can achieve the Bell value $\langle B \rangle \geq \omega$ using some measurements. Given a target state $\psi^* \in \mathcal{S}(\mathcal{H}_{\hat{Q}_A} \otimes \mathcal{H}_{\hat{Q}_B})$, the extractability $\Xi_B(\omega)$ is defined via the following min-max optimization problem:

$$\Xi_B(\omega) := \inf_{\rho \in \mathcal{B}_\omega} \sup_{\Lambda \in \mathcal{C}} F(\Lambda(\rho), \psi^*), \quad (5)$$

where $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ is the fidelity between two states $\rho, \sigma \in \mathcal{S}(\mathcal{H})$.

Example 3 (Extractability of CHSH under LO channels). To gain some intuition on how the extractability behaves, consider the CHSH extractability. For simplicity, let us consider the case in which $Q_A, Q_B, \hat{Q}_A$, and $\hat{Q}_B$ are all qubit systems, $\mathcal{C}$ is the set of LO operations, and $\psi^* = \phi^+$. It is known that all two-qubit states ρ which achieve maximum violation, $\langle B_{\text{CHSH}} \rangle = 2\sqrt{2}$, are of the form $(U_A \otimes U_B)\phi^+(U_A \otimes U_B)^\dagger$ for some local unitary

$U_A \otimes U_B$ (see, e.g., Ref. [48, Lemma 10]). In other words, every $\rho \in \mathcal{B}_{2\sqrt{2}}$ must be of this form. We then immediately see that for any $\rho \in \mathcal{B}_{2\sqrt{2}}$, there exists a $\Lambda \in \mathcal{C}$ such that

$$F(\Lambda(\rho), \phi^+) = 1, \quad (6)$$

namely, $\Lambda(\rho) = (U_A \otimes U_B)^\dagger \rho (U_A \otimes U_B)$, implying $\Xi_{B_{\text{CHSH}}}^{\text{LO}}(2\sqrt{2}) = 1$.

For the other extreme, consider the set of possible states which achieve a CHSH value of $\omega = 2$. The extractability can always be lower bounded by choosing a fixed channel of the form $\Lambda(\rho) = |00\rangle\langle 00| \forall \rho$, which satisfies $F(\Lambda(\rho), \phi^+) = 1/2$. We therefore see $\Xi_{B_{\text{CHSH}}}^{\text{LO}}(2) \geq 1/2$. Moreover, the state $|00\rangle\langle 00|$ belongs to $\mathcal{B}_2$, and $F(\Lambda(|00\rangle\langle 00|), \phi^+) \leq 1/2$ for all local channels Λ [63]. This implies that $\Xi_{B_{\text{CHSH}}}^{\text{LO}}(2) \leq 1/2$, and hence $\Xi_{B_{\text{CHSH}}}^{\text{LO}}(2) = 1/2$.

The extractability of CHSH under LO channels thus takes values in the interval $[1/2, 1]$ for $\omega \in [2, 2\sqrt{2}]$. It has been shown by Kaniewski [10] that a lower bound for all $\omega \in [2, 2\sqrt{2}]$ is given by

$$\Xi_{B_{\text{CHSH}}}^{\text{LO}}(\omega) \geq \max \left\{ \frac{1}{2} \left(1 + \frac{\omega - \omega^*}{2\sqrt{2} - \omega^*} \right), \frac{1}{2} \right\}, \quad (7)$$

where $\omega^* = (16 + 14\sqrt{2})/17 \approx 2.11$ is the threshold CHSH value below which the extractability is trivial (below $1/2$). It has been shown by Refs. [29, 61] that this threshold cannot be lowered below ≈ 2.05 . This contrasts with the tight bound on $\Xi_{B_{\text{CHSH}}}$ when $\mathcal{C}$ is taken to be the class of LOCC operations, derived by Bardyn *et al.* [59]:

$$\Xi_{B_{\text{CHSH}}}^{\text{LOCC}}(\omega) = \frac{1}{2} \left(1 + \frac{\omega - 2}{2\sqrt{2} - 2} \right). \quad (8)$$

The extractability function involves two levels of optimization. The inner optimization considers a state ρ that can achieve the Bell value ω and aims to transform it, via operations in the class $\mathcal{C}$, to a state as close as possible (in terms of fidelity, rather than trace distance) to the target state ψ^* . This provides a meaningful measure of how close a state is to the equivalence class of the target state. The outer optimization then finds the state ρ for which this distance is smallest, provided that ρ can achieve the given Bell value ω via some local measurement strategy.

