Efficient randomness certification by quantum probability estimation

Yanbao Zhang [1,*] Honghao Fu,[2] and Emanuel Knill[3,4]

[1]*NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[2]*Department of Computer Science, Institute for Advanced Computer Studies, and Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, Maryland 20742, USA*

[3]*National Institute of Standards and Technology, Boulder, Colorado 80305, USA*

[4]*Center for Theory of Quantum Matter, University of Colorado, Boulder, Colorado 80309, USA*

(Received 18 March 2019; published 7 January 2020)

For practical applications of quantum randomness generation, it is important to certify and further produce a fixed block of fresh random bits with as few trials as possible. Consequently, protocols with high finite-data efficiency are preferred. To yield such protocols with respect to quantum side information, we develop quantum probability estimation. Our approach is applicable to device-independent as well as device-dependent scenarios, and it generalizes techniques from previous works [Miller and Shi, SIAM J. Comput. **46**, 1304 (2017); Arnon-Friedman *et al.*, Nat. Commun. **9**, 459 (2018)]. Quantum probability estimation can adapt to changing experimental conditions, allows stopping the experiment as soon as the prespecified randomness goal is achieved, and can tolerate imperfect knowledge of the input distribution. Moreover, the randomness rate achieved at constant error is asymptotically optimal. For the device-independent scenario, our approach certifies the amount of randomness available in experimental results without first searching for relations between randomness and violations of fixed Bell inequalities. We implement quantum probability estimation for device-independent randomness generation in the CHSH Bell-test configuration, and we show significant improvements in finite-data efficiency, particularly at small Bell violations which are typical in current photonic loophole-free Bell tests.

DOI: 10.1103/PhysRevResearch.2.013016

I. INTRODUCTION

Randomness is important for many applications including Monte Carlo simulations, statistical sampling, randomized algorithms, and cryptography [1]. A fundamental feature of randomness is *unpredictability*, which is also exhibited by quantum measurement outcomes. Quantum mechanics thus provides natural strategies for generating randomness. For example, a uniformly random bit can be generated by measuring a two-level quantum system in an equal superposition of its two levels. In this scheme, however, to guarantee the performance one needs to trust the inner working of quantum devices. It is desirable if the generated randomness can be certified solely by statistical tests of the inputs and outputs of quantum devices. A loophole-free Bell test provides such a strategy, as first proposed in 2006 by Colbeck in his PhD thesis [2]. This strategy for certified randomness generation without trust in quantum devices is known as device-independent randomness generation (DIRG).

Many DIRG protocols [3–15] have been developed in the past ten years. They are different in the following aspects: the specific requirements on quantum devices, the Bell-test configuration applied, the security level achieved, and the asymptotic randomness rate and finite-data efficiency exhibited. Also, in the past five years, loophole-free Bell tests have been realized [16–20], enabling experimental demonstrations of DIRG [21–23]. However, due to the lack of finite-data efficiency, even the most advanced DIRG protocol with respect to *quantum side information* [13] requires a very large number of trials with current loophole-free Bell tests. With a state-of-the-art photonic loophole-free Bell test [23] the DIRG protocol in Ref. [13] requires at least 9.4×10^9 trials, corresponding to 13 hours of experiment time (see Fig. 3 of Ref. [23]), before certifying any randomness with error bounded by 10^{-5}, where, informally, the error can be thought of as the probability that the protocol output does not satisfy the certified claim. For practical applications of randomness such as randomness beacons that provide trusted public randomness [24], it is important to improve finite-data efficiency, as these applications often require short blocks of fresh random bits with minimum delay or *latency*.

Excellent finite-data efficiency for DIRG with respect to *classical side information* has been recently achieved [21,22,25,26]. Particularly, the method developed by us in Refs. [21,22] reduces the number of trials required for generating 1024 device-independent random bits with error 10^{-12} [22] by one order of magnitude as compared with the previously most advanced method (for addressing classical side information) in Refs. [3,6]. To improve the finite-data efficiency further, we developed probability estimation

*Corresponding author: yanbao.zhang.xf@hco.ntt.co.jp

[25,26] for certifying randomness against classical side information. Different from previous works [3,6,21,22], probability estimation provides an estimator, constructed as a function of experimental results, to *directly* lower-bound the amount of certifiable device-independent randomness *without* relying on a hypothesis test of local realism. The natural question then is whether we can upgrade probability estimation for certifying randomness against quantum side information.

In this work, we develop quantum probability estimation, which enables a full security analysis of DIRG with respect to quantum side information, and most importantly, yields protocols with unsurpassed finite-data efficiency. As the quantum smooth conditional min-entropy quantifies the number of near-uniform random bits certifiable in the presence of quantum side information [27], the goal of quantum probability estimation is to obtain a lower bound on the quantum smooth conditional min-entropy. For this, we first construct an estimator to *directly* lower-bound the sandwiched Rényi entropy (see theorem 2). Such an estimator is the main reason for achieving unsurpassed finite-data efficiency. Then we lower-bound the quantum smooth conditional min-entropy by the sandwiched Rényi entropy via Prop. 6.5, p. 99 of Ref. [28] (see theorem 3). We also give a sound protocol to realize end-to-end randomness generation.

Besides unsurpassed finite-data efficiency, quantum probability estimation has many other advantages over previous works [5,8–10,13–15,29], which include adaptability to changing experimental conditions, flexibility of stopping the experiment early as soon as the prespecified randomness goal is achieved, and tolerance of imperfections in the input distribution. Like entropy accumulation developed in Refs. [13–15,29], quantum probability estimation can achieve asymptotically optimal randomness rates and is broadly applicable to both device-independent and device-dependent randomness generation.

The conceptual difference between our work and previous works [5,8–10,13–15,29] for addressing quantum side information in the device-independent scenario lies in that previous works require quantifying randomness as a function of violations of fixed Bell inequalities before performing security analysis with finite data. Although Bell violations and device-independent randomness are related, they are inequivalent quantities: a stronger violation of a fixed Bell inequality does not necessarily certify a larger amount of device-independent randomness [30]. Therefore previous works usually cannot yield protocols with optimal randomness rates or finite-data efficiency. With respect to proof techniques, the main difference between our work and previous works [8,9,13–15,29], which also benefit from the recent studies of sandwiched Rényi entropies, is that quantum probability estimation provides a *tighter* lower bound on the sandwiched Rényi entropy (see theorem 2), whereas previous works establish lower bounds on the sandwiched Rényi entropy via uncertainty principles for quantum measurements (as in Refs. [8,9]) or via the conditional von Neumann entropy (as in Refs. [13–15,29]). These differences provide an informal explanation of the improvements achieved by quantum probability estimation as compared with previous works, see Fig. 2 for a comparison.

The paper is structured as follows. In Sec. II, we introduce the notation used in this work. In Sec. III, we motivate and introduce quantum probability estimation. To implement our method, we need to construct quantum estimation factors (QEFs). In Sec. IV, we show that QEFs can certify quantum smooth conditional min-entropies. Then we present an end-to-end protocol for randomness generation and prove its soundness in Sec. V. Details on the implementation of our method are provided in Secs. VI and VII. Specifically, in Sec. VI, we explain the construction of the model that describes all possible states shared between the quantum side information and the classical results after the experiment. In Sec. VII, we discuss several properties of QEFs and provide details on the construction of QEFs. In Sec. VIII, we show how the general method of quantum probability estimation is instantiated in the experimentally relevant CHSH Bell-test configuration [31] for DIRG, and then we demonstrate significant improvements on finite-data efficiency, corresponding to significant reductions in latency compared with previous works. Finally we conclude the paper in Sec. IX.

II. NOTATION

We denote classical (random) variables by uppercase letters in regular math font (such as U, V, W) and denote finite sequences of classical variables by uppercase letters in upright bold font (such as $\mathbf{C}$, $\mathbf{Z}$). As is conventional, the values of classical variables are denoted by the corresponding lowercase letters. We use juxtaposition to denote concatenation of variables or their values. For example, we write the concatenation of U and V as UV. The value space of a classical variable such as U is denoted by $\mathrm{Rng}(U)$. The cardinality of the value space of U is $|\mathrm{Rng}(U)|$. All classical variables considered in this work are assumed to have finite value spaces.

We identify classical systems with classical variables. We denote and label quantum systems with uppercase letters in sans serif font (such as D, E). Throughout this work, E plays a distinguished role as the system carrying the quantum side information. We denote the identity operator on a classical or quantum system by $\mathbb{1}$.

For a quantum system E, we denote its Hilbert space as $\mathcal{H}(\mathsf{E})$. Quantum states, which are positive semidefinite (Hermitian) operators, are denoted by lowercase Greek letters (such as ρ, σ, τ). Both normalized and un-normalized quantum states are considered in this work. Let $\mathcal{S}(\mathsf{E})$ be the set of un-normalized states, $\mathcal{S}_1(\mathsf{E}) = \{\rho_\mathsf{E} \in \mathcal{S}(\mathsf{E}) : \mathrm{tr}(\rho_\mathsf{E}) = 1\}$ be the set of normalized states, and $\mathcal{S}_{\leqslant 1}(\mathsf{E}) = \{\rho_\mathsf{E} \in \mathcal{S}(\mathsf{E}) : \mathrm{tr}(\rho_\mathsf{E}) \leqslant 1\}$ be the set of subnormalized states of E, where "tr" denotes the trace.

In this work, we study the joint states of a classical variable U and a quantum system E. Such states are called *classical-quantum states* and have the following form:

$$\rho_{U\mathsf{E}} = \sum_u |u\rangle\langle u| \otimes \rho_\mathsf{E}(u),$$

where $\rho_\mathsf{E}(u) \in \mathcal{S}(\mathsf{E})$ is the state of E given $U = u$. We denote the set of classical-quantum states of the above form by $\mathcal{S}(U\mathsf{E})$. The set of normalized states and the set of subnormalized states of $U\mathsf{E}$ are denoted by $\mathcal{S}_1(U\mathsf{E})$ and $\mathcal{S}_{\leqslant 1}(U\mathsf{E})$, respectively. If there are multiple classical

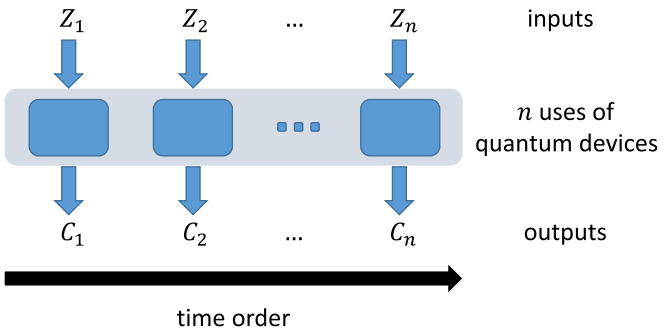

FIG. 1. Schematic of an experiment. The experiment can be either for device-independent or device-dependent randomness generation.

variables $U, V, W, \ldots$ involved in an experiment, we denote the classical-quantum states and the corresponding sets of states in similar ways. For example, $\rho_{UV\mathsf{E}}$ is the joint state of the classical variables U, V and the quantum system E, and $\mathcal{S}(UV\mathsf{E})$ is the corresponding set of classical-quantum states.

For a classical-quantum state such as $\rho_{U\mathsf{E}}$, when the quantum system E is one-dimensional the state $\rho_{U\mathsf{E}}$ (up to a normalization constant) specifies a classical probability distribution of the variable U. We also use lowercase (but different) Greek letters (such as μ, ν) to denote classical probability distributions. The probability of an event Φ according to a probability distribution μ is denoted by $\mathbb{P}_\mu(\Phi)$. The expectation of a classical variable U according to μ is denoted by $\mathbb{E}_\mu(U)$.

III. QUANTUM ESTIMATION FACTORS

Consider an experiment with *inputs* $\mathbf{Z}$ and *outputs* $\mathbf{C}$. Both the inputs and outputs are classical variables. The inputs normally consist of the random choices made for measurement settings. The outputs consist of the corresponding measurement outcomes. The inputs and outputs are determined in a sequence of n time-ordered trials, where the ith trial has input Z_i and output C_i, so $\mathbf{Z} = (Z_i)_{i=1}^n$ and $\mathbf{C} = (C_i)_{i=1}^n$, see Fig. 1. We refer to the trial inputs and outputs collectively as the trial *results*. In addition, we refer to the results from the trials preceding the upcoming one as the *past*. The past can also include initial conditions and any additional information that may have been obtained, which are usually implicit when referring to or conditioning on the past.

The external quantum system carrying the quantum side information is E, whose initial state before the experiment may be correlated with the quantum system D of the devices used. After the experiment, the quantum system D is traced out, and only the classical inputs $\mathbf{Z}$ and outputs $\mathbf{C}$ of the devices are considered. The joint state of the classical systems $\mathbf{C}$, $\mathbf{Z}$, and the quantum system E is a classical-quantum state

$$\rho_{\mathbf{CZE}} = \sum_{\mathbf{cz}} |\mathbf{cz}\rangle\langle\mathbf{cz}| \otimes \rho_{\mathsf{E}}(\mathbf{cz}) \tag{1}$$

in $\mathcal{S}_1(\mathbf{CZE})$, where $\rho_{\mathsf{E}}(\mathbf{cz})$ is the subnormalized state of E given results $\mathbf{cz}$. The trace $\mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))$ is the probability of observing the results $\mathbf{cz}$ after the experiment. In general, we consider the set of all possible classical-quantum states that can occur after the experiment. We refer to this set as the model $\mathcal{C}$ for the experiment (see Sec. VI for details). Our goal is to estimate (or strictly speaking, bound) the quantum smooth conditional min-entropy of $\mathbf{C}$ given $\mathbf{Z}$ and the side information in E, without knowing which particular normalized state $\rho_{\mathbf{CZE}}$ in the model describes the experiment.

In previous works [25,26], we considered the case that the quantum system E is one-dimensional. In this case, $\rho_{\mathsf{E}}(\mathbf{cz})$ specifies the probability of observing $\mathbf{cz}$ given the side information, which we write as $\mu_{\mathsf{E}}(\mathbf{cz})$, and so the side information is classical. The model $\mathcal{C}$ becomes the set of probability distributions μ_{E} of $\mathbf{CZ}$ that capture verified, physical constraints on device behavior. In the case of Bell tests, these constraints include the familiar nonsignaling conditions [32,33]. To deal with classical side information, we developed *probability estimation* [25,26] which can estimate the conditional probability $\mu_{\mathsf{E}}(\mathbf{C}|\mathbf{Z})$ via probability estimation factors (PEFs). Let $\mathbb{R}_{\geqslant 0}$ be the set of non-negative real numbers. A PEF with power $\beta > 0$ is a function $F : \mathrm{Rng}(\mathbf{CZ}) \to \mathbb{R}_{\geqslant 0}$ such that for all $\mu_{\mathsf{E}} \in \mathcal{C}$, $F(\mathbf{CZ})$ satisfies the PEF inequality

$$\mathbb{E}_{\mu_{\mathsf{E}}}(F(\mathbf{CZ})\mu_{\mathsf{E}}(\mathbf{C}|\mathbf{Z})^\beta) = \sum_{\mathbf{cz}} \mu_{\mathsf{E}}(\mathbf{cz})F(\mathbf{cz})\mu_{\mathsf{E}}(\mathbf{c}|\mathbf{z})^\beta \leqslant 1. \tag{2}$$

Note that $F(\mathbf{CZ})$ is a classical variable which takes value $F(\mathbf{cz})$ when the inputs and outputs are observed to be $\mathbf{z}$ and $\mathbf{c}$. In view of the PEF inequality above and the fact that $F(\mathbf{cz})\mu_{\mathsf{E}}(\mathbf{c}|\mathbf{z})^\beta \geqslant 0$ for all $\mathbf{cz}$, by Markov's inequality, we get

$$\mathbb{P}_{\mu_{\mathsf{E}}}(\mu_{\mathsf{E}}(\mathbf{C}|\mathbf{Z}) \geqslant (\epsilon F(\mathbf{CZ}))^{-1/\beta}) \leqslant \epsilon. \tag{3}$$

Equivalently, for each $\mu_{\mathsf{E}} \in \mathcal{C}$, the probability that $\mathbf{C}$ and $\mathbf{Z}$ take values $\mathbf{c}$ and $\mathbf{z}$ for which $(\epsilon F(\mathbf{C} = \mathbf{c}, \mathbf{Z} = \mathbf{z}))^{-1/\beta} \leqslant \mu_{\mathsf{E}}(\mathbf{C} = \mathbf{c}|\mathbf{Z} = \mathbf{z})$ is at most ϵ. This defines $(\epsilon F(\mathbf{CZ}))^{-1/\beta}$ as a level-ϵ probability estimator. Probability estimates provide lower bounds on the smooth min-entropy of $\mathbf{C}$ conditional on $\mathbf{ZE}$, which quantifies the amount of randomness certifiable in the presence of classical side information, as established in Refs. [25,26]. Throughout this work, we refer to a bound on a state-dependent quantity obtained from a statistic, either a lower or an upper bound depending on the context, as an estimate of the quantity interested.

In this work, we study the general case where the dimension of the quantum system E is finite but can be arbitrarily large. In the presence of quantum side information, instead of estimating conditional probabilities, we estimate sandwiched Rényi powers defined as follows. Fix $\alpha > 1$ and $\beta = \alpha - 1$. Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and $0 \leqslant \rho \ll \sigma \in \mathcal{H}$, where we write $\rho \ll \sigma$ if the support[1] of ρ is a subspace of the support of σ. The *sandwiched Rényi power of order* α *of* ρ *conditional on* σ is defined as

$$\mathcal{R}_\alpha(\rho|\sigma) = \mathrm{tr}((\sigma^{-\beta/(2\alpha)}\rho\sigma^{-\beta/(2\alpha)})^\alpha), \tag{4}$$

and the *normalized sandwiched Rényi power of order* α is defined as

$$\hat{\mathcal{R}}_\alpha(\rho|\sigma) = \frac{1}{\mathrm{tr}(\rho)}\mathcal{R}_\alpha(\rho|\sigma). \tag{5}$$

[1] If H is a linear operator on $\mathcal{H}$ and H is Hermitian, then the support of H is the span of the eigenvectors of H with nonzero eigenvalues.

We remark that the Rényi power $\mathcal{R}_\alpha(\rho|\sigma)$ is defined to be 0 if $\rho = 0$ and $\sigma = 0$, and that the normalized Rényi power $\hat{\mathcal{R}}_\alpha(\rho|\sigma)$ is defined to be 1 if $\rho = 0$. The definitions ensure that $\mathcal{R}_\alpha(\rho|\sigma)$ and $\hat{\mathcal{R}}_\alpha(\rho|\sigma)$ are always non-negative. The quantity $-\log_2(\hat{\mathcal{R}}_\alpha(\rho|\sigma))/\beta$ as defined in Refs. [34,35] is called the sandwiched Rényi entropy of order α of ρ conditional on σ. One motivation for estimating sandwiched Rényi powers is that the amount of randomness certifiable in the presence of quantum side information as quantified by the quantum smooth conditional min-entropy is bounded from below by a sandwiched Rényi entropy, see Prop. 6.5, p. 99 of Ref. [28]. Throughout this work, we assume that $\alpha > 1$ and so $\beta = \alpha - 1$ as introduced above is positive.