Computing the extractability function is challenging in general, since it involves a min-max optimization. Furthermore, the optimization runs over all channels in a given class, and all states compatible with a Bell value ω , without assuming their dimension. Additionally, the constraint $\rho \in \mathcal{B}_\omega$ is nonlinear in both the state and the measurements. To address these challenges, existing works (focused on LO extractability) have bypassed the inner optimization over channels by selecting a fixed channel for all states ρ and

values ω , resulting in a valid lower bound [10]. The issue of not assuming the system dimension can, in general, be handled numerically via moment-matrix approaches [60], or in the special case of Bell scenarios with binary inputs and binary outputs via a reduction to qubits known as Jordan's lemma [64].

Here, we derive a sequence of lower bounds on the LOCC extractability in the minimal Bell scenario for Bell functionals of the form given in Eq. (3). Moreover, our bounds can be improved further at the expense of increasing computational cost. Our results are summarized in Theorem 2, and the following text explains how this can be used to obtain a sequence of lower bounds.

Theorem 2. Let B be any Bell functional of the form Eq. (3) in the minimal Bell scenario. Then the LOCC extractability $\Xi_B(\omega)$ satisfies

$$\Xi_B(\omega) \geq \text{convex} \left(\min_{(a,b) \in \mathcal{F}_\omega} f_{a,b}(\omega) \right), \quad (9)$$

where $\text{convex}(\cdot)$ is the convex envelope (tightest convex lower bound) and

$$\begin{aligned} f_{a,b}(\omega) &:= \max_{\sigma} \lambda \omega + \mu \\ \text{such that } &\sigma - \lambda B(a, b) - \mu \mathbb{I}_4 \geq 0, \\ &\text{tr}_{\hat{Q}_A}[\sigma] = \text{tr}_{\hat{Q}_B}[\sigma] = \frac{\mathbb{I}_2}{2}, \\ &\sigma \in \mathcal{S}_2, \quad \lambda \geq 0, \quad \mu \in \mathbb{R}. \end{aligned} \quad (10)$$

Here, $\mathcal{S}_2 = \mathcal{S}(\mathcal{H}_{\hat{Q}_A} \otimes \mathcal{H}_{\hat{Q}_B})$ is the set of two-qubit density operators and $B(a, b)$ is the Bell operator B constructed from the qubit observables:

$$\begin{aligned} A_x &= \cos(a)\sigma_Z + (-1)^x \sin(a)\sigma_X, \\ B_y &= \cos(b)\sigma_Z + (-1)^y \sin(b)\sigma_X. \end{aligned}$$

The set $\mathcal{F}_\omega$ is defined as

$$\mathcal{F}_\omega = \{(a, b) \in [0, \pi/2]^{\times 2} : \exists \rho \in \mathcal{S}_2 \text{ such that } \text{tr}[B(a, b)\rho] \geq \omega\}.$$

The proof of Theorem 2 is presented in the Supplemental Material [30, Sec. 6C], (see also the Supplemental Material [30, Fig. 4] for an informal overview) and let us here discuss its implications. The first significant aspect of this result is the dimensional reduction of the optimization problem required to compute the extractability. By employing Jordan's lemma, we reduce the problem to effectively computing the extractability function within the state space of a qubit pair. Subsequently, we perform a series of reductions inspired by techniques from device-independent randomness generation and QKD protocols in

the minimal Bell scenario [17,32,39,65]. These reductions, combined with other technical results, allow us to reformulate the optimization over unital LOCC channels into a standard optimization problem over a bounded domain.

Assuming that the projective measurements performed by the two devices on the qubit pair are known, the extractability can be computed numerically. This follows from the fact that, for a fixed $(a, b) \in \mathbb{R}^2$, the optimization Eq. (10) is a semidefinite program (SDP), which can be efficiently solved using numerical techniques [66]. However, the outer maximization over all possible two-qubit Bell operators $B(a, b)$ still remains, complicating the original problem as it is no longer an SDP.

To address this, we develop a technique to discretize the parameter space of the angles $(a, b) \in [0, \pi/2] \times [0, \pi/2]$ into smaller rectangular domains (see the Supplemental Material [30, Sec. 6D]). This discretization transforms the problem into solving multiple SDPs of the form given in Eq. (10), each corresponding to a specific grid point within the rectangular domains. Specifically, for each domain, we relax the optimization problem and introduce a penalty term that scales with the dimensions of the domain, ensuring that we reliably lower bound the global minimization. By reducing the size of each rectangular domain, we achieve tighter bounds on the extractability function at the cost of solving more optimization problems, and thus an increased computation time. Furthermore, as the size of each rectangle tends to zero, the method converges to a tighter lower bound on the LOCC extractability.

Note that an analytic method for computing extractability in the LOCC case has first been introduced in Ref. [59], where only the CHSH functional has been considered. The approach presented here is significantly more general, encompassing more self-tests of the singlet—i.e., it applies to all Bell inequalities of the form given in Eq. (3). Moreover, our method allows for the simultaneous use of multiple Bell inequalities, or even the full distribution, when bounding the extractability. As a result, it provides a framework for obtaining lower bounds in the minimal Bell scenario when self-testing the singlet. Additionally, while Theorem 2 addresses the LOCC extractability, our gridding techniques can also be applied to other classes of free operations, such as the LO extractability for arbitrary Bell functionals in the minimal scenario, including those tailored to partially entangled states [29,67,68].

IX. RESULTS FOR EXAMPLE 1: CHSH BASED PROTOCOL FOR CERTIFYING ϕ^+

To illustrate our results, we consider a DISC protocol based on violating the CHSH inequality in the parallel-measurement setup, where the objective is to certify a state ε -close to ϕ^+ (see Protocol 2 in the Supplemental Material [30]). A bound on the CHSH LOCC extractability has been provided in Ref. [59], given by the linear function Eq.

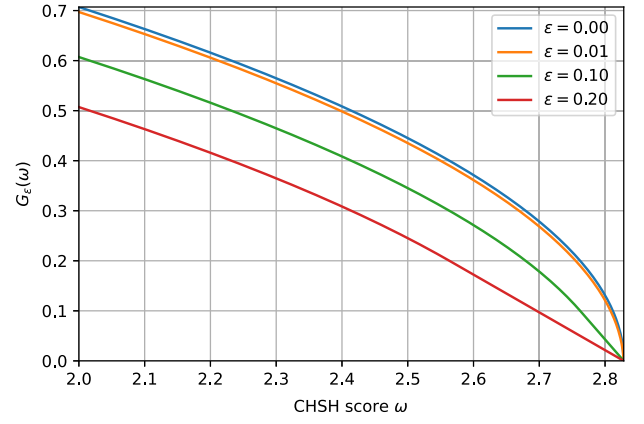


FIG. 6. A graph of $G_\varepsilon(\omega)$ for different values of ε , using LOCC extractability.

(8) for $\omega \in [2, 2\sqrt{2}]$. Using this bound, we plot the penalty function $G_\varepsilon(\omega)$ (defined via substituting $\Xi_B(\omega)$ in Eq. (4) with Eq. (8)) in Fig. 6, which provides an estimate of the security bounds as a function of the chosen abort condition, characterized by the Bell value ω .

Knowing $G_\varepsilon(\omega)$ enables us to compute the security bounds for the protocol via Theorem 1, which we present in Fig. 7. From this figure, two key trends emerge. First, we obtain tighter security from higher CHSH values ω , which arises from a smaller value of $G_\varepsilon(\omega)$. Second, security improves as the number of rounds increases, owing to a smaller penalty due to finite statistics (captured by the exponential term in Theorem 1). Additionally, we observe that for larger values of the closeness parameter ε , security is higher for the same Bell value and number of rounds. This is expected, as certifying a state that is ε -close to the target state requires a lower Bell value than certifying the target state exactly. Thus, increasing ε results in a smaller value of $G_\varepsilon(\omega)$, corresponding to a smaller penalty.

X. DISCUSSION

We have presented a composable approach for device-independent state certification under the assumption of an independent but not identically distributed source. We have introduced a definition for composable DISC security, and provided a general framework for proving security in the two-input two-output Bell scenario under LOCC operations.