Given a state $\rho_{\mathbf{CZE}} \in \mathcal{S}_1(\mathbf{CZE})$, define $\rho_{\mathsf{E}}(\mathbf{z}) = \sum_{\mathbf{c}} \rho_{\mathsf{E}}(\mathbf{cz})$ and

$$\rho_{\mathbf{ZE}} = \sum_{\mathbf{z}} |\mathbf{z}\rangle\langle\mathbf{z}| \otimes \rho_{\mathsf{E}}(\mathbf{z}). \tag{6}$$

Note that $\rho_{\mathbf{ZE}} \in \mathcal{S}_1(\mathbf{ZE})$ and $\rho_{\mathbf{ZE}} = \mathrm{tr}_{\mathbf{C}}(\rho_{\mathbf{CZE}})$, where $\mathrm{tr}_{\mathbf{C}}$ is the partial trace over system $\mathbf{C}$. As discussed above, when the quantum system E is one-dimensional, $\rho_{\mathsf{E}}(\mathbf{cz}) = \mu_{\mathsf{E}}(\mathbf{cz})$ and so $\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) = \mu_{\mathsf{E}}(\mathbf{c}|\mathbf{z})^\beta$, making the connection to Eq. (2). Moreover, sandwiched Rényi powers provide lower bounds on the amount of certifiable randomness. These motivate us to define *quantum probability estimation*, with $\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z}))$ taking the role that $\mu_{\mathsf{E}}(\mathbf{c}|\mathbf{z})^\beta$ takes in classical probability estimation. With this in mind, we introduce quantum estimation factors (QEFs) as the quantum generalization of PEFs. A QEF with power $\beta > 0$ is a function $F : \mathrm{Rng}(\mathbf{CZ}) \to \mathbb{R}_{\geqslant 0}$ such that for all normalized states $\rho_{\mathbf{CZE}}$ in the model $\mathcal{C}$, $F(\mathbf{CZ})$ satisfies the QEF inequality

$$\sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))F(\mathbf{cz})\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) = \sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \leqslant 1. \tag{7}$$

The concept of a QEF generalizes techniques for certifying randomness against quantum side information used in previous works [9,13]. In particular, the role of QEFs is similar to the role of the weighting terms in the weighted $(1+\epsilon)$-randomness function of Eq. (6.4) in Ref. [9]. QEFs also play a role similar to that of the quantum systems $D_i\overline{D}_i$ in Eq. (16) of Ref. [13]. The existence of QEFs is suggested by the existence and construction of PEFs shown in our previous works [25,26]. Methods for constructing nontrivial and useful QEFs will be provided in Sec. VII. In this and the next two sections, we will present results for randomness certification using QEFs.

A QEF with power β can be interpreted as an estimator of a normalized sandwiched Rényi power of order $\alpha = 1 + \beta$. We formalize this interpretation as follows.

Theorem 1. Let $F(\mathbf{CZ})$ be a QEF with power β for the model $\mathcal{C}$. For an arbitrary normalized state $\rho_{\mathbf{CZE}}$ in $\mathcal{C}$,

$$\mathbb{P}_{\mu(\mathbf{CZ})}(1/(\epsilon F(\mathbf{CZ})) \leqslant \hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{CZ})\big|\rho_{\mathsf{E}}(\mathbf{Z}))) \leqslant \epsilon,$$

where $\mu(\mathbf{CZ}) = \mathrm{tr}_{\mathsf{E}}(\rho_{\mathbf{CZE}})$.

According to the theorem, for each normalized state $\rho_{\mathbf{CZE}}$ in the model $\mathcal{C}$, the probability that $\mathbf{C}$ and $\mathbf{Z}$ take values $\mathbf{c}$ and $\mathbf{z}$ for which $1/(\epsilon F(\mathbf{cz})) \leqslant \hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z}))$ is at most ϵ. This defines $1/(\epsilon F(\mathbf{CZ}))$ as a level-ϵ estimator of the normalized sandwiched Rényi power $\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{CZ})|\rho_{\mathsf{E}}(\mathbf{Z}))$, which is the QEF analog of the statement below Eq. (3) for PEFs.

Proof. According to the QEF inequality at the normalized state $\rho_{\mathbf{CZE}}$ and in view of the fact that $\mu(\mathbf{cz}) = \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))$,

$$\begin{aligned} 1 &\geqslant \sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))F(\mathbf{cz})\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})\big|\rho_{\mathsf{E}}(\mathbf{z})) \\ &= \sum_{\mathbf{cz}} \mu(\mathbf{cz})F(\mathbf{cz})\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\ &= \mathbb{E}_{\mu(\mathbf{CZ})}(F(\mathbf{CZ})\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{CZ})|\rho_{\mathsf{E}}(\mathbf{Z}))). \end{aligned}$$

Since $F(\mathbf{CZ})\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{CZ})|\rho_{\mathsf{E}}(\mathbf{Z})) \geqslant 0$ and by Markov's inequality,

$$\mathbb{P}_{\mu(\mathbf{CZ})}(F(\mathbf{CZ})\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{CZ})|\rho_{\mathsf{E}}(\mathbf{Z})) \geqslant 1/\epsilon) \leqslant \epsilon.$$

The theorem follows by rearranging the inequality defining the event in the probability on the left-hand side. ■

In view of our previous result [25,26] that level-ϵ estimators of the conditional probability $\mu_{\mathsf{E}}(\mathbf{C}|\mathbf{Z})$ provide lower bounds on the smooth conditional min-entropy in the presence of classical side information and the observation that the normalized sandwiched Rényi power $\hat{\mathcal{R}}_\alpha(\rho_{\mathsf{E}}(\mathbf{CZ})|\rho_{\mathsf{E}}(\mathbf{Z}))$ reduces to $\mu_{\mathsf{E}}(\mathbf{C}|\mathbf{Z})^\beta$ when the quantum system E is one-dimensional, theorem 1 suggests that lower bounds on the smooth conditional min-entropy in the presence of quantum side information can be obtained with QEFs. To obtain such lower bounds, we take advantage of the relation between sandwiched Rényi powers and quantum smooth conditional min-entropies established by Prop. 6.5, p. 99 of Ref. [28]. For this, we need to derive upper bounds on sandwiched Rényi powers (corresponding to lower bounds on sandwiched Rényi entropies) in a way different from theorem 1. With these considerations, we present our first main result.

Theorem 2. Let $\rho_{\mathbf{CZE}}$ be a state in $\mathcal{S}_1(\mathbf{CZE})$. Suppose that $F(\mathbf{CZ}) \geqslant 0$ satisfies the QEF inequality (7) at $\rho_{\mathbf{CZE}}$. Fix $q \in (0,1]$ and write the event $\Phi = \{\mathbf{cz} : F(\mathbf{cz}) \geqslant 1/q^\beta\}$. Let $\Phi' \subseteq \Phi$ and let $\kappa = \sum_{\mathbf{cz}\in\Phi'} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))$ be the probability of the event Φ' according to the classical probability distribution of relevant events induced by the state $\rho_{\mathbf{CZE}}$. Denote the normalized classical-quantum state conditional on Φ' by $\rho_{\mathbf{CZE}|\Phi'}$, and let $\rho_{\mathbf{ZE}} = \mathrm{tr}_{\mathbf{C}}(\rho_{\mathbf{CZE}})$. Then

$$\mathcal{R}_\alpha(\rho_{\mathbf{CZE}|\Phi'}|\mathbb{1}_{\mathbf{C}} \otimes \rho_{\mathbf{ZE}}) \leqslant \frac{q^\beta}{\kappa^\alpha}. \tag{8}$$

Proof. The normalized classical-quantum state conditional on Φ' can be explicitly written as

$$\rho_{\mathbf{CZE}|\Phi'} = \sum_{\mathbf{cz}\in\Phi'} |\mathbf{cz}\rangle\langle\mathbf{cz}| \otimes \rho_{\mathsf{E}}(\mathbf{cz})/\kappa. \tag{9}$$

Direct calculation establishes the following equality:

$$\mathcal{R}_\alpha(\rho_{\mathbf{CZE}|\Phi'}|\mathbb{1}_{\mathbf{C}} \otimes \rho_{\mathbf{ZE}}) = \sum_{\mathbf{cz}\in\Phi'} \mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})/\kappa\big|\rho_{\mathsf{E}}(\mathbf{z})). \tag{10}$$

Then, the bound in the theorem statement follows immediately from the QEF inequality (7) and the non-negativity of both sandwiched Rényi powers and QEFs. Specifically, it suffices to rewrite the QEF inequality and drop irrelevant

terms:

$$\begin{aligned} 1 &\geqslant \sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\ &\geqslant \sum_{\mathbf{cz}\in\Phi'} F(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\ &\geqslant \sum_{\mathbf{cz}\in\Phi'} \frac{1}{q^\beta}\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\ &= \sum_{\mathbf{cz}\in\Phi'} \frac{\kappa^\alpha}{q^\beta}\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})/\kappa|\rho_{\mathsf{E}}(\mathbf{z})). \end{aligned}$$

Using Eq. (10), the claimed inequality is obtained by multiplying both sides of the above inequality by q^β/κ^α ■.

We remark that for experimentally relevant models a QEF with power β is a PEF with the same power, as the model for an experiment in the presence of quantum side information is a superset of the model for the experiment in the presence of classical side information. For Bell-test configurations, considering that a PEF is a test factor for the hypothesis test of local realism (see the last paragraph of the main text in the arXiv version of Ref. [26]), so is a QEF. Therefore, if a finite sequence of trial results $\mathbf{CZ}$ is explainable by local realism and $F(\mathbf{CZ})$ is a QEF with power β for the experiment, according to Ref. [36] the event Φ in the statement of theorem 2 would happen with probability at most q^β (which is parallel to the statement for a PEF in the last paragraph of the main text in the arXiv version of Ref. [26]).

IV. QUANTUM SMOOTH CONDITIONAL MIN-ENTROPY

The amount of randomness that is available in the presence of quantum side information is characterized by the quantum conditional min-entropy [27]. Below we first specialize the definitions of relevant quantities in Refs. [27,37] to the family of classical-quantum states treated in this work. Then we show that QEFs can certify the presence of randomness in $\mathbf{C}$ conditional on $\mathbf{ZE}$.

We consider the classical-quantum state $\rho_{\mathbf{CZE}}$ which may be subnormalized. The state $\rho_{\mathbf{CZE}}$ has *maximum probability* (abbreviated as *max-prob* below) p of $\mathbf{C}$ given $\mathbf{ZE}$ if there exists a normalized state $\sigma_{\mathbf{ZE}} \in \mathcal{S}_1(\mathbf{ZE})$ such that $\rho_{\mathsf{E}}(\mathbf{cz}) \leqslant p\sigma_{\mathsf{E}}(\mathbf{z})$ for all $\mathbf{cz}$. The exact max-prob of $\mathbf{C}$ given $\mathbf{ZE}$ at $\rho_{\mathbf{CZE}}$ is

$$\begin{aligned} P_{\max}(\mathbf{C}|\mathbf{ZE})_\rho = \inf_{\sigma_{\mathbf{ZE}}} \inf_p \{p : \rho_{\mathsf{E}}(\mathbf{cz}) \leqslant p\sigma_{\mathsf{E}}(\mathbf{z}) \quad \text{for all } \mathbf{cz}, \\ \sigma_{\mathbf{ZE}} \in \mathcal{S}_1(\mathbf{ZE})\}. \end{aligned} \tag{11}$$

The quantity $H_\infty(\mathbf{C}|\mathbf{ZE})_\rho = -\log_2(P_{\max}(\mathbf{C}|\mathbf{ZE})_\rho)$ is called the *quantum conditional min-entropy* of $\mathbf{C}$ given $\mathbf{ZE}$ at $\rho_{\mathbf{CZE}}$. When writing a state such as $\rho_{\mathbf{CZE}}$ in a subscript we omit the underlying systems of the state if there is no ambiguity. It is conventional to focus on additive entropy quantities. However, since PEF- and QEF-based estimates are naturally related to probabilities, we find it convenient to focus on multiplicative, probability-related quantities instead.

The quantum conditional min-entropy provides a lower bound on the number of near-uniform random bits that can be extracted from $\mathbf{C}$ conditional on $\mathbf{ZE}$ but this bound is unnecessarily conservative [27]. A better bound may be provided by the quantum *smooth* conditional min-entropy. Assume that $\rho_{\mathbf{CZE}}$ is a normalized classical-quantum state. Then $\rho_{\mathbf{CZE}}$ has *ϵ-smooth max-prob p* of $\mathbf{C}$ given $\mathbf{ZE}$ if there exists a subnormalized state $\rho'_{\mathbf{CZE}}$ which has exact max-prob $P_{\max}(\mathbf{C}|\mathbf{ZE})_{\rho'} \leqslant p$ and is within purified distance ϵ from $\rho_{\mathbf{CZE}}$. Here, the purified distance [37] between the normalized state $\rho_{\mathbf{CZE}}$ and the subnormalized state $\rho'_{\mathbf{CZE}}$ is defined as

$$\mathrm{PD}(\rho_{\mathbf{CZE}}, \rho'_{\mathbf{CZE}}) = \sqrt{1 - \left(\sum_{\mathbf{cz}} \mathrm{tr}(|\sqrt{\rho_{\mathsf{E}}(\mathbf{cz})}\sqrt{\rho'_{\mathsf{E}}(\mathbf{cz})}|)\right)^2}, \tag{12}$$

where for a matrix M, its modulus $|M|$ is given by $|M| = \sqrt{M^\dagger M}$. The exact ϵ-smooth max-prob of $\mathbf{C}$ given $\mathbf{ZE}$ at $\rho_{\mathbf{CZE}}$ is

$$\begin{aligned} P^\epsilon_{\max}(\mathbf{C}|\mathbf{ZE})_\rho = \inf_{\rho'_{\mathbf{CZE}}} \{P_{\max}(\mathbf{C}|\mathbf{ZE})_{\rho'} : \rho'_{\mathbf{CZE}} \in \mathcal{S}_{\leqslant 1}(\mathbf{CZE}), \\ \mathrm{PD}(\rho_{\mathbf{CZE}}, \rho'_{\mathbf{CZE}}) \leqslant \epsilon\}. \end{aligned} \tag{13}$$

The quantity $H^\epsilon_\infty(\mathbf{C}|\mathbf{ZE})_\rho = -\log_2(P^\epsilon_{\max}(\mathbf{C}|\mathbf{ZE})_\rho)$ is called the *quantum ϵ-smooth conditional min-entropy* of $\mathbf{C}$ given $\mathbf{ZE}$ at $\rho_{\mathbf{CZE}}$. The above definitions are monotonic in the smoothness parameter ϵ. For example, if $P^\epsilon_{\max}(\mathbf{C}|\mathbf{ZE})_\rho \leqslant p$ and $\epsilon' > \epsilon$, then $P^{\epsilon'}_{\max}(\mathbf{C}|\mathbf{ZE})_\rho \leqslant p$.

The second main result of this work is that QEFs yield lower bounds on quantum smooth conditional min-entropies, which is formalized as follows.

Theorem 3. Fix $q', \epsilon, \kappa' \in (0, 1]$. Write the event $\Phi' = \{\mathbf{cz} : F(\mathbf{cz}) \geqslant 1/(q'^\beta(\epsilon^2/2))\}$. Under the same conditions as in theorem 2 with $q = q'(1-\sqrt{1-\epsilon^2})^{1/\beta} \in (0, 1]$, *either* $\kappa = \sum_{\mathbf{cz}\in\Phi'} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz})) < \kappa'$ *or* the quantum smooth conditional min-entropy satisfies

$$H^\epsilon_\infty(\mathbf{C}|\mathbf{ZE})_{\rho_{\mathbf{CZE}|\Phi'}} \geqslant -\log_2(q') + \frac{\alpha}{\beta}\log_2(\kappa').$$

The event Φ' can be interpreted as the event that the experiment succeeds, and κ is the probability of success according to the classical probability distribution of relevant events induced by the state $\rho_{\mathbf{CZE}}$.

Proof. The theorem is an immediate consequence of theorem 2 and Prop. 6.5, p. 99 of Ref. [28]. We first apply Prop. 6.5, p. 99 of Ref. [28] with the following substitutions: (1) $\rho \to \rho_{\mathbf{CZE}|\Phi'}$ in Eq. (9) and (2) $\sigma \to \rho_{\mathbf{ZE}}$ in Eq. (6). With our notation, this gives

$$\begin{aligned} \inf_{\rho'_{\mathbf{CZE}}} \inf_p \{p : \rho'_{\mathsf{E}}(\mathbf{cz}) \leqslant p\rho_{\mathsf{E}}(\mathbf{z}) \text{ for all } \mathbf{cz}, \\ \rho'_{\mathbf{CZE}} \in \mathcal{S}_{\leqslant 1}(\mathbf{CZE}), \mathrm{PD}(\rho_{\mathbf{CZE}|\Phi'}, \rho'_{\mathbf{CZE}}) \leqslant \epsilon\} \\ \leqslant \left(\frac{\mathcal{R}_\alpha(\rho_{\mathbf{CZE}|\Phi'}|\mathbb{1}_{\mathbf{C}} \otimes \rho_{\mathbf{ZE}})}{1-\sqrt{1-\epsilon^2}}\right)^{1/\beta}. \end{aligned} \tag{14}$$

According to the definition of $P^\epsilon_{\max}$ in Eq. (13), the left-hand side of Eq. (14) is an upper bound of $P^\epsilon_{\max}(\mathbf{C}|\mathbf{ZE})_{\rho_{\mathbf{CZE}|\Phi'}}$. Therefore

$$P^\epsilon_{\max}(\mathbf{C}|\mathbf{ZE})_{\rho_{\mathbf{CZE}|\Phi'}} \leqslant \left(\frac{\mathcal{R}_\alpha(\rho_{\mathbf{CZE}|\Phi'}|\mathbb{1}_{\mathbf{C}} \otimes \rho_{\mathbf{ZE}})}{1-\sqrt{1-\epsilon^2}}\right)^{1/\beta}. \tag{15}$$

Considering that $1-\sqrt{1-\epsilon^2} > \epsilon^2/2$ when $\epsilon \in (0, 1]$, we have $\Phi' \subseteq \Phi$. Hence we can apply theorem 2 and by

combining Eq. (15) with Eq. (8), we get

$$P^{\epsilon}_{\max}(\mathbf{C}|\mathbf{ZE})_{\rho_{\mathbf{CZE}|\Phi'}} \leqslant \left(\frac{q^{\beta}}{(1-\sqrt{1-\epsilon^2})\kappa^{\alpha}}\right)^{1/\beta} = \frac{q'}{\kappa^{\alpha/\beta}}, \tag{16}$$

which is equivalent to the statement in the theorem considering the relation between κ and κ'. ■

V. QUANTUM RANDOMNESS GENERATION

The last theorem indicates that QEFs can certify the presence of randomness with respect to quantum side information. With a quantum-proof extractor, we can design an end-to-end randomness-generation protocol to extract near-uniform random bits. Our goal is to make this protocol sound, meaning that the protocol has guaranteed performance no matter how low the success probability is. In this section, we first discuss the extractor used, as it determines the choices of various parameters in the protocol. Then we formalize the definition of soundness. Finally, we present our randomness-generation protocol and prove its soundness.

A. Quantum-proof strong extractors

The input, output, and seed to an extractor are denoted by C, R, and S. Define $n_i = \log_2(|\mathrm{Rng}(C)|)$, $k_o = \log_2(|\mathrm{Rng}(R)|)$, and $k_s = \log_2(|\mathrm{Rng}(S)|)$. When C, R, and S are bit strings, n_i, k_o, and k_s are their respective lengths. The seed S has a uniform probability distribution and is independent of all other classical variables and quantum systems.

Consider a function $\mathrm{Ext} : \mathrm{Rng}(C) \times \mathrm{Rng}(S) \to \mathrm{Rng}(R)$. The function Ext is called a *quantum-proof strong extractor* with parameters $(n_i, k_s, k_o, k_i, \epsilon_x)$ if for every normalized classical-quantum state $\rho_{C\mathsf{E}} = \sum_c |c\rangle\langle c| \otimes \rho_{\mathsf{E}}(c)$ with $H_\infty(C|\mathsf{E})_\rho \geqslant k_i$, the joint state $\rho_{RS\mathsf{E}}$ of the extractor output $R = \mathrm{Ext}(C, S)$, the seed S and the quantum system E satisfies

$$\mathrm{PD}(\rho_{RS\mathsf{E}}, \tau_{RS} \otimes \rho_{\mathsf{E}}) \leqslant \epsilon_x, \tag{17}$$

where τ_{RS} is a fully mixed and normalized state of dimension $2^{k_s+k_o}$ and ρ_{E} is the marginal state of E according to $\rho_{C\mathsf{E}}$. Inequality (17) asserts that the joint state of R and S is nearly uniform (a property of strong extractors) and almost independent of the quantum side information in E (a property of quantum-proof extractors). A specific strong extractor is Trevisan's extractor [38], which is proven to be quantum-proof in Ref. [39].

To ensure the inequality in Eq. (17) hold, the parameters $(n_i, k_s, k_o, k_i, \epsilon_x)$ need to satisfy a set of constraints, called *extractor constraints*. The extractor constraints depend on the specific quantum-proof strong extractor to be used, but these constraints always include that $1 \leqslant k_i \leqslant n_i$, $k_s \geqslant 0$, $k_o \leqslant k_i$, and $0 < \epsilon_x \leqslant 1$.

B. Protocol soundness

A generic randomness-generation protocol $\mathcal{G}$ produces three outputs: $R_{\mathcal{G}}$—a bit string of length k_o consisting of fresh random bits generated by the protocol, $S_{\mathcal{G}}$—a bit string of length k_s consisting of the random seed S required for running the protocol, and $P_{\mathcal{G}}$—a flag whose value 0 or 1 indicates failure or success, respectively. The outputs $R_{\mathcal{G}}$, $S_{\mathcal{G}}$ and $P_{\mathcal{G}}$ are determined not only by the inputs $\mathbf{Z}$ and outputs $\mathbf{C}$ of the devices, but also by the specific quantum-proof strong extractor Ext used and its seed S.

Given a normalized state $\rho_{\mathbf{CZE}}$ in the model $\mathcal{C}$, we denote the normalized classical-quantum state of the classical variables $R_{\mathcal{G}}$, $S_{\mathcal{G}}$, $P_{\mathcal{G}}$, $\mathbf{Z}$ and the quantum system E after running the protocol with the extractor Ext on $\rho_{\mathbf{CZE}}$ by $\rho_{R_{\mathcal{G}}S_{\mathcal{G}}P_{\mathcal{G}}\mathbf{ZE}}$. The normalized state conditional on success $P_{\mathcal{G}} = 1$ is denoted by $\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{ZE}|(P_{\mathcal{G}}=1)}$. A randomness-generation protocol $\mathcal{G}$ is ϵ-*sound* at the normalized state $\rho_{\mathbf{CZE}}$ if there exists a normalized state $\sigma_{\mathbf{ZE}} \in \mathcal{S}_1(\mathbf{ZE})$ such that

$$\mathrm{PD}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{ZE}|(P_{\mathcal{G}}=1)}, \tau_{R_{\mathcal{G}}S_{\mathcal{G}}} \otimes \sigma_{\mathbf{ZE}})\mathbb{P}_\rho(P_{\mathcal{G}} = 1) \leqslant \epsilon, \tag{18}$$

where $\tau_{R_{\mathcal{G}}S_{\mathcal{G}}}$ is a fully mixed and normalized state of dimension $2^{k_o+k_s}$ and $\mathbb{P}_\rho(P_{\mathcal{G}} = 1)$ is the probability of success according to the classical probability distribution of relevant events induced by the state $\rho_{R_{\mathcal{G}}S_{\mathcal{G}}P_{\mathcal{G}}\mathbf{ZE}}$.

The protocol $\mathcal{G}$ is ϵ-sound for a model $\mathcal{C}$ if it is ϵ-sound at all normalized states in the model. Our goal is to obtain an ϵ-sound protocol for the model of the randomness-generation experiment. We emphasize that the soundness error ϵ absorbs the contribution of the success probability and so unlike the certification of quantum smooth conditional min-entropy as done in theorem 3, a soundness statement does not require a presumed bound κ' on the success probability.

Our definitions of quantum-proof strong extractors and protocol soundness differ from others such as those in Refs. [40,41] by requiring small purified distance instead of small trace distance, where the trace distance between two normalized states ρ and σ is defined as

$$\mathrm{D}(\rho, \sigma) = \tfrac{1}{2}\mathrm{tr}(|\rho - \sigma|), \tag{19}$$

where $|\rho - \sigma|$ is the modulus of the matrix $(\rho - \sigma)$. With this change we can take advantage of the extendibility of the purified distance to previously traced-out quantum systems in order to analyze the composability of protocols involving the same devices, see Appendix A for a detailed discussion. We also note that as the purified distance is an upper bound of the trace distance (see Prop. 3.3, p. 50 of Ref. [37]), our definitions imply the definitions in Refs. [40,41].

We remark that a protocol $\mathcal{G}$ is called κ-*complete* for a model $\mathcal{C}$ if there exist a normalized state $\rho'_{\mathbf{CZE}}$ in the model and the corresponding state $\rho'_{R_{\mathcal{G}}S_{\mathcal{G}}P_{\mathcal{G}}\mathbf{ZE}}$ after running the protocol according to which the success probability satisfies $\mathbb{P}_{\rho'}(P_{\mathcal{G}} = 1) \geqslant \kappa$. Completeness is an important factor to consider when designing an experiment, while soundness guarantees the performance of the protocol regardless of the actual implementation of the experiment.

C. QEF-based randomness-generation protocol

The end-to-end randomness-generation protocol is displayed in protocol 1, where the notation $0^{\frown k}$ denotes a string of k consecutive zeros. We emphasize that as specified in protocol 1, the parameters k_o, k_s, k_i, ϵ, ϵ_x, n and β are determined before running the experiment. In this work, the QEF $F(\mathbf{CZ})$ with power β for a sequence of trials is constructed by multiplying the QEFs $F_i(C_iZ_i)$ with the same power β for

Protocol 1: Input-conditional randomness generation.

Input :
- k_o—the number of fresh random bits to be generated.
- ϵ—the soundness error satisfying $\epsilon \in (0, 1]$.

Given :
- An experiment with inputs $\mathbf{Z}$ and outputs $\mathbf{C}$ of length n, as specified in the first paragraph of Sec. III.
- A QEF $F(\mathbf{CZ})$ with power β for the model $\mathcal{C}$ of the experiment (see the paragraph including Eq. (7)).
- A quantum-proof strong extractor Ext (see Sec. V A).

Promise:
- The set $\mathcal{X}$ defined by $\mathcal{X} = \{(k_s, k_i, \epsilon_x) : (n_i, k_s, k_o, k_i, \epsilon_x < \epsilon)$ satisfies the extractor constraints for Ext (see Sec. V A), where $n_i = \log_2(|\mathrm{Rng}(\mathbf{C})|)\}$ is nonempty.

Output : $R_{\mathcal{G}}, S_{\mathcal{G}}, P_{\mathcal{G}}$ as specified in the first paragraph of Sec. V B.

Choose $(k_s, k_i, \epsilon_x) \in \mathcal{X}$;
Get an instance s of the uniformly random seed S of length k_s;
Set $\epsilon_h = (\epsilon - \epsilon_x)$;
If $\beta > 1$, then set $p = 2^{-k_i}\epsilon^{(\beta-1)/\beta}$, otherwise set $p = 2^{-k_i}$;
Set $f_{\min} = 1/(p^{\beta}(\epsilon_h^2/2))$;
Run the experiment and get an instance $\mathbf{cz}$ of $\mathbf{CZ}$;
Compute $f = F(\mathbf{cz})$;
if $f < f_{\min}$ **then**
  Return $P_{\mathcal{G}} = 0, R_{\mathcal{G}} = 0^{\frown k_o}, S_{\mathcal{G}} = s$; // `Protocol failed.`
else
  Return $P_{\mathcal{G}} = 1, R_{\mathcal{G}}$=Ext$(\mathbf{c}, s), S_{\mathcal{G}}$=$s$; // `Protocol succeeded.`
end

each individual trial i, $i = 1, 2, \ldots, n$ (see Sec. VII B). In this case, the trialwise QEF $F_i(C_iZ_i)$ needs only to be fixed before the ith trial rather than before the start of the experiment. We assume that the set $\mathcal{X}$ defined in protocol 1 is nonempty. This assumption needs to be checked before invoking the protocol, and the input parameters can be adjusted to ensure that the assumption holds.

The soundness of protocol 1 can be proven by composing theorem 3 with the quantum-proof strong extractor used.

Theorem 4. Protocol 1 is an ϵ-sound randomness-generation protocol for the model $\mathcal{C}$.

Proof. Let $\rho_{\mathbf{CZE}}$ be an arbitrary normalized classical-quantum state in the model $\mathcal{C}$ from which $\mathbf{CZ}$ is instantiated to $\mathbf{cz}$ when running the protocol. Write the event $\Phi = \{\mathbf{cz} : F(\mathbf{cz}) \geqslant f_{\min} = 1/(p^{\beta}(\epsilon_h^2/2))\}$ such that when $\mathbf{cz} \in \Phi$, the protocol succeeds, that is, $P_{\mathcal{G}} = 1$. Let $\kappa = \sum_{\mathbf{cz}\in\Phi} \mathrm{Tr}(\rho_{\mathsf{E}}(\mathbf{cz})) = \mathbb{P}_{\rho}(P_{\mathcal{G}} = 1)$ be the probability of success according to the classical probability distribution of relevant events induced by the state $\rho_{\mathbf{CZE}}$.

We first consider the case $\kappa \in [\epsilon, 1]$. We apply theorem 3 with the following substitutions: (1) $\epsilon \to \epsilon_h/\kappa$ and (2) $q' \to p\kappa^{2/\beta}$. With these substitutions, the event Φ' in the statement of theorem 3 becomes the same as the event Φ defined above, and so the parameter κ in the statement of theorem 3 becomes the same as the parameter κ introduced above. According to Eq. (16), we have

$$P_{\max}^{\epsilon_h/\kappa}(\mathbf{C}|\mathbf{ZE})_{\rho_{\mathbf{CZE}|\Phi}} \leqslant p\kappa^{2/\beta}/\kappa^{\alpha/\beta} = p\kappa^{(1-\beta)/\beta}. \tag{20}$$

The protocol's choice of p depends on β. Specifically, if $\beta \leqslant 1$, then $p\kappa^{(1-\beta)/\beta} \leqslant p = 2^{-k_i}$, and if $\beta > 1$, considering that $\kappa \in [\epsilon, 1]$ we have $p\kappa^{(1-\beta)/\beta} \leqslant p\epsilon^{(1-\beta)/\beta} = 2^{-k_i}$. Hence, we always have $p\kappa^{(1-\beta)/\beta} \leqslant 2^{-k_i}$, and so from Eq. (20), we get

$$P_{\max}^{\epsilon_h/\kappa}(\mathbf{C}|\mathbf{ZE})_{\rho_{\mathbf{CZE}|\Phi}} \leqslant 2^{-k_i}. \tag{21}$$

The extractor constraints ensure that $k_i \leqslant n_i = \log_2(|\mathrm{Rng}(\mathbf{C})|)$, so $2^{-k_i}|\mathrm{Rng}(\mathbf{C})| \geqslant 1$. According to lemma 7 in Appendix B, there exists a normalized state $\rho'_{\mathbf{CZE}}$ such that

$$\mathrm{PD}(\rho_{\mathbf{CZE}|\Phi}, \rho'_{\mathbf{CZE}}) \leqslant \epsilon_h/\kappa \tag{22}$$

and

$$P_{\max}(\mathbf{C}|\mathbf{ZE})_{\rho'} \leqslant 2^{-k_i}, \tag{23}$$

that is, $H_{\infty}(\mathbf{C}|\mathbf{ZE})_{\rho'} \geqslant k_i$. Because the parameters $(n_i, k_s, k_o, k_i, \epsilon_x)$ satisfy the extractor constraints, we can apply the quantum-proof strong extractor Ext with the state $\rho'_{\mathbf{CZE}}$ and get

$$\mathrm{PD}(\rho'_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{ZE}}, \tau_{R_{\mathcal{G}}S_{\mathcal{G}}} \otimes \rho'_{\mathbf{ZE}}) \leqslant \epsilon_x, \tag{24}$$

where $\tau_{R_{\mathcal{G}}S_{\mathcal{G}}}$ is a fully mixed and normalized state of dimension $2^{k_o+k_s}$.

Since the purified distance satisfies the data-processing inequality (theorem 3.4, p. 51 of Ref. [37]), from Eq. (22), we get

$$\mathrm{PD}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{ZE}|\Phi}, \rho'_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{ZE}}) \leqslant \epsilon_h/\kappa. \tag{25}$$

The triangle inequality for the purified distance (Prop. 3.2, p. 50 of Ref. [37]) together with Eqs. (24) and (25) yield

$$\mathrm{PD}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{ZE}|\Phi}, \tau_{R_{\mathcal{G}}S_{\mathcal{G}}} \otimes \rho'_{\mathbf{ZE}}) \leqslant \epsilon_x + \epsilon_h/\kappa.$$

We multiply both sides by κ for

$$\mathrm{PD}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{ZE}|\Phi}, \tau_{R_{\mathcal{G}}S_{\mathcal{G}}} \otimes \rho'_{\mathbf{ZE}})\kappa \leqslant \epsilon_x\kappa + \epsilon_h \leqslant \epsilon_x + \epsilon_h = \epsilon.$$

For the case $\kappa < \epsilon$, since the purified distance cannot be larger than one,

$$\mathrm{PD}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{ZE}|\Phi}, \tau_{R_{\mathcal{G}}S_{\mathcal{G}}} \otimes \rho_{\mathbf{ZE}|\Phi})\kappa \leqslant \kappa < \epsilon.$$

Therefore the condition for ϵ-soundness is satisfied for the full range of values of κ at the state $\rho_{\mathbf{CZE}}$. Because $\rho_{\mathbf{CZE}}$ is an arbitrary normalized state in the model $\mathcal{C}$, protocol 1 is ϵ-sound for the model $\mathcal{C}$. ■

VI. CONSTRUCTION OF MODELS

In order to perform quantum probability estimation, we first need to specify the *model* for the experiment. The model is the set of all possible classical-quantum states that can occur at the end of the experiment.

The model for the whole experiment is normally constructed by combining models for the individual trials, where the model for a trial specifies the set of all possible states describing the joint state of the classical results at the trial and the quantum system E. The model for a trial can depend on the past and is usually specified by known constraints on the trial. In the case of Bell tests, these constraints include the familiar nonsignaling conditions [32,33] and the requirement that the trial results can be achieved with measurements on separate quantum systems according to the configuration.

We refer to the operation of combining trial models as *model chaining*. When chaining trial models, a Markov-chain condition on the inputs $\mathbf{Z}$ and outputs $\mathbf{C}$ is required in order

to certify randomness in $\mathbf{C}$ conditional on both $\mathbf{Z}$ and E (see Sec. VI B for details). This is similar to the Markov-chain condition required by entropy accumulation [13,29]. Since quantum probability estimation can be applied to trials satisfying the Markov-chain condition, it does not require the trials to be independent and identically distributed (i.i.d.).

In this section, we give a formal definition of a model and explain the details behind the model construction. For this, we consider an experiment performed with quantum devices for either device-dependent or device-independent randomness generation, as described in Fig. 1. Before the experiment, the initial state of the quantum devices may be correlated with an external quantum system E. After the experiment, we obtain the inputs $\mathbf{Z}$ and outputs $\mathbf{C}$. At each trial of the experiment, we allow arbitrary one-way communication from the system E to the devices. For example, E can initialize the state of the quantum devices via a one-way communication channel. We also allow the possibility that the device initialization at a trial by E depends on the past inputs preceding the trial. This implies that the random inputs $\mathbf{Z}$ can come from public-randomness sources, as first pointed out in Ref. [6]. However, at any stage of the experiment, the information of the outputs $\mathbf{C}$ cannot be leaked to E.

A. General models

A model is generally denoted by $\mathcal{C}$. To specify the classical variable or variables that a model depends on, we use $\mathcal{C}(U), \mathcal{C}(UV)$, etc. The default quantum system underlying a model is E. A *model* $\mathcal{C}(U)$ *for* $U\mathsf{E}$ is defined as a subset of classical-quantum states $\rho_{U\mathsf{E}}$ in $\mathcal{S}(U\mathsf{E})$ closed under multiplication by non-negative real numbers. The set of normalized classical-quantum states in $\mathcal{C}(U)$ is denoted by $\mathcal{N}(\mathcal{C}(U)) = \{\rho_{U\mathsf{E}} : \rho_{U\mathsf{E}} \in \mathcal{C}(U) \text{ and } \rho_{U\mathsf{E}} \in \mathcal{S}_1(U\mathsf{E})\}$. In a similar way, we can define a model that depends on several classical variables, such as $\mathcal{C}(UV)$ for $UV\mathsf{E}$.

A model becomes *classical* when the quantum system E is one-dimensional or traced out. In this case, the model specifies the set of un-normalized probability distributions of the underlying classical variable or variables. A classical model for U is denoted by $\mathcal{C}_{\mathrm{cl}}(U)$.