For future directions, it would be interesting to apply our protocols in practice. Clearly, the advantage lies in the composable integration of DISC with any other composable protocol. For example, consider a protocol $\mathcal{P}$ which, when given as input the state ϕ^+ , outputs a state $\mathcal{P}(\phi^+)$ satisfying $\|\mathcal{P}(\phi^+) - \sigma_{\text{ideal}}\|_1 \leq \epsilon'$, where σ_{ideal} is some target output state of $\mathcal{P}$. Now, suppose that the DISC protocol outputs a state ρ_{real} with the property [69] $\|\rho_{\text{real}} - \phi^+\|_1 \leq \epsilon$. Then the composable security

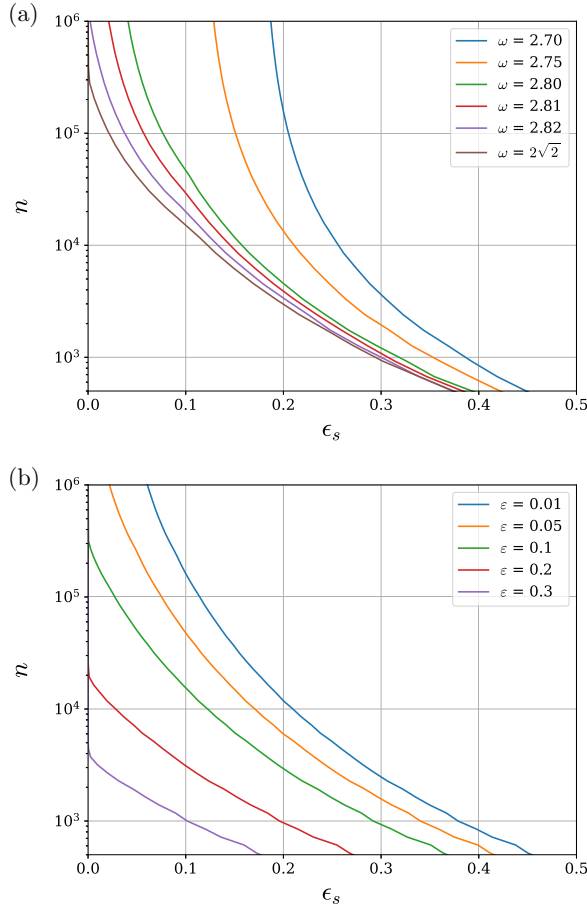


FIG. 7. A comparison of the security parameters for different conditions using the CHSH inequality. (a) A plot of the security parameter ϵ_s versus the number of rounds n for different CHSH values ω . Here, we set $\epsilon = 0.1$ and κ is chosen to achieve a completeness error of $\epsilon_c = 10^{-2}$. The choice of ϵ_c follows standard values used in related device-independent protocols (see, e.g., Ref. [20]). (b) A plot of the security parameter ϵ_s versus the number of rounds n for different values of ϵ , assuming a CHSH value of $\omega = 2\sqrt{2}$. The parameter κ is chosen to achieve a completeness error of $\epsilon_c = 10^{-2}$.

definition ensures that, when the DISC protocol output is used as an input to $\mathcal{P}$, the result is secure: $\|\mathcal{P}(\rho_{\text{real}}) - \sigma_{\text{ideal}}\|_1 \leq \epsilon + \epsilon'$. Such applications might include the certification of other quantum resources, along the lines of Ref. [70], where state certification is an essential building block.

We also note that DISC is not vulnerable to the same device-reuse attacks as in, e.g., device-independent quantum key distribution [71]. This follows from the fact that no classical information is kept private from an adversary during the protocol. It is then an interesting question if DISC always remains secure when the measurement devices are reused.

It would also be interesting to improve the DISC security statement. Both a large Bell violation and a large

number of copies are currently required to obtain a composable security proof, which is limiting in practice. This could be due to two reasons. First, the proof technique relies on inequalities and bounds that may not be tight, suggesting room for improvement in obtaining sharper security bounds. For example, our security proof employs Hoeffding's inequality, which could potentially be replaced by tighter alternatives such as those used in Ref. [7]. The second reason is that, from a fundamental point of view, it is an inherently strong requirement to ensure general security under any future protocol usage. Consequently, achieving tight security bounds for small Bell violations and low numbers of rounds may be infeasible [40].

Nevertheless, it is notable that composable security can be achieved. Moreover, our security bounds are tighter than those obtained using LO extractability bounds. In realistic experimental implementations, improved certification could be achieved by relaxing the stringent fully DI assumptions and incorporating justified partial assumptions. For instance, the fair-sampling assumption could be employed to account for poor detector efficiencies. Additionally, similar results may be obtained in a semi-DI setting, where assumptions on system dimensions are introduced.

Another promising direction would be to certify more than one copy of the target state. In fact, our current approach can be straightforwardly modified to accommodate this. However, the soundness parameter ϵ_s scales as $\sqrt{1 - c^m}$, where c is the single-copy extractability for the threshold Bell value which does not cause the protocol to abort, and m is the number of certified copies. We therefore see that the resulting protocol will not be efficient, in the sense that a large number of copies can only be certified when $c \approx 1$, which demands both a near-maximum Bell violation and a large number of samples n . Furthermore, there are recent no-go results [40] which rule out sample efficient and composable state certification when the desired certification is “exact,” i.e., the target state is certified rather than tolerating small deviations from it. Thus, understanding what is possible for composable multiple-copy DI state certification is an appealing direction.

In addition, it would be useful to relax the assumption of independent state preparation in each round. Removing this assumption and allowing for general memory effects would lead to a more general security proof. As discussed in Ref. [7], the task of certifying one copy can be achieved under an arbitrarily correlated source (see also Refs. [72,73] for a device-dependent approach), and such techniques may provide a path to establishing similar results in our composable framework. However, extending the DISC framework of Ref. [7] to multiple copies in the fully non-IID setting remains an open question. Due to the more demanding requirement of composability, we expect that this will be at least as challenging to establish in

our case. Moreover, there are potential limitations when considering a fully general measurement process. As discussed in Ref. [11, Sec. 2.2.1], the ability to “not measure” a quantum system and hold it in memory necessitates some separation between the state and measurement devices.

Our result on the LOCC extractability for the singlet state may also be of independent interest. This quantity serves as the natural DI counterpart to the well-known singlet fraction [74], extending its relevance to the DI setting. This raises open questions regarding its potential applications in other areas of entanglement theory, as well as in the development of new DI protocols. Additionally, our results provide another avenue for exploring the relationship between nonlocality and entanglement [39], which remains a fundamental topic of investigation.

Finally, it is also interesting to consider a weaker certification criterion—namely, certifying the presence of *any* pure entangled state rather than a specific one. Such a certification could have significant cryptographic applications, as it has been demonstrated that randomness and cryptographic keys can be extracted in a fully device-independent manner from nonmaximally entangled, yet still entangled, states [67,75].

ACKNOWLEDGMENTS

We are grateful to Peter Brown, Roger Colbeck, and Ivan Šupić for insightful discussions. We also thank Cameron Foreman, Ashutosh Rai, Olgierd Żurek, Mirjam Weilenmann, and anonymous referees for their valuable feedback on earlier versions of this work. R.B. and J.B. are supported by the National Research Foundation of Korea (Grants No. NRF-2021R1A2C2006309 and No. NRF-2022M1A3C2069728) and the Institute for Information and Communication Technology Promotion (IITP) (Grants No. RS-2023-00229524 and No. RS-2025-02304540). L.W. acknowledges funding support from the Engineering and Physical Sciences Research Council (EPSRC) (Grant No. EP/SO23607/1) and the European Union Horizon Europe research and innovation program under the project “Quantum Secure Networks Partnership” (QSNP, Grant Agreement No. 101114043). Preliminary investigations for this work were supported by the EPSRC via the Quantum Communications Hub (Grant No. EP/T001011/1) during RB’s time at the University of York.

DATA AVAILABILITY

No data were created or analyzed beyond what is included in this article.