Model chaining is formally specified as follows. Suppose that $\mathcal{C}(U)$ is a model for $U\mathsf{E}$ and for each u, $\mathcal{C}_u(V)$ is a u-dependent model for $V\mathsf{E}$. We write $\mathcal{C}_U(V)$ for the family of u-dependent models consisting of all $\mathcal{C}_u(V)$. The result of *chaining* $\mathcal{C}(U)$ *and* $\mathcal{C}_U(V)$ is the model $\mathcal{C}(UV)$ for $UV\mathsf{E}$ defined by

$$\mathcal{C}(U)\circ\mathcal{C}_U(V) = \{\rho_{UV\mathsf{E}} : \rho_{U\mathsf{E}} \doteq \mathrm{tr}_V(\rho_{UV\mathsf{E}}) \in \mathcal{C}(U) \text{ and for all } u,\ \rho_{uV\mathsf{E}} \in \mathcal{C}_u(V)\}, \tag{26}$$

where $\rho_{uV\mathsf{E}}$ is the u-dependent classical-quantum state for $V\mathsf{E}$ determined from $\rho_{UV\mathsf{E}} = \sum_{uv} |uv\rangle\langle uv| \otimes \rho_{\mathsf{E}}(uv)$ by $\rho_{uV\mathsf{E}} = \sum_v |v\rangle\langle v| \otimes \rho_{\mathsf{E}}(uv)$.

The chaining operation can be applied inductively to construct a model for the whole experiment from models for the individual trials. Let us consider an experiment with a finite sequence of classical variables $\mathbf{U} = (U_i)_{i=1}^n$, where U_i is the classical variable associated with the i'th trial of the experiment. (In a randomness-generation experiment, $U_i = C_i Z_i$.) Let $\mathbf{U}_{<i} = (U_j)_{j=1}^{i-1}$ and $\mathbf{u}_{<i} = (u_j)_{j=1}^{i-1}$ be the sequences of classical variables and their values before the ith trial. The sequences $\mathbf{U}_{\leqslant i}$ and $\mathbf{u}_{\leqslant i}$ are defined similarly. By convention, $\mathbf{U}_{\leqslant 0}$ and $\mathbf{u}_{\leqslant 0}$ are empty sequences. We construct the model $\mathcal{C}(\mathbf{U})$ by chaining past-conditional models $\mathcal{C}_{\mathbf{U}_{<i}}(U_i)$. The trial models $\mathcal{C}_{\mathbf{U}_{<i}}(U_i)$ can be constructed by considering all allowed measurements for the device configuration in an experiment, as described in the next paragraph. We call such trial models *induced models*.

Consider a generic trial and the associated classical variable U, where for generic trials we omit the trial index and make the dependence on the past results implicitly by dropping the subscript. Let D be the quantum system of the devices and $\rho_{\mathsf{DE}} \in \mathcal{S}(\mathsf{DE})$ be the joint state of the quantum systems D and E before the trial. The state ρ_{DE} can be arbitrary as the system E is inaccessible from the experiment and also has the freedom to prepare the state ρ_{DE}. Moreover, the state ρ_{DE} can be un-normalized, as it is prepared probabilistically conditional on the past results. Let $\mathcal{P}_{\mathsf{D}}(U)$ be a family of positive-operator valued measures (POVMs) of D with outcome U. Then the trial model *induced* by the family $\mathcal{P}_{\mathsf{D}}(U)$ of POVMs is defined as

$$\mathcal{M}(\mathcal{P}_{\mathsf{D}}(U);\mathsf{E}) = \left\{ \sum_u |u\rangle\langle u| \otimes \mathrm{tr}_{\mathsf{D}}(\rho_{\mathsf{DE}}(P_{\mathsf{D}}(u)\otimes \mathbb{1}_{\mathsf{E}})) : \rho_{\mathsf{DE}} \in \mathcal{S}(\mathsf{DE}), P_{\mathsf{D}}(U) \in \mathcal{P}_{\mathsf{D}}(U) \right\}.$$

The specific family $\mathcal{P}_{\mathsf{D}}(U)$ of POVMs may depend on the past results; however, each POVM $P_{\mathsf{D}}(U)$ in $\mathcal{P}_{\mathsf{D}}(U)$ should be consistent with the behavior of the quantum devices at the trial. For example, in Bell-test configurations the system D can be decomposed into several subsystems associated with each local party. Therefore the POVM $P_{\mathsf{D}}(U)$ should have a tensor-product structure over these subsystems. When U contains inputs with known probability distributions, the POVM is additionally constrained, see Eqs. (34) and (35) for an example. In partially device-dependent applications, one may also trust the form of the specific measurements or the dimensions of the subsystems.

Finally we consider a special kind of map of quantum states and the corresponding closure property of models. We call a map $\mathcal{E}$ on $\mathcal{H}(\mathsf{E})$ a pure completely positive map (pCP map) if it is of the form $\mathcal{E}(\rho) = M\rho M^\dagger$ for some linear operator M on $\mathcal{H}(\mathsf{E})$. A pCP map $\mathcal{E}$ transforms a state $\rho_{U\mathsf{E}} \in \mathcal{S}(U\mathsf{E})$ according to

$$\mathcal{E}(\rho_{U\mathsf{E}}) = \sum_u |u\rangle\langle u| \otimes (M\rho_{\mathsf{E}}(u)M^\dagger).$$

The model $\mathcal{C}(U)$ is pCP-*closed* if for each pCP map $\mathcal{E}$ and each state $\rho_{U\mathsf{E}}$ in $\mathcal{C}(U)$ the resulting state $\mathcal{E}(\rho_{U\mathsf{E}})$ is still in $\mathcal{C}(U)$. The pCP-closure property is satisfied by the induced model $\mathcal{M}(\mathcal{P}_{\mathsf{D}}(U);\mathsf{E})$. To prove this pCP-closure property, it suffices to observe that by definitions, pCP maps on $\mathcal{H}(\mathsf{E})$ preserve $\mathcal{S}(\mathsf{E})$, and POVMs of D with outcome U commute with pCP maps on $\mathcal{H}(\mathsf{E})$. The pCP-closure property is useful for constructing QEFs, see Sec. VII B for details.

B. Models for input-conditional randomness generation

For randomness generation, the sequence of classical variables $\mathbf{U}$ in an experiment usually consists of both the inputs $\mathbf{Z}$ and outputs $\mathbf{C}$. In order to certify randomness in the outputs $\mathbf{C}$ conditional on the inputs $\mathbf{Z}$ as well as the quantum side information in E, we need to restrict the chained models such that at each trial i, information about the past outputs $\mathbf{C}_{<i}$ cannot be leaked through the input Z_i. For this we require that the input Z_i is independent of the past outputs $\mathbf{C}_{<i}$ given E and the past inputs $\mathbf{Z}_{<i}$. Because E is quantum, this is formulated by means of a short quantum Markov chain [42].

Specifically, models for input-conditional randomness generation can be constructed by inductively applying the chaining operation defined as follows. Let $\mathcal{C}(\mathbf{C}_{<i}\mathbf{Z}_{<i})$ be a model for $\mathbf{C}_{<i}\mathbf{Z}_{<i}\mathsf{E}$, $\mathcal{C}_{\mathbf{C}_{<i}\mathbf{Z}_{<i}}(C_iZ_i)$ be a family of models for $C_iZ_i\mathsf{E}$ consisting of all $\mathcal{C}_{\mathbf{c}_{<i}\mathbf{z}_{<i}}(C_iZ_i)$, and $\mathcal{C}(\mathbf{C}_{<i}\mathbf{Z}_{<i})\circ \mathcal{C}_{\mathbf{C}_{<i}\mathbf{Z}_{<i}}(C_iZ_i)$ be the standard chained model. The result of *chaining* $\mathcal{C}(\mathbf{C}_{<i}\mathbf{Z}_{<i})$ *and* $\mathcal{C}_{\mathbf{C}_{<i}\mathbf{Z}_{<i}}(C_iZ_i)$ *with conditionally independent inputs* is the model $\mathcal{C}(\mathbf{C}_{<i}\mathbf{Z}_{<i})\circ_{Z_i|\mathbf{Z}_{<i}}\mathcal{C}_{\mathbf{C}_{<i}\mathbf{Z}_{<i}}(C_iZ_i)$ consisting of the members $\rho_{\mathbf{C}_{\leqslant i}\mathbf{Z}_{\leqslant i}\mathsf{E}}$ such that $\rho_{\mathbf{C}_{\leqslant i}\mathbf{Z}_{\leqslant i}\mathsf{E}}$ is in the chained model $\mathcal{C}(\mathbf{C}_{<i}\mathbf{Z}_{<i})\circ\mathcal{C}_{\mathbf{C}_{<i}\mathbf{Z}_{<i}}(C_iZ_i)$ and $\rho_{\mathbf{C}_{<i}\mathbf{Z}_{\leqslant i}\mathsf{E}} = \mathrm{tr}_{C_i}(\rho_{\mathbf{C}_{\leqslant i}\mathbf{Z}_{\leqslant i}\mathsf{E}})$ is a short quantum Markov chain over $\mathbf{Z}_{<i}\mathsf{E}$ (see Appendix C for the definition of short quantum Markov chains).

In practice, the input Z_i at each trial i is treated as a *free* choice in the sense that Z_i is independent of other classical variables, the quantum devices used and the quantum system E. Given this independence, the model $\mathcal{C}(\mathbf{CZ})$ can be constructed by chaining the trial models $\mathcal{C}_{\mathbf{C}_{<1}\mathbf{Z}_{<1}}(C_1Z_1)$, $\mathcal{C}_{\mathbf{C}_{<2}\mathbf{Z}_{<2}}(C_2Z_2),\ldots,\mathcal{C}_{\mathbf{C}_{<n}\mathbf{Z}_{<n}}(C_nZ_n)$ with the standard chaining operation of Eq. (26). Independence ensures that each state $\rho_{\mathbf{CZE}}$ in the chained model $\mathcal{C}(\mathbf{CZ})$ satisfies the short quantum Markov-chain condition over $\mathbf{Z}_{<i}\mathsf{E}$ for each i. Indeed, the short quantum Markov-chain condition is satisfied if and only if at each trial i, the input Z_i is independent of the past outputs $\mathbf{C}_{<i}$ given E and the past inputs $\mathbf{Z}_{<i}$ [42].

Models constructed by chaining with conditionally independent inputs capture the standard experimental configurations for randomness generation with free setting choices, including both device-dependent and device-independent scenarios. We remark that there is no restriction on the dynamics of the devices between trials, nor is there any reason to explicitly represent this dynamics. The model keeps track only of the joint state of $\mathbf{CZ}\mathsf{E}$, and with the formulation of induced trial models, any quantum systems or quantum operations that the devices use over the course of the experiment are subsumed by the trial models and the chaining constructions.

VII. CONSTRUCTION OF QEFS

In this section, we first give an expression for the QEF inequality imposed by an arbitrary state (not necessarily normalized) in the model $\mathcal{C}(\mathbf{CZ})$. Then we discuss several properties of QEFs. Next we show that QEFs for models obtained by chaining with conditionally independent inputs can be constructed by multiplying QEFs for the individual trial models in the chain. QEFs for later trial models may depend on the results of earlier trials, so we refer to the construction of QEFs above as QEF chaining. Finally, we formulate the construction of trialwise QEFs as an optimization problem.

Let $\rho_{\mathbf{CZE}}$ be an arbitrary state in $\mathcal{C}(\mathbf{CZ})$. The QEF inequality with power β at $\rho_{\mathbf{CZE}}$ is given by

$$\sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \leqslant \mathrm{tr}(\rho_{\mathbf{CZE}}), \tag{27}$$

where $\rho_{\mathsf{E}}(\mathbf{cz})$ and $\rho_{\mathsf{E}}(\mathbf{z})$ are the un-normalized marginal states of E given the results $\mathbf{cz}$ and $\mathbf{z}$ according to $\rho_{\mathbf{CZE}}$. Both sides of the QEF inequality in Eq. (27) are positively homogeneous of degree 1 in $\rho_{\mathbf{CZE}}$. It follows that to show a function $F:\mathrm{Rng}(\mathbf{CZ})\to\mathbb{R}_{\geqslant 0}$ is a QEF for $\mathcal{C}(\mathbf{CZ})$, it is necessary and sufficient that the QEF inequality holds for normalized states in $\mathcal{N}(\mathcal{C}(\mathbf{CZ}))$. For normalized states, the QEF inequality becomes the inequality in Eq. (7). Similarly, we can define QEFs for each individual trial model. We remark that the QEF inequality in Eq. (27) is helpful for proving properties of QEFs as well as QEF chaining, while the QEF inequality in Eq. (7) is used for numerical constructions of QEFs.

A. Properties of QEFs

Here are a few useful properties of QEFs; their proofs are given in Appendix E.

Property 1. For all models $\mathcal{C}(\mathbf{CZ})$, the constant function $F(\mathbf{cz})=1$ for all $\mathbf{cz}\in\mathrm{Rng}(\mathbf{CZ})$ is a QEF with power β for each $\beta>0$.

Let $\mathrm{Cone}(\mathcal{C}(\mathbf{CZ}))$ be the convex cone generated by $\mathcal{C}(\mathbf{CZ})$. Then we have

Property 2. A function $F:\mathrm{Rng}(\mathbf{CZ})\to\mathbb{R}_{\geqslant 0}$ is a QEF with power β for $\mathcal{C}(\mathbf{CZ})$ if and only if the function is a QEF with power β for $\mathrm{Cone}(\mathcal{C}(\mathbf{CZ}))$.

According to property 2, if $\mathrm{Cone}(\mathcal{C}'(\mathbf{CZ}))\supseteq\mathcal{C}(\mathbf{CZ})$, then every QEF for $\mathcal{C}'(\mathbf{CZ})$ is a QEF for $\mathcal{C}(\mathbf{CZ})$. Thus a strategy for constructing QEF sis to find an easily characterized model $\mathcal{C}'(\mathbf{CZ})$ whose convex closure contains the model $\mathcal{C}(\mathbf{CZ})$ of interest.

Let $\mathcal{E}_{\mathbf{Z}}$ be an arbitrary family of $\mathbf{z}$-dependent completely positive and trace preserving (CPTP) maps $\mathcal{E}_{\mathbf{z}}$ on $\mathcal{H}(\mathsf{E})$. As an operation, $\mathcal{E}_{\mathbf{Z}}$ transforms a state $\rho_{\mathbf{CZE}}$ according to

$$\mathcal{E}_{\mathbf{Z}}(\rho_{\mathbf{CZE}}) = \sum_{\mathbf{cz}} |\mathbf{cz}\rangle\langle\mathbf{cz}|\otimes\mathcal{E}_{\mathbf{z}}(\rho_{\mathsf{E}}(\mathbf{cz})).$$

Define the model $\mathcal{E}_{\mathbf{Z}}(\mathcal{C}(\mathbf{CZ}))$ as

$$\mathcal{E}_{\mathbf{Z}}(\mathcal{C}(\mathbf{CZ})) = \{\mathcal{E}_{\mathbf{Z}}(\rho_{\mathbf{CZE}}) : \rho_{\mathbf{CZE}}\in\mathcal{C}(\mathbf{CZ})\}.$$

Then, another property is that

Property 3. A function $F:\mathrm{Rng}(\mathbf{CZ})\to\mathbb{R}_{\geqslant 0}$ is a QEF with power β for $\mathcal{E}_{\mathbf{Z}}(\mathcal{C}(\mathbf{CZ}))$ if the function is a QEF with power β for $\mathcal{C}(\mathbf{CZ})$.

Property 3 is useful for certifying randomness in the situation where the system E learns the input Z_i to the devices after each trial i. For this situation, we start with the model $\mathcal{C}(\mathbf{CZ})$ for $\mathbf{CZ}\mathsf{E}$ and construct the QEFs $F(\mathbf{CZ})$ for $\mathcal{C}(\mathbf{CZ})$ (see the next section for the construction details). After the experiment, as E learns the inputs $\mathbf{Z}$, the change of E can be modelled by a family $\mathcal{E}_{\mathbf{Z}}$ of $\mathbf{z}$-dependent CPTP maps $\mathcal{E}_{\mathbf{z}}$ on $\mathcal{H}(\mathsf{E})$. Therefore the model becomes $\mathcal{E}_{\mathbf{Z}}(\mathcal{C}(\mathbf{CZ}))$. According to property 3, the constructed QEFs are still valid for $\mathcal{E}_{\mathbf{Z}}(\mathcal{C}(\mathbf{CZ}))$.

For the next property, we define a function $K:\mathrm{Rng}(\mathbf{CZ})\to\mathbb{R}$ to be an entropy estimator for the model

$\mathcal{C}(\mathbf{CZ})$ if for all states $\rho_{\mathbf{CZE}}$ in the model,

$$\sum_{\mathbf{cz}} K(\mathbf{cz})\mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz})) \leqslant H_1(\mathbf{C}|\mathbf{ZE})_\rho, \tag{28}$$

where $H_1(\mathbf{C}|\mathbf{ZE})_\rho$ is the conditional von Neumann entropy (in binary logarithm) of $\mathbf{C}$ given $\mathbf{ZE}$ at $\rho_{\mathbf{CZE}}$. Every QEF yields an entropy estimator.

Property 4. Let $F(\mathbf{CZ})$ be a QEF with power β for $\mathcal{C}(\mathbf{CZ})$. Then $\log_2(F(\mathbf{CZ}))/\beta$ is an entropy estimator for $\mathcal{C}(\mathbf{CZ})$.

The affine min-tradeoff functions required for entropy accumulation [13,29] are closely related with the entropy estimators defined above. With our notation, an affine min-tradeoff function f for the model $\mathcal{C}(\mathbf{CZ})$ is a linear and real function of the probability distribution $\mu(\mathbf{CZ})$ such that $f(\mu(\mathbf{CZ})) \leqslant H_1(\mathbf{C}|\mathbf{ZE})_\rho$ for all normalized states $\rho_{\mathbf{CZE}}$ in $\mathcal{C}(\mathbf{CZ})$ which have the marginal $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathbf{CZE}}) = \mu(\mathbf{CZ})$. Since f is linear and real, we can write $f(\mu(\mathbf{CZ})) = \sum_{\mathbf{cz}} a_{\mathbf{cz}}\mu(\mathbf{cz}) + a_0 = \sum_{\mathbf{cz}}(a_{\mathbf{cz}} + a_0)\mu(\mathbf{cz})$ with real numbers $a_{\mathbf{cz}}$ and a_0, so $f(\mu(\mathbf{CZ})) = \mathbb{E}_\mu(K(\mathbf{CZ}))$ where $K(\mathbf{CZ}) : \mathbf{cz} \mapsto a_{\mathbf{cz}} + a_0$ is an entropy estimator. According to property 4, affine min-tradeoff functions can be derived from QEFs. It is an interesting problem to see whether the affine min-tradeoff functions derived from QEFs can improve on the ones previously obtained [13] for entropy accumulation.