-
- [1] A. K. Ekert, Quantum cryptography based on Bell’s theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [2] A. Acin, 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).
- [3] R. Colbeck, Ph.D. thesis, Trinity College, University of Cambridge, 2007, also available as <https://arxiv.org/abs/0911.3814>.
- [4] S. Pironio, A. Acin, 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* **464**, 1021 (2010).
- [5] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Nonlocal correlations as an information-theoretic resource, *Phys. Rev. A* **71**, 022101 (2005).
- [6] J.-D. Bancal, K. Redeker, P. Sekatski, W. Rosenfeld, and N. Sangouard, Self-testing with finite statistics enabling the certification of a quantum network link, *Quantum* **5**, 401 (2021).
- [7] A. Gočanin, I. Šupić, and B. Dakić, Sample-efficient device-independent quantum state verification and certification, *PRX Quantum* **3**, 010317 (2022).
- [8] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS-98)* (IEEE Computer Society, Los Alamitos, California, USA, 1998), p. 503.
- [9] D. Mayers and A. Yao, Self testing quantum apparatus, *QIC* **4**, 273 (2004).
- [10] J. Kaniewski, Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities, *Phys. Rev. Lett.* **117**, 070402 (2016).
- [11] R. Arnon-Friedman and J.-D. Bancal, Device-independent certification of one-shot distillable entanglement, *New J. Phys.* **21**, 033010 (2019).
- [12] A. Philip and M. M. Wilde, Device-independent certification of multipartite distillable entanglement, *Phys. Rev. A* **111**, 012436 (2025).
- [13] L. dos Santos Martins, N. Laurent-Puig, I. Šupić, D. Markham, and E. Diamanti, Experimental sample-efficient and device-independent GHZ state certification, *ArXiv:2407.13529*.
- [14] S. Storz, A. Kulikov, J. D. Schär, V. Barizien, X. Valcarce, F. Berterottière, N. Sangouard, J.-D. Bancal, and A. Wallraff, Complete self-testing of a system of remote superconducting qubits, *Phys. Rev. Lett.* **135**, 030801 (2005).
- [15] M. M. E. Schmid, M. Antesberger, H. Cao, W. hao Zhang, B. Dakić, L. A. Rozema, and P. Walther, in *Quantum 2.0 Conference and Exhibition* (Optica Publishing Group, Rotterdam, Netherlands, 2024), p. QM2C.7.
- [16] J. Barrett, L. Hardy, and A. Kent, No signalling and quantum key distribution, *Phys. Rev. Lett.* **95**, 010503 (2005).
- [17] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, *New J. Phys.* **11**, 045021 (2009).
- [18] J. Barrett, R. Colbeck, and A. Kent, Unconditionally secure device-independent quantum key distribution with only two devices, *Phys. Rev. A* **86**, 062326 (2012).
- [19] U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, *Phys. Rev. Lett.* **113**, 140501 (2014).
- [20] 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).