Besides the above four properties, there are two additional properties satisfied by QEFs:

Property 5. Let $F(\mathbf{CZ})$ be a QEF with power β for $\mathcal{C}(\mathbf{CZ})$. Then for all $\beta' \geqslant \beta$, $F(\mathbf{CZ})$ is a QEF with power β' for $\mathcal{C}(\mathbf{CZ})$.

Property 6. Let $F(\mathbf{CZ})$ be a QEF with power β for $\mathcal{C}(\mathbf{CZ})$. Then for $0 < \gamma \leqslant 1$, $F(\mathbf{CZ})^\gamma$ is a QEF with power $\gamma\beta$ for $\mathcal{C}(\mathbf{CZ})$.

Property 5 is useful for studying the finite-data performance of QEFs, while property 6 helps to study the asymptotic behavior of randomness generation according to QEFs, see Sec. VII C for more discussions.

B. QEF chaining

Consider an arbitrary trial indexed by i. For past results $\mathbf{c}_{<i}\mathbf{z}_{<i}$, let $\mathcal{C}_{\mathbf{c}_{<i}\mathbf{z}_{<i}}(C_iZ_i)$ be a trial model for $C_iZ_i\mathsf{E}$ which can depend on the past. Suppose that the trial model $\mathcal{C}_{\mathbf{c}_{<i}\mathbf{z}_{<i}}(C_iZ_i)$ is pCP-closed. Let $\mathcal{C}_{\mathbf{C}_{<i}\mathbf{Z}_{<i}}(C_iZ_i)$ be a family of such trial models consisting of all $\mathcal{C}_{\mathbf{c}_{<i}\mathbf{z}_{<i}}(C_iZ_i)$. Suppose that for each trial model $\mathcal{C}_{\mathbf{c}_{<i}\mathbf{z}_{<i}}(C_iZ_i)$, we are able to construct the QEF $F_{\mathbf{c}_{<i}\mathbf{z}_{<i}}(C_iZ_i)$, where the subscript of the QEF indicates that its construction can depend on the past results $\mathbf{c}_{<i}\mathbf{z}_{<i}$. Let $F_{\mathbf{C}_{<i}\mathbf{Z}_{<i}}(C_iZ_i)$ be a family of trialwise QEFs consisting of all $F_{\mathbf{c}_{<i}\mathbf{z}_{<i}}(C_iZ_i)$. If the model $\mathcal{C}(\mathbf{CZ})$ is obtained by chaining the trial models $\mathcal{C}_{\mathbf{C}_{<1}\mathbf{Z}_{<1}}(C_1Z_1), \mathcal{C}_{\mathbf{C}_{<2}\mathbf{Z}_{<2}}(C_2Z_2), \ldots, \mathcal{C}_{\mathbf{C}_{<n}\mathbf{Z}_{<n}}(C_nZ_n)$ with conditionally independent inputs, then the QEFs $F(\mathbf{CZ})$ for $\mathcal{C}(\mathbf{CZ})$ can be constructed by multiplying or chaining the trialwise QEFs $F_{\mathbf{C}_{<i}\mathbf{Z}_{<i}}(C_iZ_i)$, $i = 1, 2, \ldots, n$. This construction follows from the next theorem by induction. To simplify the notation in the next theorem, we consider a generic trial with input Z and output C, and we denote the past inputs and outputs by $\mathbf{Z}$ and $\mathbf{C}$.

Theorem 5. Let $\mathcal{C}(\mathbf{CZ})$ be a model for $\mathbf{CZE}$ and for each $\mathbf{cz}$, let $\mathcal{C}_{\mathbf{cz}}(CZ)$ be a pCP-closed model for $CZ\mathsf{E}$. If $G(\mathbf{CZ})$ is a QEF with power β for $\mathcal{C}(\mathbf{CZ})$, and for each $\mathbf{cz}$, $F_{\mathbf{cz}}(CZ)$ is a QEF with power β for $\mathcal{C}_{\mathbf{cz}}(CZ)$, then the function $G \diamond F : \mathrm{Rng}(\mathbf{CZ}) \times \mathrm{Rng}(CZ) \to \mathbb{R}_{\geqslant 0}$ defined as $G \diamond F(\mathbf{cz}cz) = G(\mathbf{cz})F_{\mathbf{cz}}(cz)$ for all $\mathbf{cz} \in \mathrm{Rng}(\mathbf{CZ})$ and $cz \in \mathrm{Rng}(CZ)$ is a QEF with power β for the chained model $\mathcal{C}(\mathbf{CZ}) \circ_{Z|\mathbf{Z}} \mathcal{C}_{\mathbf{CZ}}(CZ)$ with conditionally independent inputs.

The proof of theorem 5 can be found in Appendix D.

In practice, each $\mathcal{C}_{\mathbf{cz}}(CZ)$ is a trial model induced by a family of POVMs. Thus the pCP-closure property required in theorem 5 is satisfied. Moreover, in standard situations for randomness generation, the input Z at a trial is a free choice. So, the model chaining with conditionally independent inputs required in theorem 5 is also satisfied. Accordingly, we can construct QEFs for a sequence of trials by chaining trialwise QEFs.

An advantage of QEF chaining is that trialwise QEFs can be adapted while the trials are acquired. Specifically, let k be the number of trials performed (or analyzed) so far. According to QEF chaining, the next trial's QEF $F_{k+1}(C_{k+1}Z_{k+1}) \equiv F_{\mathbf{C}_{\leqslant k}\mathbf{Z}_{\leqslant k}}(C_{k+1}Z_{k+1})$ can depend arbitrarily on the past results $\mathbf{C}_{\leqslant k}\mathbf{Z}_{\leqslant k}$. In particular, one can check the statistics of recent trials to infer whether the probability distribution of trial results has changed and if so, adapt the construction of the next trial's QEF accordingly.

A consequence of the above adaptive construction of trialwise QEFs is that one can stop acquiring trials as soon as the chained QEF takes a value larger than or equal to the threshold $f_{\min}$ in protocol 1. Specifically, if the value of the chained QEF so far, $\prod_{i=1}^k F_i(c_iz_i)$ with $k < n$, already exceeds the threshold $f_{\min}$, then one can set all future QEFs $F_i(C_iZ_i)$, where $i = k+1, \ldots, n$, to be the constant 1, which is a valid QEF according to property 1. Since this eliminates any contribution from future trials to the final chained QEF value, it is not necessary to perform the future trials at this point. Instead, we pad the trial outputs $\mathbf{c}_{\leqslant k}$ observed so far with zeros in order to run randomness extraction according to protocol 1, as the protocol requires a fixed number n of trials determined before the experiment. This ability of early stopping is exploited in our companion experimental work [43].

C. QEF optimization

Let $F_i(C_iZ_i)$ be a QEF with power β for the i'th trial in an experiment. According to QEF chaining, the product $\prod_{i=1}^n F_i(C_iZ_i)$ is a QEF with power β for the whole experiment consisting of n trials. A construction of good trialwise QEFs can be derived as follows. The experiment successfully implements protocol 1 if the chained QEF satisfies the condition $\prod_{i=1}^n F_i(C_iZ_i) \geqslant f_{\min} = 1/(p^\beta(\epsilon_h^2/2))$, or equivalently,

$$\sum_{i=1}^n \log_2(F_i(C_iZ_i))/\beta + \log_2\left(\epsilon_h^2/2\right)/\beta \geqslant -\log_2(p). \tag{29}$$

Hence, we aim to obtain a large expected value of the left-hand side of the above equation with as few trials as possible. For this purpose, *before* the experiment we can choose values for p and ϵ_h (see protocol 1) and optimize over the trialwise QEFs and the power β such that the number of trials required for success, n_{exp}, is minimized. Then we fix the number of trials n in the experiment to be a number larger than the minimum number of trials, so that the actual experiment

succeeds with high probability if the quantum devices used are honest. Moreover, during the experiment we have the freedom to adapt the QEF $F_i(C_iZ_i)$ *before* the ith trial where p, ϵ_h, β and n are already fixed. All these optimizations are based on the construction of trialwise QEFs given fixed β and other parameters. This construction is detailed in the next paragraph.

Consider a generic next trial with results CZ and model $\mathcal{C}(CZ)$. Based on prior calibrations or the frequencies of observed results in past trials, we can determine a distribution $\nu(CZ) \in \mathcal{N}(\mathcal{C}_{\rm cl}(CZ)) \doteq {\rm tr}_{\mathsf{E}}(\mathcal{N}(\mathcal{C}(CZ)))$ that is (hopefully) a good approximation to the distribution of the next trial's results. If each trial has the same distribution $\nu(CZ)$ and each trial model is the identical $\mathcal{C}(CZ)$, then after n trials the left-hand side of Eq. (29) is expected to be $\mathbb{E}_\nu(n\log_2(F(CZ))/\beta + \log_2(\epsilon_h^2/2)/\beta)$. Here, $F(CZ)$ is a QEF with power β for $\mathcal{C}(CZ)$ and we use the same trialwise QEF for each trial. Thus one way to optimize QEFs *before* the next trial is as follows:

$$\begin{aligned} &\text{Max:}\mathbb{E}_\nu\left(n\log_2(F(CZ))/\beta + \log_2\left(\epsilon_h^2/2\right)/\beta\right) \\ &\text{Subject to } (1) F(cz) \geqslant 0, \text{ for all } cz, \\ &\qquad (2)\sum_{cz} F(cz)\mathcal{R}_\alpha(\rho_{\mathsf{E}}(cz)|\rho_{\mathsf{E}}(z)) \leqslant 1, \\ &\qquad \text{for all } \rho_{CZ\mathsf{E}} \in \mathcal{N}(\mathcal{C}(CZ)). \end{aligned} \tag{30}$$

The objective function is strictly concave and the constraints are linear, so there is a unique maximum. More details on QEF optimization in the CHSH Bell-test configuration are available in the next section. We emphasize that the trialwise QEF returned by the above optimization problem is optimal only when the trial results are i.i.d. with distribution $\nu(CZ)$ and with the identical trial model $\mathcal{C}(CZ)$, but it is always valid by definition regardless of the actual distribution of the next trial's results as long as the trial model is $\mathcal{C}(CZ)$.

Before the experiment, we also would like to minimize the number of trials $n_{\rm exp}$ required for the experiment to succeed. For this, we consider an equivalent task for randomness beacons—certifying a fixed number, b, of bits of quantum ϵ_h-smooth conditional min-entropy with as few trials as possible, where the distribution of each trial's results is the same $\nu(CZ) \in \mathcal{N}(\mathcal{C}_{\rm cl}(CZ))$ with the identical trial model $\mathcal{C}(CZ)$. For this task, we assume that the actual probability of success is larger than or equal to a positive κ' fixed beforehand. We informally justify this assumption below. Good reference values for randomness beacons are $b = 512$ and $\epsilon_h = \kappa' = 2^{-64}$. A tight lower bound on the number of trials required for satisfying the above randomness-beacon task is denoted as $n_{{\rm QEF},b}$, which depends on ϵ_h and κ' implicitly. An expression for $n_{{\rm QEF},b}$ is derived in the next paragraph.

In view of theorem 3 and Eq. (29), if the actual probability of success is larger than or equal to κ', then conditional on success the amount of quantum ϵ_h-smooth conditional min-entropy certified after n trials is

$$\log_2(f_{\rm min})/\beta + \log_2\left(\epsilon_h^2/2\right)/\beta + \alpha\log_2(\kappa')/\beta. \tag{31}$$

Success requires that $\sum_{i=1}^n \log_2(F_i(C_iZ_i)) \geqslant \log_2(f_{\rm min})$. Define the quantity

$$g(\beta) = \sup_F \mathbb{E}_\nu(\log_2(F(CZ))/\beta), \tag{32}$$

where the supremum is over trialwise QEFs $F(CZ)$ with power β for $\mathcal{C}(CZ)$. Since each trial has the same distribution $\nu(CZ)$ and each trial model is the identical $\mathcal{C}(CZ)$, we can set all trialwise QEFs F_i, $i = 1, 2, \ldots, n$, with power β to be the same QEF F that witnesses the value $g(\beta)$ defined in Eq. (32). So, the expectation of $\sum_{i=1}^n \log_2(F_i(C_iZ_i))/\beta$ is $ng(\beta)$. For adequate probability of success, we therefore need $\log_2(f_{\rm min})/\beta$ smaller than $ng(\beta)$ by an amount that is asymptotically small compared to $ng(\beta)$. For the present analysis, we simply set $\log_2(f_{\rm min})/\beta = ng(\beta)$ to determine a number of trials, n_b, required for certifying b bits of quantum ϵ_h-smooth conditional min-entropy according to

$$n_b g(\beta) + \log_2\left(\epsilon_h^2/2\right)/\beta + \alpha\log_2(\kappa')/\beta \geqslant b,$$

or equivalently,

$$n_b \geqslant \frac{b\beta - \log_2\left(\epsilon_h^2/2\right) - \alpha\log_2(\kappa')}{\beta g(\beta)}.$$

Minimizing the right-hand side over all possible trialwise QEFs gives a lower bound on the number of trials required, which is given as

$$n_{{\rm QEF},b} = \inf_\beta \frac{b\beta - \log_2\left(\epsilon_h^2/2\right) - \alpha\log_2(\kappa')}{\beta g(\beta)}. \tag{33}$$

The lower bound $n_{{\rm QEF},b}$ may be considered tight to lowest order in the sense that one needs only to increase the number of trials used in practice by an amount that is asymptotically small compared to $n_{{\rm QEF},b}$, in order to guarantee sufficient probability of success. Here, the probability of success can be estimated according to the distribution of a sum of i.i.d. random variables associated with the logarithm of the trialwise QEF used.

Since $b \geqslant 0$ and $\kappa' \leqslant 1$, Eq. (33) shows that the number of trials must exceed the minimum of $-\log_2(\epsilon_h^2/2)/(\beta g(\beta))$ before randomness can be certified, which suggests that the maximum of $\beta g(\beta)$ is a good indicator of finite-data performance. From property 5 one can see that the maximum of $\beta g(\beta)$ is achieved in the limit where β goes to infinity. The finite-data performance of QEFs is illustrated in Sec. VIII B.

We remark that for each fixed β, the quantity $g(\beta)$ defined in Eq. (32) can be identified as the maximum asymptotic entropy rate at constant ϵ_h and κ' witnessed by trialwise QEFs with power β when each trial has the same distribution $\nu(CZ)$ and each trial model is the identical $\mathcal{C}(CZ)$. We skip the justification and refer to Sec. 5.4 of Ref. [44] for details. The maximum asymptotic entropy rate witnessed by all possible trialwise QEFs for $\mathcal{C}(CZ)$ is $g_0 = \sup_{\beta>0} g(\beta)$. From property 6 one can see that the rate $g(\beta)$ is nonincreasing in β. Thus g_0 is determined by the limit as β goes to zero. In fact, g_0 can be proven to be equal to the worst-case conditional von Neumann entropy $H_1(C|Z\mathsf{E})$ over all states $\rho_{CZ\mathsf{E}}$ allowed by the trial model $\mathcal{C}(CZ)$ such that ${\rm tr}_{\mathsf{E}}(\rho_{CZ\mathsf{E}}) = \nu(CZ)$, see Sec. 6.5 of Ref. [44]. Since this worst-case conditional von Neumann entropy is a tight upper bound on the asymptotic randomness rate [45], quantum probability estimation is asymptotically optimal and we identify g_0 as the asymptotic randomness rate achieved by quantum probability estimation at constant ϵ_h and κ'.

VIII. QEFS FOR THE CHSH BELL-TEST CONFIGURATION

We consider DIRG with the experimentally relevant two-party, two-setting, two-outcome Bell-test configuration, referred to as the CHSH configuration [31]. The parties are labeled A and B. The quantum system D of the devices can be decomposed into two subsystems $\mathsf{D_A}$ and $\mathsf{D_B}$ held by A and B respectively. In each trial, a source (which could be under control of E) prepares a state ρ_{DE} shared between D and E, and the party A (B) randomly chooses a setting X (Y) and obtains a measurement outcome A (B). We write $Z = XY$ for the inputs of the trial, and $C = AB$ for the outputs of the trial. For the CHSH configuration, $A, B, X, Y \in \{0, 1\}$.

The trial model for $ABXY\mathsf{E}$ is induced by a family of input-dependent POVMs of D with free inputs XY. In an experiment, the input distribution $\mu(XY)$ is usually not exactly known, but it is reasonable to assume that the inputs XY are free choices, independent of other classical variables and the quantum systems D, E. Denote the classical model for the inputs XY by $\mathcal{C}_{\rm cl}(XY)$. In most cases the normalized classical model $\mathcal{N}(\mathcal{C}_{\rm cl}(XY))$ is a convex polytope. We assume that the input distribution $\mu(XY) \in \mathcal{N}(\mathcal{C}_{\rm cl}(XY))$. Denote the family of input-dependent POVMs of D by $\mathcal{P}_{\mathsf{D},XY}(AB)$. Each POVM in $\mathcal{P}_{\mathsf{D},XY}(AB)$ has a tensor-product structure over the two subsystems $\mathsf{D_A}$ and $\mathsf{D_B}$. Furthermore, according to the nonsignaling conditions [32,33] the output of A (or B) is independent of the input of B (or A). Therefore, for arbitrary inputs xy and outputs ab the POVM element $P_{\mathsf{D},xy}(ab)$ is of the form $P_{\mathsf{D_A},x}(a) \otimes P_{\mathsf{D_B},y}(b)$, where $P_{\mathsf{D_A},x}(A)$ and $P_{\mathsf{D_B},y}(B)$ are POVMs of $\mathsf{D_A}$ and $\mathsf{D_B}$ respectively.

Given the inputs xy, the induced model for $AB\mathsf{E}$ is

$$\mathcal{M}(\mathcal{P}_{\mathsf{D},xy}(AB);\mathsf{E}) = \left\{ \sum_{ab} |ab\rangle\langle ab| \otimes \mathrm{tr}_{\mathsf{D}}\big(\rho_{\mathsf{DE}}(P_{\mathsf{D_A},x}(a) \otimes P_{\mathsf{D_B},y}(b) \otimes \mathbb{1}_{\mathsf{E}})\big) : \rho_{\mathsf{DE}} \in \mathcal{S}(\mathsf{DE}), P_{\mathsf{D_A},x}(A) \otimes P_{\mathsf{D_B},y}(B) \in \mathcal{P}_{\mathsf{D},xy}(AB) \right\}. \quad (34)$$

If the inputs XY are free with distribution $\mu(XY) \in \mathcal{N}(\mathcal{C}_{\rm cl}(XY))$ and for each xy the induced model for $AB\mathsf{E}$ is $\mathcal{M}(\mathcal{P}_{\mathsf{D},xy}(AB);\mathsf{E})$, then the trial model for $ABXY\mathsf{E}$ is given by

$$\mathcal{C}_{222}(ABXY) = \left\{ \sum_{xy} \mu(xy)|xy\rangle\langle xy| \otimes \rho_{AB\mathsf{E}|xy} : \mu(XY) \in \mathcal{N}(\mathcal{C}_{\rm cl}(XY)), \text{ and for each } xy,\ \rho_{AB\mathsf{E}|xy} \in \mathcal{M}(\mathcal{P}_{\mathsf{D},xy}(AB);\mathsf{E}) \right\}. \quad (35)$$

We emphasize that in the CHSH Bell-test configuration each trial model is the identical $\mathcal{C}_{222}(ABXY)$, even if the results obtained from a sequence of time-ordered trials are not i.i.d. and even if the distribution of free inputs $\mu(XY)$ is not exactly known as long as $\mu(XY) \in \mathcal{N}(\mathcal{C}_{\rm cl}(XY))$.

In Sec. VIII A, we simplify both the characterization of the model $\mathcal{C}_{222}(ABXY)$ and the corresponding construction of QEFs for certifying randomness against quantum side information. Then we demonstrate the finite-data performance of QEFs in Sec. VIII B.

A. Simple characterization of $\mathcal{C}_{222}(ABXY)$

In the device-independent scenario, the dimension of each quantum system D or E can take an arbitrarily large but finite value. By the usual dilation argument, we can consider only projective measurements $P_{\mathsf{D_A},x}(A)$ and $P_{\mathsf{D_B},y}(B)$ in Eq. (34). For the CHSH Bell-test configuration, we can further simplify the characterization of the models $\mathcal{M}(\mathcal{P}_{\mathsf{D},xy}(AB);\mathsf{E})$ for all xy according to the next theorem. For this, we need the rank-1 projectors on a qubit defined by

$$Q_{0;\theta}(s) = \tfrac{1}{2}(\mathbb{1} + (-1)^s\sigma_z),$$
$$Q_{1;\theta}(s) = \tfrac{1}{2}(\mathbb{1} + (-1)^s(\cos(\theta)\sigma_z + \sin(\theta)\sigma_x)), \quad (36)$$

where $s \in \{0, 1\}$, $\theta \in (-\pi, \pi]$, and σ_z and σ_x are two of the Pauli matrices, corresponding to the observables along the z and x axes of the Bloch sphere. Note that each of the sets $\{Q_{0;\theta}(s), s = 0, 1\}$ and $\{Q_{1;\theta}(s), s = 0, 1\}$ is a POVM on a qubit, where the values 0 or 1 in the subscript of Q indicate the corresponding setting choices. The Hilbert space of a qubit is denoted by $\mathbb{C}^2$.

Theorem 6. For each value xy of the trial inputs, the induced model $\mathcal{M}(\mathcal{P}_{\mathsf{D},xy}(AB);\mathsf{E})$ consists of positive combinations of states $\rho_{AB\mathsf{E}|xy}$ expressible in the form

$$\rho_{AB\mathsf{E}|xy} = \sum_{ab} |ab\rangle\langle ab| \otimes (U\tau^{1/2}\Pi_{ab|xy}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}})\tau^{1/2}U^\dagger), \quad (37)$$

where $\tau \in \mathbb{C}^2 \otimes \mathbb{C}^2$ is a positive semidefinite operator, $\Pi_{ab|xy}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}) = Q_{x;\theta_{\mathsf{A}}}(a) \otimes Q_{y;\theta_{\mathsf{B}}}(b) \in \mathbb{C}^2 \otimes \mathbb{C}^2$ is a rank-1 projector with $\theta_{\mathsf{A}}, \theta_{\mathsf{B}} \in (-\pi, \pi]$, and U is an isometry from $\mathbb{C}^2 \otimes \mathbb{C}^2$ to $\mathcal{H}(\mathsf{E})$.

We remark that both τ and U are independent of the inputs xy and outputs ab. Unless it is necessary to emphasize the projector $\Pi_{ab|xy}$ as a function of θ_{A} and θ_{B}, below we abbreviate it as $\Pi_{ab|xy}$. The theorem follows from a well-known analysis going back to Ref. [46] and even earlier Ref. [47]; a nice version of this analysis is in Sec. 2.4.1 of Ref. [48]. A detailed proof is given in Appendix F.

Theorem 6 provides a computationally accessible construction of QEFs for the model $\mathcal{C}_{222}(ABXY)$ as explained in the next few paragraphs. Consider the case that the normalized classical model $\mathcal{N}(\mathcal{C}_{\rm cl}(XY))$ for the inputs XY is a convex polytope with a finite number of extremal distributions $\mu_k(XY)$, $k = 1, 2, \ldots, K$. In the experimental demonstration of DIRG reported in our companion work [43], $K = 4$. Let $\rho_{ABXY\mathsf{E}} \in \mathcal{N}(\mathcal{C}_{222}(ABXY))$ be a normalized state. In view of theorem 6 and the fact that $\mathcal{N}(\mathcal{C}_{\rm cl}(XY))$ is a convex polytope with K extreme points, the state $\rho_{ABXY\mathsf{E}}$ can be written as a convex combination of normalized states

$$\rho^{(k)}_{ABXY\mathsf{E}} = \sum_{xy} \mu_k(xy)|xy\rangle\langle xy| \otimes \rho_{AB\mathsf{E}|xy}, \quad k = 1, 2, \ldots, K, \quad (38)$$

where each $\rho_{AB\mathsf{E}|xy}$ has the form of Eq. (37). Therefore by property 2, the QEF inequality with power β for $F(ABXY)$ at $\rho_{ABXY\mathsf{E}}$ is implied by the set of QEF inequalities with power

β at $\rho^{(k)}_{ABXY\mathsf{E}}$, $k = 1, 2, \ldots, K$. We also note that since the state $\rho^{(k)}_{ABXY\mathsf{E}}$ is normalized and $\sum_{xy} \mu_k(xy) = 1$, the operator τ in Eq. (37) satisfies $\mathrm{tr}(\tau) = 1$, that is, τ is a normalized state in $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Direct calculation shows that the QEF inequality with power β for $F(ABXY)$ at $\rho^{(k)}_{ABXY\mathsf{E}}$ is

$$\sum_{abxy} F(abxy)\mu_k(xy)\mathrm{tr}((\tau^{1/(2\alpha)}\Pi_{ab|xy}\tau^{1/(2\alpha)})^\alpha) \leqslant 1. \quad (39)$$

As $\Pi_{ab|xy}$ is a rank-1 projector,

$$\mathrm{tr}((\tau^{1/(2\alpha)}\Pi_{ab|xy}\tau^{1/(2\alpha)})^\alpha) = (\mathrm{tr}(\tau^{1/(2\alpha)}\Pi_{ab|xy}\tau^{1/(2\alpha)}))^\alpha.$$

Further, considering the invariance of the trace under cyclic permutations, the QEF inequality in Eq. (39) simplifies to

$$\sum_{abxy} F(abxy)\mu_k(xy)(\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}))^\alpha \leqslant 1. \quad (40)$$

Therefore, to verify that a function $F : \mathrm{Rng}(ABXY) \to \mathbb{R}_{\geqslant 0}$ is a QEF with power β for $\mathcal{C}_{222}(ABXY)$, it is necessary and sufficient to check that the QEF inequality in Eq. (40) holds for all $\theta_\mathsf{A}, \theta_\mathsf{B} \in (-\pi, \pi]$, $\tau \geqslant 0$ with $\mathrm{tr}(\tau) = 1$, and μ_k with $k = 1, 2, \ldots, K$.

Given an arbitrary non-negative function $F' : \mathrm{Rng}(ABXY) \to \mathbb{R}_{\geqslant 0}$ and a power $\beta > 0$, define

$$W_{F',\alpha,k}(\theta_\mathsf{A}, \theta_\mathsf{B}, \tau) = \sum_{abxy} F'(abxy)\mu_k(xy)(\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}))^\alpha \quad (41)$$

for each extremal distribution μ_k. Then for each k we can formulate the following optimization problem

$$\begin{aligned} f_k \doteq \text{Max: } & W_{F',\alpha,k}(\theta_\mathsf{A}, \theta_\mathsf{B}, \tau) \\ \text{Subject to: } & \tau \geqslant 0 \text{ and } \mathrm{tr}(\tau) = 1, \\ & -\pi < \theta_\mathsf{A}, \theta_\mathsf{B} \leqslant \pi. \end{aligned} \quad (42)$$

Once the above optimization problems are solved, we can set $f_{\max} = \max\{f_k : k = 1, 2, \ldots, K\}$. Then the function $F : \mathrm{Rng}(ABXY) \to \mathbb{R}_{\geqslant 0}$ defined as $F(abxy) = F'(abxy)/f_{\max}$ for all $abxy \in \mathrm{Rng}(ABXY)$ is a valid QEF with power β for the model $\mathcal{C}_{222}(ABXY)$, since it satisfies the QEF inequality in Eq. (40).

Given a method to determine f_k, any generic local search method can be used to find the best QEF for solving the convex-optimization problem in Eq. (30). So, in this work, we focus on methods for determining f_k. We provide a numerical method for determining both a lower and an upper bound on f_k as detailed in Appendix G. Below we refer to the optimization problem in Eq. (42) as QEF verification, since from the solution f_k a valid QEF can be constructed. We emphasize that the method presented in Appendix G works with arbitrary non-negative functions $F' : \mathrm{Rng}(ABXY) \to \mathbb{R}_{\geqslant 0}$. In the following section, we derive QEFs by this method from PEFs, because not only are effective methods for constructing PEFs available but also PEFs exhibit unsurpassed finite-data efficiency [25,26]. Recall that QEFs and PEFs address quantum and classical side information, respectively. Hence, by QEF verification we can upgrade the security analysis with respect to classical side information to that with respect to quantum side information.

B. Finite-data performance of QEFs

In this section, we compare quantum probability estimation with entropy accumulation [13,29] on their finite-data performances. We also reanalyze the data from the first experimental demonstration of certified randomness for DIRG [3] to enhance its security against quantum side information.

It is best to construct optimal QEFs by solving the optimization problem in Eq. (30) directly. However, an effective algorithm for finding optimal QEFs has not yet been well developed. Instead, here we construct valid QEFs. Such a QEF can be obtained with the following steps. We first construct an optimal PEF $F'(ABXY)$ with power β as in our previous works [25,26]. Then, given $F'(ABXY)$ and $\alpha = 1 + \beta$, we determine both an upper and a lower bounds on $f_{\max}$ [as introduced below Eq. (42)] with the method in Appendix G. We denote the lower and upper bounds obtained by $f_{\max,\mathrm{lb}}$ and $f_{\max,\mathrm{ub}}$, respectively. Finally, we obtain a valid QEF $F(ABXY)$ with power β by dividing the PEF by the upper bound $f_{\max,\mathrm{ub}}$, that is, $F(abxy) = F'(abxy)/f_{\max,\mathrm{ub}}$ for all $abxy$. We emphasize that the QEFs derived from PEFs perform well as demonstrated below, however, they are not optimal in terms of the asymptotic randomness rate or finite-data efficiency exhibited. If numerically effective methods for solving the QEF optimization problem in Eq. (30) are available, we can improve the asymptotic randomness rate and finite-data efficiency in the presence of quantum side information.

In our study, we assume that the inputs XY at each trial are free with the uniform distribution. So the trial model of interest is $\mathcal{C}_{222}(ABXY)$ as specified in Eq. (35) but under the restriction that the input distribution is uniform. To construct PEFs, we consider the classical trial model $\mathcal{T}(ABXY)$ of distributions of $ABXY$ with uniformly random inputs, satisfying both nonsignaling conditions [32] and Tsirelson's bounds [49]. The optimization over PEFs with a fixed power β for $\mathcal{T}(ABXY)$ is a convex-optimization problem, see Sec. VIII of Ref. [25] for details. For each optimal PEF used, we found that both $f_{\max,\mathrm{lb}}$ and $f_{\max,\mathrm{ub}}$ are indistinguishable from 1 at high precision. Therefore the constructed QEF for the trial model $\mathcal{C}_{222}(ABXY)$ with uniformly random inputs is well-performing in the sense that it performs as well as the optimal PEF used for the classical trial model $\mathcal{T}(ABXY)$. We emphasize that when the input distribution is close to uniform, the QEF derived from a PEF performs as well as the original PEF as demonstrated below and in our companion work [43]. However, when the input distribution is far away from uniform (for example, when the total-variation distance between the input and uniform distributions is larger than 0.7) and when the power β is small enough (for example, when β is smaller than 10^{-7}), we observed that the certified upper bound $f_{\max,\mathrm{ub}}$ could be larger than 1 by a non-negligible amount such that the QEF derived from a PEF does not perform as well as the original PEF.

We first compare the minimum numbers of trials required by quantum probability estimation and by entropy accumulation [13,29] to ensure that the quantum ϵ_h-smooth conditional min-entropy estimate is positive, under the assumption that

the trial results are i.i.d. with distribution ν. We note that like our method, entropy accumulation works without the i.i.d. assumption, but the finite-data performance of each method depends on the actual distribution of each trial's results. With quantum probability estimation, the minimum number of trials required is denoted by $n_{\mathrm{QEF},b=0}$, where the expression for $n_{\mathrm{QEF},b}$ is given in Eq. (33). With entropy accumulation (EAT) as implemented in Ref. [13], the minimum number of trials required is denoted by $n_{\mathrm{EAT},b=0}$. An explicit expression for $n_{\mathrm{EAT},b}$ is given in Eq. (S34)[2] of our previous work [26]. Like $n_{\mathrm{QEF},b}$, the expression for $n_{\mathrm{EAT},b}$ is associated with moderate completeness depending on the distribution of a sum of i.i.d. random variables as discussed in Sec. VII C.

To determine the number $n_{\mathrm{QEF},b=0}$, we need to solve a minimization over all QEFs $F(ABXY)$ with power $\beta > 0$, given the distribution ν of trial results, the smoothness error ϵ_h, and a presumed lower bound κ' on the success probability that we need to protect against [see Eq. (33)]. Denote the objective function to be minimized by $m_{\mathrm{QEF},b=0}(F, \beta; \nu, \epsilon_h, \kappa')$. Then, $n_{\mathrm{QEF},b=0} = \min_{F,\beta} m_{\mathrm{QEF},b=0}(F, \beta; \nu, \epsilon_h, \kappa')$. Since numerical methods for QEF verification but not for QEF optimization are available, we determine an upper bound on $n_{\mathrm{QEF},b=0}$ instead. For this, we first minimize the expression for $m_{\mathrm{QEF},b=0}(F', \beta; \nu, \epsilon_h, \kappa')$ over PEFs $F'(ABXY)$ with $\beta > 0$ by the numerical method developed in Ref. [25]. Suppose that the minimum is witnessed by the PEF $F'_s(ABXY)$ with the power β_s. Next we obtain both an upper bound $f_{\max,\mathrm{ub}}$ and a lower bound $f_{\max,\mathrm{lb}}$ on $f_{\max}$ for $F'_s(ABXY)$ according to the method in Appendix G. So, the function F_s : $\mathrm{Rng}(ABXY) \to \mathbb{R}_{\geqslant 0}$ defined as $F_s(abxy) = F'_s(abxy)/f_{\max,\mathrm{ub}}$ for all $abxy \in \mathrm{Rng}(ABXY)$ is a valid QEF with the power β_s. Then we can determine an upper bound $n'_{\mathrm{QEF},b=0} \doteq m_{\mathrm{QEF},b=0}(F_s, \beta_s; \nu, \epsilon_h, \kappa')$ on the number $n_{\mathrm{QEF},b=0}$.

For specific comparisons, we need to fix the distribution ν and the smoothness error ϵ_h, as well as the presumed lower bound κ' on the success probability. We choose $\epsilon_h = \kappa' = 10^{-6}$. The quantum smooth conditional min-entropy estimate by either quantum probability estimation or entropy accumulation depends on ϵ_h and κ' in similar ways, so we expect our choice of ϵ_h and κ' to be representative. We emphasize that the amount of quantum ϵ_h-smooth conditional min-entropy certified by either method (before randomness extraction) depends on κ'; however, in an end-to-end randomness-generation protocol it is not necessary to specify a value of κ' for a soundness statement (see our protocol 1 and its soundness proof of theorem 4, for example). For the distribution ν of trial results $ABXY$, we consider the following three families as in our previous work [26] for certifying randomness against classical side information:

(1) $\mathcal{P}_{\mathrm{E}} = \{\nu_{\mathrm{E},\theta}\}_{0<\theta\leqslant\pi/4}$, where A and B share the unbalanced Bell state $|\Psi_\theta\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle$ with $\theta \in (0, \pi/4]$.

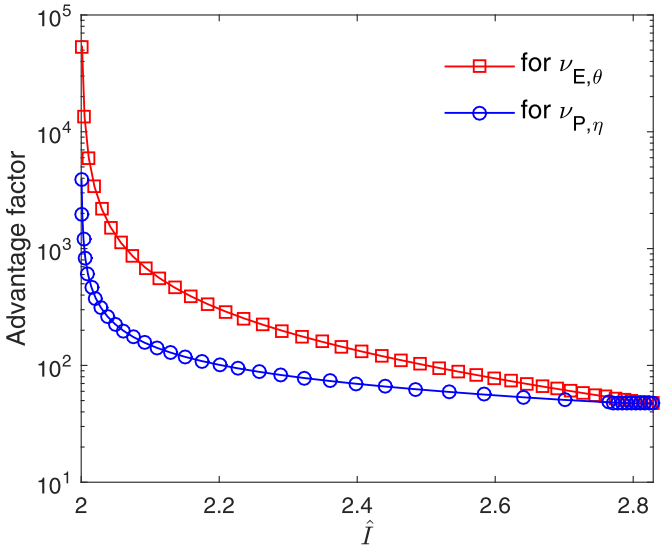

FIG. 2. QEF advantage factors as a function of $\hat{I}$. Shown are values for $f_{\nu_{\mathrm{E},\theta}}$ and $f_{\nu_{\mathrm{P},\eta}}$ when setting $\epsilon_h = \kappa' = 10^{-6}$. The QEFs used are derived from PEFs with the same power β for the classical trial model $\mathcal{T}(ABXY)$ by solving the QEF verification in Eq. (42). We verified that the quantity $f_{\max}$ as introduced below Eq. (42) is indistinguishable from 1 at high precision, specifically, $f_{\max} \in [1, 1 + 4 \times 10^{-8}]$, for each of the points indicated by open circles or squares.

(2) $\mathcal{P}_{\mathrm{W}} = \{\nu_{\mathrm{W},p}\}_{1/\sqrt{2}<p\leqslant 1}$, where A and B share the Werner state $p|\Psi_{\pi/4}\rangle\langle\Psi_{\pi/4}| + (1-p)\mathbb{1}/4$ with $p \in (1/\sqrt{2}, 1]$.