- [21] R. Colbeck and A. Kent, Private randomness expansion with untrusted devices, *J. Phys. A: Math. Gen.* **44**, 095305 (2011).
- [22] C. A. Miller and Y. Shi, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing, STOC '14* (ACM, New York, USA, 2014), p. 417.
- [23] C. A. Miller and Y. Shi, Universal security for randomness expansion from the spot-checking protocol, *SIAM J. Comput.* **46**, 1304 (2017).
- [24] R. Colbeck and R. Renner, Free randomness can be amplified, *Nat. Phys.* **8**, 450 (2012).
- [25] R. Renner, Ph.D. thesis, Swiss Federal Institute of Technology, Zurich, 2005, also available as <https://arxiv.org/abs/quant-ph/0512258>.
- [26] C. Portmann and R. Renner, Cryptographic security of quantum key distribution, *ArXiv:1409.3525*
- [27] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, *Quantum* **4**, 337 (2020).
- [28] We refer to this scenario with two parties as the minimal Bell scenario.
- [29] T. Coopmans, J. Kaniewski, and C. Schaffner, Robust self-testing of two-qubit states, *Phys. Rev. A* **99**, 052123 (2019).
- [30] See the Supplemental Material at <http://link.aps.org/supplemental/10.1103/1j5f-qjhx> for protocols, proofs, and additional discussions and including additional references [76–83].
- [31] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, Computing secure key rates for quantum cryptography with untrusted devices, *npj Quantum Inf.* **7**, 158 (2021).
- [32] R. Bhavsar, S. Ragy, and R. Colbeck, Improved device-independent randomness expansion rates using two sided randomness, *New J. Phys.* **25**, 093035 (2023).
- [33] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, *Quantum* **8**, 1445 (2024).
- [34] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, *Commun. Math. Phys.* **379**, 867 (2020).
- [35] F. Dupuis and O. Fawzi, Entropy accumulation with improved second-order term, *IEEE Trans. Inf. Theory* **65**, 7596 (2019).
- [36] T. Metger, O. Fawzi, D. Sutter, and R. Renner, Generalised entropy accumulation, *Commun. Math. Phys.* **405**, 261 (2024).
- [37] Y. Zhang, H. Fu, and E. Knill, Efficient randomness certification by quantum probability estimation, *Phys. Rev. Res.* **2**, 013016 (2020).
- [38] C. Foreman, S. Wright, A. Edgington, M. Berta, and F. J. Curchod, Practical randomness amplification and privatisation with implementations on quantum computers, *Quantum* **7**, 969 (2023).
- [39] Y. Zhu, X. Zhang, and X. Ma, Interplay among entanglement, measurement incompatibility, and nonlocality, *Quantum Sci. Technol.* **9**, 045008 (2024).
- [40] F. Wiesner, Z. Chaoui, D. Kessler, A. Pappa, and M. Karvonen, Why quantum state verification cannot be both efficient and secure: A categorical approach, *ArXiv:2411.04767*.
- [41] A. Rai, M. Pivoluska, S. Sasmal, M. Banik, S. Ghosh, and M. Plesch, Self-testing quantum states via nonmaximal violation in Hardy’s test of nonlocality, *Phys. Rev. A* **105**, 052227 (2022).
- [42] J. S. Bell, in *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, UK, 1987), Chap. 2.
- [43] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed experiment to test local hidden-variable theories, *Phys. Rev. Lett.* **23**, 880 (1969).
- [44] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [45] Y. Wang, X. Wu, and V. Scarani, All the self-testings of the singlet for two binary measurements, *New J. Phys.* **18**, 025021 (2016).
- [46] T. P. Le, C. Meroni, B. Sturmfels, R. F. Werner, and T. Ziegler, Quantum correlations in the minimal scenario, *Quantum* **7**, 947 (2023).
- [47] V. Barizien, P. Sekatski, and J.-D. Bancal, Custom Bell inequalities from formal sums of squares, *Quantum* **8**, 1333 (2024).
- [48] L. Woollorton, P. Brown, and R. Colbeck, Device-independent quantum key distribution with arbitrarily small nonlocality, *Phys. Rev. Lett.* **132**, 210802 (2024).
- [49] The notion of closeness referred to here, and throughout the paper, is with respect to the trace distance, unless stated otherwise. Specifically, a state ρ is said to be ε -close to σ if $\frac{1}{2}\|\rho - \sigma\|_1 \leq \varepsilon$, where $\|A\|_1 := \text{tr}[\sqrt{A^\dagger A}]$ denotes the trace norm.
- [50] The assumption that the devices are noncommunicating can be justified in two standard ways: (i) by employing shielding mechanisms that prevent any exchange of information, or (ii) by enforcing spacelike separation during the measurement rounds, which guarantees that the devices cannot signal to one another.
- [51] M. Ben-Or and D. Mayers, General security definition and composability for quantum & classical protocols, *ArXiv:quant-ph/0409062*.
- [52] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory of Cryptography*, edited by J. Kilian (Springer-Verlag, Berlin, 2005), p. 386.
- [53] D. Unruh, Simulatable security for quantum protocols, *ArXiv:quant-ph/0409125*.
- [54] R. Renner and R. König, in *Theory of Cryptography Conference* (Springer, Cambridge, MA, USA, 2005), p. 407.
- [55] 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. Photon.* **12**, 1012 (2020).
- [56] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and C. C.-W. Lim, Security of device-independent quantum key distribution protocols: A review, *Quantum* **7**, 932 (2023).
- [57] Recall that for binary projective measurements derived from observables with eigenvalues ± 1 , the POVM elements are $M_{a|x} = \frac{1}{2}(\mathbb{I} + (-1)^a A_x)$ and $N_{b|y} = \frac{1}{2}(\mathbb{I} + (-1)^b B_y)$, so that $M_{0|x} - M_{1|x} = A_x$ and $N_{0|y} - N_{1|y} = B_y$.