(3) $\mathcal{P}_{\mathrm{P}} = \{\nu_{\mathrm{P},\eta}\}_{2/3<\eta\leqslant 1}$, where each of A and B performs measurements with detectors of efficiency $\eta \in (2/3, 1]$ to close the detection loophole [50]. For each family, the distribution of the inputs XY is uniform. To generate the distribution $\nu_{\mathrm{E},\theta}$ or $\nu_{\mathrm{W},p}$, A and B choose their measurements such that the expected CHSH value $\hat{I}$ [31], given by $\hat{I} = \mathbb{E}(4(1-2XY)(-1)^{A+B})$, is maximized; while to generate the distribution $\nu_{\mathrm{P},\eta}$, A and B choose both the unbalanced Bell state $|\Psi_\theta\rangle$ shared between them and their measurements such that the statistical strength for rejecting local realism [51,52] is maximized. The family $\mathcal{P}_{\mathrm{E}}$ and $\mathcal{P}_{\mathrm{W}}$ represent the best and worst cases for conditional min-entropy as a function of $\hat{I}$, while $\mathcal{P}_{\mathrm{P}}$ is experimentally relevant, particularly for photonic experiments. The values for the parameter θ, p or η of each family are chosen such that $\hat{I}$ is above the classical upper bound 2 [31] (and of course not larger than the quantum maximum $2\sqrt{2}$ [49]). We note that $\hat{I}$ increases monotonically with each parameter θ, p or η.

For each family of distributions above, we determine the QEF advantage factor given by $f_\nu = n_{\mathrm{EAT},b=0}/n'_{\mathrm{QEF},b=0}$. For the distributions $\nu_{\mathrm{W},p}$, the advantage factor depends weakly on $\hat{I}$: $f_{\nu_{\mathrm{W},p}}$ increases from 45.6 at $\hat{I} = 2.008$ to 47.1 at $\hat{I} = 2\sqrt{2}$. For the other two families of distributions, the advantage factor can be much larger, particularly at $\hat{I}$ near 2, as shown in Fig. 2. We also verified that entropy accumulation with improved second-order in Ref. [14] can reduce $n_{\mathrm{EAT},b=0}$ *only* by a factor of no more than 2.02. Moreover, we verified that the above comparison results are almost unchanged when the identical value for ϵ_h and κ' varies from 10^{-2} to 10^{-20}.

[2]Here we reduce the value of $n_{\mathrm{EAT},b}$ obtained in our previous work [26] further by replacing the factor $\log_2(13)$ in theorem 16 of Ref. [26] with $\log_2(9)$. This improvement was first noticed in Ref. [41].

Next we re-analyze the work of Pironio *et al.* in 2010 [3], which reported the first experimental demonstration of certified randomness for DIRG with a Bell test free of the detection loophole. From the results of the experiment, the presence of 42 bits of smooth conditional min-entropy with the error 10^{-2} was certified in Ref. [3], where this error is related to a smoothness error but does not reflect currently accepted soundness definitions. The value for the error and that the certification did not take into account the success probability or quantum side information were clarified in subsequent papers [6,7]. A question is whether the experiment could have certified positive smooth conditional min-entropy with respect to quantum side information, which is answered as follows.

The experiment of Ref. [3] consisted of 3016 trials, of which we use the first 1000 for calibration. From the calibration data, we determine a distribution ν of trial results in the classical trial model $\mathcal{T}(ABXY)$ by maximum likelihood assuming i.i.d. trials (see Sec. VIII B of Ref. [25] for more details of this step). To find a PEF and its power β, we maximize the objective function in Eq. (30) with $n = 2016$, $\epsilon_h = 10^{-2}$, the distribution ν determined from the calibration data, and the replacement of a QEF by a PEF with the same power β.

After calibration, we determine that $f_{\max}$ for the PEF found satisfies $f_{\max} \in [1, 1 + 9.56 \times 10^{-6}]$. The bounds were computed at the numerical precision of $2^{-52} \approx 2.22 \times 10^{-16}$ with Matlab, then verified with Mathematica at the precision of 10^{-32}. From the PEF found and the upper bound on $f_{\max}$, we can obtain a valid QEF and apply this QEF to the remaining 2016 trials. The obtained QEF witnesses 127.86 bits of quantum smooth conditional min-entropy with $\epsilon_h = 10^{-2}$ in the experiment reported in Ref. [3], *if* the presumed lower bound κ' on the success probability in theorem 3 is formally set to be 1. We note that for the observed frequencies of trial results in this experiment, entropy accumulation implemented in Ref. [13] requires 54688 trials; while entropy accumulation with improved second-order in Ref. [14] requires 27620 trials, much more than the 3016 trials available in Ref. [3], in order to certify any random bits at the same ϵ_h and κ' as above. Here, the assignment of $\kappa' = 1$ is purely formal for comparison with respect to the soundness criteria implicit in Ref. [3]. These soundness criteria are now considered inadequate. With modern soundness criteria and at $\epsilon_h = \kappa' = 3 \times 10^{-2}$, the number of bits witnessed by the QEF is 72.70. This number is derived from the experimental QEF value. In a protocol, the number of bits to be produced needs to be determined before the experiment and would have to be set to a smaller number to ensure sufficiently high probability of success.

IX. CONCLUSION

The finite-data efficiency is an important factor for practical applications of device-independent randomness generation (DIRG). Previously available DIRG protocols with respect to quantum side information do not exhibit sufficiently high finite-data efficiency, so they require too many experimental trials even with the state-of-the-art photonic loophole-free Bell tests. In this work, we develop quantum probability estimation to yield DIRG protocols with unsurpassed finite-data efficiency and with respect to quantum side information. This enables a practical device-independent randomness beacon where a block of 512 device-independent random bits is generated with an average experiment time of less than 5 min and with certified error bounded by 2^{-64}, see our companion experimental work [43]. Our work also enables the realization of device-independent randomness expansion in the near future. Moreover, quantum probability estimation can be applied to the device-dependent scenario, which can result in more efficient randomness generation.

In contrast with previous works for addressing quantum side information, quantum probability estimation does not rely on fixed Bell inequalities for certifying device-independent randomness. The main result of quantum probability estimation is that the product of trialwise quantum estimation factors (QEFs) yields an estimator of the sandwiched Rényi entropy. Quantum probability estimation can further lower-bound the quantum smooth conditional min-entropy after considering the relation between sandwiched Rényi entropies and quantum smooth conditional min-entropies established in the literature. The implementation of quantum probability estimation requires well-performing trialwise QEFs. For DIRG with the CHSH Bell-test configuration, we provide a numerical approach to effectively construct such QEFs. It is straightforward to extend this numerical approach to Bell-test configurations with multiple parties as long as each party can randomly perform one of two binary-outcome measurements, see the last section of Ref. [44] for details.

Certifying quantum smooth conditional min-entropies is also the central task for quantum key distribution (QKD) [53]. In principle, quantum probability estimation can be extended to improve the finite-data efficiency of QKD, particularly device-independent QKD. For this, we need to certify the quantum smooth conditional min-entropy evaluated at a classical-quantum state after the error-correction step in QKD as done in Ref. [13]. We also need to develop alternative numerical approaches for constructing trialwise QEFs. We will address the details required for this extension in the future work.

ACKNOWLEDGMENTS

We thank Carl Miller and Peter Bierhorst for stimulating discussions and constructive suggestions on the paper writing. We also thank Dzmitry Matsukevich for providing the experimental data for Ref. [3] and Rotem Arnon-Friedman for discussing choices of security parameters. This work includes contributions of the National Institute of Standards and Technology, which are not subject to U.S. copyright. The use of trade names is for informational purposes only and does not imply endorsement or recommendation by the U.S. government.

APPENDIX A: PROTOCOL COMPOSABILITY

Other definitions of soundness for randomness generation use the trace distance instead of the purified distance as used in this work. The purified distance allows for extension to previously traced-out quantum systems such as that of the devices used in the protocol. This enables analysis of protocol

composition involving the same devices which may have memory (see the next two paragraphs). This kind of composition could introduce the possibility of memory attacks, whereby the devices leak information about the results of past protocols through leakage channels enabled by later protocols [45]. For randomness-generation protocols, such a leakage channel is introduced by the success flag $P_{\mathcal{G}}$: The devices can modify their future behavior so that the flags $P_{\mathcal{G}}$ of later protocols depend on the results of past protocols. A detailed discussion of memory attacks for randomness generation is in the supplemental material of Ref. [54]. We note that our protocol presented in Sec. V C of the main text has fixed-length outputs, which avoids leakage channels based on the length of the output but does not eliminate implementation-dependent leakage channels such as variations in timing or side-effects of using randomness.

We do not formally analyze composition of randomness-generation protocols with the same devices, and unrestricted composability is not assured. But to support such composition, we require that the devices are permanently isolated from E and that they never gain knowledge of the seeds used for randomness extraction. The latter supports the following strategy to mitigate $P_{\mathcal{G}}$-based leakage channels: Anticipate the number of future instances of the protocol and reduce the number of bits extracted from the current protocol accordingly. The requirements may be difficult to guarantee in practice but can be weakened once the randomness generated in past protocols is used, see the discussion in Ref. [54].

Let D be the quantum system of the devices, and let $\rho_{R_{\mathcal{G}}S_{\mathcal{G}}P_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}}$ be the actual, normalized state of the classical variables $R_{\mathcal{G}}, S_{\mathcal{G}}, P_{\mathcal{G}}$, $\mathbf{Z}$ and the quantum systems D, E after running the protocol. Thus $\rho_{R_{\mathcal{G}}S_{\mathcal{G}}P_{\mathcal{G}}\mathbf{Z}\mathsf{E}} = \mathrm{tr}_{\mathsf{D}}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}P_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}})$. Here, information about the outputs $\mathbf{C}$ may be contained in the quantum state of D. If the protocol is ϵ-sound, then the extension property of the purified distance (Cor. 3.6, p. 52 of Ref. [37]) implies that there exists a normalized state $\sigma_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}}$ such that

$$\begin{aligned}&\mathrm{PD}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}|(P_{\mathcal{G}}=1)}, \sigma_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}})\\ &\quad = \mathrm{PD}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{Z}\mathsf{E}|(P_{\mathcal{G}}=1)}, \tau_{R_{\mathcal{G}}S_{\mathcal{G}}} \otimes \sigma_{\mathbf{Z}\mathsf{E}}) \qquad \text{(A1)}\end{aligned}$$

and

$$\mathrm{tr}_{\mathsf{D}}(\sigma_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}}) = \tau_{R_{\mathcal{G}}S_{\mathcal{G}}} \otimes \sigma_{\mathbf{Z}\mathsf{E}}, \qquad \text{(A2)}$$

where $\tau_{R_{\mathcal{G}}S_{\mathcal{G}}} \otimes \sigma_{\mathbf{Z}\mathsf{E}}$ witnesses the ϵ-soundness according to the definition in Sec. V B of the main text. As the purified distance $\mathrm{PD}(\rho, \sigma)$ is an upper bound of the trace distance $\mathrm{D}(\rho, \sigma)$ (Prop. 3.3, p. 50 of Ref. [37]), from Eq. (18) in the main text and Eq. (A1), we get

$$\mathrm{D}(\rho_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}|(P_{\mathcal{G}}=1)}, \sigma_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}})\mathbb{P}_{\rho}(P_{\mathcal{G}} = 1) \leqslant \epsilon. \qquad \text{(A3)}$$

Therefore the soundness in terms of small purified distance implies the soundness in terms of small trace distance even if the previously traced-out quantum system of the devices is included. Here the soundness in terms of small trace distance is defined as existence of a normalized state $\sigma_{R_{\mathcal{G}}S_{\mathcal{G}}\mathbf{Z}\mathsf{D}\mathsf{E}}$ satisfying Eqs. (A2) and (A3). Our soundness definition thus enables composability analysis of protocols involving the same devices, where the composability is evaluated in terms of small trace distance.

APPENDIX B: A LEMMA USED IN THE PROOF OF THEOREM 4

Lemma 7. Suppose that a normalized state $\rho_{\mathbf{C}\mathbf{Z}\mathsf{E}}$ has ϵ-smooth max-prob p of $\mathbf{C}$ given $\mathbf{Z}\mathsf{E}$ with $p|\mathrm{Rng}(\mathbf{C})| \geqslant 1$. Then there exists a normalized state $\rho''_{\mathbf{C}\mathbf{Z}\mathsf{E}}$ such that $P_{\max}(\mathbf{C}|\mathbf{Z}\mathsf{E})_{\rho''} \leqslant p$ and $\mathrm{PD}(\rho_{\mathbf{C}\mathbf{Z}\mathsf{E}}, \rho''_{\mathbf{C}\mathbf{Z}\mathsf{E}}) \leqslant \epsilon$.

The condition $p|\mathrm{Rng}(\mathbf{C})| \geqslant 1$ is satisfied in protocol 1 of the main text for randomness generation.

Proof. Let $\rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}}$ be a subnormalized state and $\sigma_{\mathbf{Z}\mathsf{E}}$ be a normalized state such that $\mathrm{PD}(\rho_{\mathbf{C}\mathbf{Z}\mathsf{E}}, \rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}}) \leqslant \epsilon$ and $\rho'_{\mathsf{E}}(\mathbf{cz}) \leqslant p\sigma_{\mathsf{E}}(\mathbf{z})$ for all $\mathbf{cz}$. Let

$$\delta = 1 - \sum_{\mathbf{cz}} \mathrm{tr}(\rho'_{\mathsf{E}}(\mathbf{cz}))$$

and

$$\zeta = \sum_{\mathbf{cz}} \mathrm{tr}(p\sigma_{\mathsf{E}}(\mathbf{z}) - \rho'_{\mathsf{E}}(\mathbf{cz})) = p|\mathrm{Rng}(C)| - (1 - \delta).$$

Then $\delta \geqslant 0$ as the state $\rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}}$ is subnormalized. Since $p|\mathrm{Rng}(C)| \geqslant 1$, we have $\zeta \geqslant \delta$. Let

$$\tau_{\mathbf{C}\mathbf{Z}\mathsf{E}} = (\delta/\zeta)(p\mathbb{1}_{\mathbf{C}} \otimes \sigma_{\mathbf{Z}\mathsf{E}} - \rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}}).$$

Then $\mathrm{tr}(\tau_{\mathbf{C}\mathbf{Z}\mathsf{E}}) = \delta$ and $0 \leqslant \tau_{\mathbf{C}\mathbf{Z}\mathsf{E}} \leqslant p\mathbb{1}_{\mathbf{C}} \otimes \sigma_{\mathbf{Z}\mathsf{E}} - \rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}}$.

We can now define

$$\rho''_{\mathbf{C}\mathbf{Z}\mathsf{E}} = \rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}} + \tau_{\mathbf{C}\mathbf{Z}\mathsf{E}}.$$

Then we have $\rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}} \leqslant \rho''_{\mathbf{C}\mathbf{Z}\mathsf{E}}$, $\mathrm{tr}(\rho''_{\mathbf{C}\mathbf{Z}\mathsf{E}}) = 1$, and $\rho''_{\mathbf{C}\mathbf{Z}\mathsf{E}} \leqslant p\mathbb{1}_{\mathbf{C}} \otimes \sigma_{\mathbf{Z}\mathsf{E}}$, that is, $\rho''_{\mathsf{E}}(\mathbf{cz}) \leqslant p\sigma_{\mathsf{E}}(\mathbf{z})$ for all $\mathbf{cz}$. Thus $P_{\max}(\mathbf{C}|\mathbf{Z}\mathsf{E})_{\rho''} \leqslant p$.

Since $\rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}} \leqslant \rho''_{\mathbf{C}\mathbf{Z}\mathsf{E}}$, we have that for all $\mathbf{cz}$, $\rho'_{\mathsf{E}}(\mathbf{cz}) \leqslant \rho''_{\mathsf{E}}(\mathbf{cz})$ and so by theorem 3.25, p. 155 of Ref. [55]

$$\mathrm{tr}(|\sqrt{\rho_{\mathsf{E}}(\mathbf{cz})}\sqrt{\rho'_{\mathsf{E}}(\mathbf{cz})}|) \leqslant \mathrm{tr}(|\sqrt{\rho_{\mathsf{E}}(\mathbf{cz})}\sqrt{\rho''_{\mathsf{E}}(\mathbf{cz})}|).$$

Therefore, according to the definition of the purified distance in Eq. (12) of the main text we have $\mathrm{PD}(\rho_{\mathbf{C}\mathbf{Z}\mathsf{E}}, \rho''_{\mathbf{C}\mathbf{Z}\mathsf{E}}) \leqslant \mathrm{PD}(\rho_{\mathbf{C}\mathbf{Z}\mathsf{E}}, \rho'_{\mathbf{C}\mathbf{Z}\mathsf{E}}) \leqslant \epsilon$. ■

APPENDIX C: QUANTUM MARKOV CHAINS

For randomness certification with explicit conditioning on inputs, we make use of the concept of short quantum Markov chains [42]. Below we specialize the definition of short quantum Markov chains in Ref. [42] to the family of classical-quantum states considered in this work.

Consider a classical-quantum state $\rho_{UVW\mathsf{E}}$ of classical systems U, V, W and quantum system E. The state $\rho_{UVW\mathsf{E}}$ is said to be a *short quantum Markov chain over* $W\mathsf{E}$, written as $\rho_{UVW\mathsf{E}} \in U \leftrightarrow W\mathsf{E} \leftrightarrow V$, if for all w, there exists a factorization $\mathcal{H}(\mathsf{E}) = \bigoplus_k \mathcal{H}(\mathsf{E}_{1,k}(wU)) \otimes \mathcal{H}(\mathsf{E}_{2,k}(wV))$ such that $\rho_{\mathsf{E}}(uvw) = \bigoplus_k \sigma_{\mathsf{E}_{1,k}}(wu) \otimes \tau_{\mathsf{E}_{2,k}}(wv)$ for all $uv \in \mathrm{Rng}(UV)$. The definition is symmetric in U and V. That is, $\rho_{UVW\mathsf{E}} \in U \leftrightarrow W\mathsf{E} \leftrightarrow V$ if and only if $\rho_{UVW\mathsf{E}} \in V \leftrightarrow W\mathsf{E} \leftrightarrow U$.

APPENDIX D: PROOF OF THEOREM 5

A main step in the proof of theorem 5 of the main text is to apply the next lemma in order to change the conditioner of a sandwiched Rényi power from the marginal state to another

one. This change requires conditions on the relationship between the two conditioners. The conditions are expressed by introducing an auxiliary classical variable U and a classical-quantum state $\xi_{UZ\mathsf{E}}$ which is a short quantum Markov chain over E. Below we first present the lemma used and its proof. Then we prove theorem 5 of the main text.