- [58] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, UK, 2013).
- [59] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Device-independent state estimation based on Bell's inequalities, *Phys. Rev. A* **80**, 062327 (2009).
- [60] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Physical characterization of quantum devices from nonlocal correlations, *Phys. Rev. A* **91**, 022115 (2015).
- [61] X. Valcarce, P. Sekatski, D. Orsucci, E. Oudot, J.-D. Bancal, and N. Sangouard, What is the minimum CHSH score certifying that a state resembles the singlet? *Quantum* **4**, 246 (2020).
- [62] The trivial extractability in this context is the maximum fidelity between any separable state and the target state (see Ref. [27, Sec. 3.6] for details). This value can always be achieved regardless of the underlying state. See also Example 3.
- [63] This follows from the fact that the maximum fidelity between ϕ^+ and $\Lambda(|00\rangle\langle 00|)$ is achieved when $\Lambda(|00\rangle\langle 00|)$ is any pure separable state corresponding to the largest Schmidt coefficient of $|\phi^+\rangle$.
- [64] C. Jordan, Essai sur la géométrie à n dimensions, *Bull. Soc. Math. France* **3**, 103 (1875).
- [65] R. Bhavsar, Ph.D. thesis, Department of Mathematics, University of York (2023), also available as <https://arxiv.org/abs/2311.13528>.
- [66] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, United Kingdom, 2004).
- [67] A. Acín, S. Massar, and S. Pironio, Randomness versus nonlocality and entanglement, *Phys. Rev. Lett.* **108**, 100402 (2012).
- [68] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, *Phys. Rev. A* **91**, 052111 (2015).
- [69] Here, for ease of discussion, we have omitted the fact that both the DISC protocol and $\mathcal{P}$ may abort.
- [70] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, Certifying the building blocks of quantum computers from Bell's theorem, *Phys. Rev. Lett.* **121**, 180505 (2018).
- [71] J. Barrett, R. Colbeck, and A. Kent, Memory attacks on device-independent quantum cryptography, *Phys. Rev. Lett.* **110**, 010503 (2013).
- [72] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario, *Phys. Rev. A* **100**, 062335 (2019).
- [73] H. Zhu and M. Hayashi, Efficient verification of pure quantum states in the adversarial scenario, *Phys. Rev. Lett.* **123**, 260504 (2019).
- [74] M. Horodecki, P. Horodecki, and R. Horodecki, General teleportation channel, singlet fraction, and quasidistillation, *Phys. Rev. A* **60**, 1888 (1999).
- [75] E. Woodhead, A. Acín, and S. Pironio, Device-independent quantum key distribution with asymmetric CHSH inequalities, *Quantum* **5**, 443 (2021).
- [76] C. Fuchs and J. van de Graaf, Cryptographic distinguishability measures for quantum-mechanical states, *IEEE Trans. Inf. Theory* **45**, 1216 (1999).
- [77] L. Contento, A. Ern, and R. Vermiglio, A linear-time approximate convex envelope algorithm using the double Legendre-Fenchel transform with application to phase separation, *Comput. Optim. Appl.* **60**, 231 (2015).
- [78] A. M. Zubkov and A. A. Serov, A complete proof of universal inequalities for the distribution function of the binomial law, *Theory Prob. Appl.* **57**, 539 (2013).
- [79] S. Simons, in *Minimax and Applications*, edited by D.-Z. Du and P. M. Pardalos (Springer US, Boston, Massachusetts, 1995), p. 1.
- [80] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, UK, 2004).
- [81] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín, Scalable Bell inequalities for qubit graph states and robust self-testing, *Phys. Rev. Lett.* **124**, 020402 (2020).
- [82] G. Murta and F. Baccari, Self-testing with dishonest parties and device-independent entanglement certification in quantum communication networks, *Phys. Rev. Lett.* **131**, 140201 (2023).
- [83] T. Sharma, R. Bhavsar, J. Ramakrishnan, P. Chandravan-shi, S. Prabhakar, A. Biswas, and R. P. Singh, Enhancing key rates of QKD protocol by coincidence detection, *Adv. Quantum Technol.* **8**, 2400685 (2025).