Lemma 8. Let $F : \mathrm{Rng}(CZ) \to \mathbb{R}_{\geqslant 0}$ be a QEF with power β for $\mathcal{C}(CZ)$. Consider $\sigma_{CZ\mathsf{E}} = \sum_{cz} |cz\rangle\langle cz| \otimes \sigma_{\mathsf{E}}(cz) \in \mathcal{C}(CZ)$ and $\zeta_{Z\mathsf{E}} = \sum_z |z\rangle\langle z| \otimes \zeta_{\mathsf{E}}(z) \in \mathcal{S}(Z\mathsf{E})$ such that $\sigma_{\mathsf{E}}(z) = \sum_c \sigma_{\mathsf{E}}(cz) \ll \zeta_{\mathsf{E}}(z)$ for all z. Let $\sigma_{Z\mathsf{E}} = \mathrm{tr}_C(\sigma_{CZ\mathsf{E}})$, $\sigma_{\mathsf{E}} = \mathrm{tr}_{CZ}(\sigma_{CZ\mathsf{E}})$, $\zeta_{\mathsf{E}} = \mathrm{tr}_Z(\zeta_{Z\mathsf{E}})$, and U be a classical variable with $\mathrm{Rng}(U) = \{0, 1\}$. Define the states

$$\begin{aligned}\xi_{UZ\mathsf{E}} &= |0\rangle_U\langle 0| \otimes \sigma_{Z\mathsf{E}} + |1\rangle_U\langle 1| \otimes \zeta_{Z\mathsf{E}},\\ \chi_{\mathsf{E}} &= \zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)},\\ \rho_{CZ\mathsf{E}} &= \sum_{cz} |cz\rangle\langle cz| \otimes \left(\chi_{\mathsf{E}}^{\beta/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2}\right).\end{aligned} \tag{D1}$$

If $\rho_{CZ\mathsf{E}} \in \mathcal{C}(CZ)$ and $\xi_{UZ\mathsf{E}} \in U \leftrightarrow \mathsf{E} \leftrightarrow Z$, then the QEF inequality at $\rho_{CZ\mathsf{E}}$ is equivalent to

$$\sum_{cz} F(cz)\mathcal{R}_\alpha(\sigma_{\mathsf{E}}(cz)|\zeta_{\mathsf{E}}(z)) \leqslant \mathcal{R}_\alpha(\sigma_{\mathsf{E}}|\zeta_{\mathsf{E}}). \tag{D2}$$

The membership condition that $\rho_{CZ\mathsf{E}} \in \mathcal{C}(CZ)$ is satisfied if $\mathcal{C}(CZ)$ is pCP-closed. In the proof below, the main technique applied is the fact that $M^\dagger M \sim_U MM^\dagger$ for all square matrices M, where $\sim_U$ denotes equality up to conjugation by a unitary matrix, or equivalently, that $M^\dagger M$ and $MM^\dagger$ have the same spectrum with multiplicities. The fact that $M^\dagger M \sim_U MM^\dagger$ is due to the singular-value decomposition of the square matrix M.

Proof. Since $\rho_{CZ\mathsf{E}} \in \mathcal{C}(CZ)$, we have the QEF inequality

$$\sum_{cz} F(cz)\mathcal{R}_\alpha(\rho_{\mathsf{E}}(cz)|\rho_{\mathsf{E}}(z)) \leqslant \mathrm{tr}(\rho_{CZ\mathsf{E}}), \tag{D3}$$

where

$$\rho_{\mathsf{E}}(cz) = \chi_{\mathsf{E}}^{\beta/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2} \tag{D4}$$

and

$$\rho_{\mathsf{E}}(z) = \sum_c \rho_{\mathsf{E}}(cz) = \chi_{\mathsf{E}}^{\beta/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(z)\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2}. \tag{D5}$$

Thus, in order to prove the equivalence of Eqs. (D2) and (D3), we only need to show the following two equalities: (1) $\mathcal{R}_\alpha(\sigma_{\mathsf{E}}|\zeta_{\mathsf{E}}) = \mathrm{tr}(\rho_{CZ\mathsf{E}})$ and (2) $\mathcal{R}_\alpha(\sigma_{\mathsf{E}}(cz)|\zeta_{\mathsf{E}}(z)) = \mathcal{R}_\alpha(\rho_{\mathsf{E}}(cz)|\rho_{\mathsf{E}}(z))$ for all cz.

We first observe that

$$\begin{aligned}\rho_{\mathsf{E}} &= \mathrm{tr}_{CZ}(\rho_{CZ\mathsf{E}})\\ &= \chi_{\mathsf{E}}^{\beta/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2}\\ &= \left(\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\right)^\alpha,\end{aligned}$$

where the last equality follows from the definition of χ_{E} in Eq. (D1). In view of the above equation and the definition of sandwiched Rényi powers in Eq. (4) of the main text, we have $\mathcal{R}_\alpha(\sigma_{\mathsf{E}}|\zeta_{\mathsf{E}}) = \mathrm{tr}(\rho_{\mathsf{E}})$. Considering that $\mathrm{tr}(\rho_{CZ\mathsf{E}}) = \mathrm{tr}(\rho_{\mathsf{E}})$, we thus obtain the first desired equality.

We next prove the second desired equality. For this, it suffices to prove the spectral equivalence

$$\begin{aligned}&\rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\rho_{\mathsf{E}}(cz)\rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\\ &\quad\sim_U \zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)},\end{aligned} \tag{D6}$$

for each cz. The lemma assumes that for all z, $\sigma_{\mathsf{E}}(z) = \sum_c \sigma_{\mathsf{E}}(cz) \ll \zeta_{\mathsf{E}}(z)$, so the support of $\sigma_{\mathsf{E}}(cz)$ is contained in that of $\zeta_{\mathsf{E}}(z)$ for the right-hand side of Eq. (D6). Starting from the left-hand side and substituting the expression of $\rho_{\mathsf{E}}(cz)$, we get

$$\begin{aligned}&\rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\rho_{\mathsf{E}}(cz)\rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\\ &\quad= \rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2}\rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\\ &\quad\sim_U \sigma_{\mathsf{E}}(cz)^{1/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2}\rho_{\mathsf{E}}(z)^{-\beta/\alpha}\chi_{\mathsf{E}}^{\beta/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)^{1/2},\end{aligned} \tag{D7}$$

where for the above spectral equivalence we used the fact that $M^\dagger M \sim_U MM^\dagger$ with $M = \sigma_{\mathsf{E}}(cz)^{1/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2}\rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)}$.

To simplify the spectral equivalence in Eq. (D7) further, we use the definition of short quantum Markov chains. Since $\xi_{UZ\mathsf{E}} \in U \leftrightarrow \mathsf{E} \leftrightarrow Z$, there exists a factorization $\mathcal{H}(\mathsf{E}) = \bigoplus_k \mathcal{H}(\mathsf{E}_{1,k}(U)) \otimes \mathcal{H}(\mathsf{E}_{2,k}(Z))$ such that

$$\sigma_{\mathsf{E}}(z) = \bigoplus_k \sigma_{\mathsf{E}_{1,k}} \otimes \xi_{\mathsf{E}_{2,k}}(z), \quad \zeta_{\mathsf{E}}(z) = \bigoplus_k \zeta_{\mathsf{E}_{1,k}} \otimes \xi_{\mathsf{E}_{2,k}}(z). \tag{D8}$$

Let $\xi_{\mathsf{E}_{2,k}} = \sum_z \xi_{\mathsf{E}_{2,k}}(z)$. Then Eq. (D8) implies that

$$\sigma_{\mathsf{E}} = \bigoplus_k \sigma_{\mathsf{E}_{1,k}} \otimes \xi_{\mathsf{E}_{2,k}}, \quad \zeta_{\mathsf{E}} = \bigoplus_k \zeta_{\mathsf{E}_{1,k}} \otimes \xi_{\mathsf{E}_{2,k}}.$$

From the above equation and in view of the definition of χ_{E} in Eq. (D1), we have $\chi_{\mathsf{E}} = \bigoplus_k \chi_{\mathsf{E}_{1,k}} \otimes \xi_{\mathsf{E}_{2,k}}^{1/\alpha}$, where

$$\chi_{\mathsf{E}_{1,k}} = \zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}_{1,k}}\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}. \tag{D9}$$

The operator $\chi_{\mathsf{E}_{1,k}}$ is well defined since the assumption that $\sigma_{\mathsf{E}}(z) \ll \zeta_{\mathsf{E}}(z)$ in the statement of the lemma ensures that $\sigma_{\mathsf{E}_{1,k}} \ll \zeta_{\mathsf{E}_{1,k}}$ for each k. With the direct-sum expressions for ζ_{E} and χ_{E}, we get

$$\begin{aligned}\chi_{\mathsf{E}}^{\beta/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)} &= \bigoplus_k \left(\chi_{\mathsf{E}_{1,k}}^{\beta/2}\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\right) \otimes \mathbb{1}_{\mathsf{E}_{2,k}},\\ \zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2} &= \bigoplus_k \left(\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}_{1,k}}^{\beta/2}\right) \otimes \mathbb{1}_{\mathsf{E}_{2,k}},\end{aligned} \tag{D10}$$

where $\mathbb{1}_{\mathsf{E}_{2,k}}$ is the projector onto the support of $\xi_{\mathsf{E}_{2,k}}$ in $\mathcal{H}(\mathsf{E}_{2,k})$. From Eqs. (D8) and (D10) and in view of the expressions of $\rho_{\mathsf{E}}(z)$ in Eq. (D5) and $\chi_{\mathsf{E}_{1,k}}$ in Eq. (D9), we obtain

$$\begin{aligned}&\rho_{\mathsf{E}}(z)^{-\beta/\alpha}\\ &\quad= \left(\chi_{\mathsf{E}}^{\beta/2}\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(z)\zeta_{\mathsf{E}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}}^{\beta/2}\right)^{-\beta/\alpha}\\ &\quad= \bigoplus_k \left(\chi_{\mathsf{E}_{1,k}}^{\beta/2}\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}_{1,k}}\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}_{1,k}}^{\beta/2}\right)^{-\beta/\alpha} \otimes \xi_{\mathsf{E}_{2,k}}(z)^{-\beta/\alpha}\\ &\quad= \bigoplus_k \chi_{\mathsf{E}_{1,k}}^{-\beta} \otimes \xi_{\mathsf{E}_{2,k}}(z)^{-\beta/\alpha}.\end{aligned} \tag{D11}$$

Let $\Pi_{\mathsf{E}_{1,k}}$ be the projector onto the support of $\chi_{\mathsf{E}_{1,k}}$ and $\Pi_{\mathsf{E}} = \bigoplus_k \Pi_{\mathsf{E}_{1,k}} \otimes \mathbb{1}_{\mathsf{E}_{2,k}}$ be the projector onto the support of χ_{E}. Substituting the identities obtained in Eqs. (D10) and (D11) and continuing from the last line of Eq. (D7), we get

$$\begin{aligned}
&\rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\rho_{\mathsf{E}}(cz)\rho_{\mathsf{E}}(z)^{-\beta/(2\alpha)} \\
&\quad\sim_U \sigma_{\mathsf{E}}(cz)^{1/2}\left(\bigoplus_k \left(\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\chi_{\mathsf{E}_{1,k}}^{\beta/2}\chi_{\mathsf{E}_{1,k}}^{-\beta}\chi_{\mathsf{E}_{1,k}}^{\beta/2}\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\right)\otimes \xi_{\mathsf{E}_{2,k}}(z)^{-\beta/\alpha}\right)\sigma_{\mathsf{E}}(cz)^{1/2} \\
&\quad= \sigma_{\mathsf{E}}(cz)^{1/2}\left(\bigoplus_k \left(\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\Pi_{\mathsf{E}_{1,k}}\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\right)\otimes \xi_{\mathsf{E}_{2,k}}(z)^{-\beta/\alpha}\right)\sigma_{\mathsf{E}}(cz)^{1/2} \\
&\quad= \sigma_{\mathsf{E}}(cz)^{1/2}\left(\bigoplus_k \left(\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\Pi_{\mathsf{E}_{1,k}}\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\right)\otimes \left(\xi_{\mathsf{E}_{2,k}}(z)^{-\beta/(2\alpha)}\mathbb{1}_{\mathsf{E}_{2,k}}\xi_{\mathsf{E}_{2,k}}(z)^{-\beta/(2\alpha)}\right)\right)\sigma_{\mathsf{E}}(cz)^{1/2} \\
&\quad= \sigma_{\mathsf{E}}(cz)^{1/2}\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\Pi_{\mathsf{E}}\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)^{1/2} \\
&\quad\sim_U \Pi_{\mathsf{E}}\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\Pi_{\mathsf{E}},
\end{aligned} \tag{D12}$$

where to obtain the second last line we used Eq. (D8), and to obtain the spectral equivalence in the last line we used the fact that $M^\dagger M \sim_U MM^\dagger$ with $M = \Pi_{\mathsf{E}}\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)^{1/2}$.

The support of $\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(cz)\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}$ is contained in that of $\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(z)\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}$. In view of Eqs. (D8) and (D9), the support of $\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}\sigma_{\mathsf{E}}(z)\zeta_{\mathsf{E}}(z)^{-\beta/(2\alpha)}$ is the direct sum of the supports of $(\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}\sigma_{\mathsf{E}_{1,k}}\zeta_{\mathsf{E}_{1,k}}^{-\beta/(2\alpha)}) \otimes \xi_{\mathsf{E}_{2,k}}(z)^{1/\alpha} = \chi_{\mathsf{E}_{1,k}} \otimes \xi_{\mathsf{E}_{2,k}}(z)^{1/\alpha}$, which is contained in the support of χ_{E}. Therefore the projector Π_{E} onto the support of χ_{E} can be eliminated from the final expression in Eq. (D12) to finish the proof of Eq. (D6). ■

Now we can prove theorem 5 of the main text as follows.

Proof. Consider an arbitrary state $\rho_{\mathbf{CZ}CZ\mathsf{E}} = \sum_{\mathbf{cz}cz} |\mathbf{cz}cz\rangle\langle\mathbf{cz}cz| \otimes \rho_{\mathsf{E}}(\mathbf{cz}cz) \in \mathcal{C}(\mathbf{CZ}) \circ_{Z|\mathbf{Z}} \mathcal{C}_{\mathbf{CZ}}(CZ)$. For each $\mathbf{cz}$, the state $\rho_{\mathbf{cz}CZ\mathsf{E}} = \sum_{cz} |cz\rangle\langle cz| \otimes \rho_{\mathsf{E}}(\mathbf{cz}cz) \in \mathcal{C}_{\mathbf{cz}}(CZ)$ according to the model chaining defined in Eq. (26) of the main text. Let $F_{\mathbf{cz}}(CZ)$ be a QEF with power β for $\mathcal{C}_{\mathbf{cz}}(CZ)$. The main step in this proof is to show that for each $\mathbf{cz}$,

$$\sum_{cz} F_{\mathbf{cz}}(cz)\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz}cz)|\rho_{\mathsf{E}}(\mathbf{z}z)) \leqslant \mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})), \tag{D13}$$

where $\rho_{\mathsf{E}}(\mathbf{z}z)$, $\rho_{\mathsf{E}}(\mathbf{cz})$ and $\rho_{\mathsf{E}}(\mathbf{z})$ are the un-normalized marginal states of E given the respective results $\mathbf{z}z$, $\mathbf{cz}$ and $\mathbf{z}$ according to $\rho_{\mathbf{CZ}CZ\mathsf{E}}$.

Suppose that the inequality in Eq. (D13) is proven. Then we have

$$\begin{aligned}
&\sum_{\mathbf{cz}cz} G(\mathbf{cz})F_{\mathbf{cz}}(cz)\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz}cz)|\rho_{\mathsf{E}}(\mathbf{z}z)) \\
&\quad= \sum_{\mathbf{cz}} G(\mathbf{cz}) \sum_{cz} F_{\mathbf{cz}}(cz)\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz}cz)|\rho_{\mathsf{E}}(\mathbf{z}z)) \\
&\quad\leqslant \sum_{\mathbf{cz}} G(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad\leqslant \mathrm{tr}(\rho_{\mathbf{CZ}\mathsf{E}}) = \mathrm{tr}(\rho_{\mathbf{CZ}CZ\mathsf{E}}),
\end{aligned}$$

where the inequality in the third line follows from Eq. (D13), and the inequality in the fourth line follows from the facts that $G(\mathbf{CZ})$ is a QEF with power β for $\mathcal{C}(\mathbf{CZ})$ and that the state $\rho_{\mathbf{CZ}\mathsf{E}} \doteq \mathrm{tr}_{CZ}(\rho_{\mathbf{CZ}CZ\mathsf{E}})$ is in the model $\mathcal{C}(\mathbf{CZ})$ according to the model chaining defined in Eq. (26) of the main text. Because $\rho_{\mathbf{CZ}CZ\mathsf{E}}$ is an arbitrary state in the chained model $\mathcal{C}(\mathbf{CZ}) \circ_{Z|\mathbf{Z}} \mathcal{C}_{\mathbf{CZ}}(CZ)$, the above inequality shows that the function $G \diamond F$ defined in the statement of theorem 5 of the main text is a QEF with power β as claimed.

The desired inequality in Eq. (D13) can be obtained *if* lemma 8 is applicable. Specifically, we need to apply lemma 8 with the following substitutions: (1) $\sigma_{CZ\mathsf{E}} \to \rho_{\mathbf{cz}CZ\mathsf{E}}$, (2) $\zeta_{Z\mathsf{E}} \to \rho_{\mathbf{z}Z\mathsf{E}}$, and (3) $F(CZ) \to F_{\mathbf{cz}}(CZ)$, where $\rho_{\mathbf{z}Z\mathsf{E}} = \sum_z |z\rangle\langle z| \otimes \rho_{\mathsf{E}}(\mathbf{z}z)$ with $\rho_{\mathsf{E}}(\mathbf{z}z) = \sum_{\mathbf{c}c} \rho_{\mathsf{E}}(\mathbf{cz}cz)$. Then $\xi_{UZ\mathsf{E}}$ defined in lemma 8 becomes

$$\xi_{UZ\mathsf{E}} = |0\rangle_U\langle 0| \otimes \rho_{\mathbf{cz}Z\mathsf{E}} + |1\rangle_U\langle 1| \otimes \rho_{\mathbf{z}Z\mathsf{E}}, \tag{D14}$$

where $\rho_{\mathbf{cz}Z\mathsf{E}} = \sum_z |z\rangle\langle z| \otimes \rho_{\mathsf{E}}(\mathbf{cz}z)$ with $\rho_{\mathsf{E}}(\mathbf{cz}z) = \sum_c \rho_{\mathsf{E}}(\mathbf{cz}cz)$.

To apply lemma 8, we need to verify the short quantum Markov-chain condition $\xi_{UZ\mathsf{E}} \in U \leftrightarrow \mathsf{E} \leftrightarrow Z$ for each $\mathbf{cz}$. This follows from $\rho_{\mathbf{CZ}Z\mathsf{E}} \in \mathbf{C} \leftrightarrow \mathbf{Z}\mathsf{E} \leftrightarrow Z$ according to the definition of model chaining with conditionally independent inputs in Sec. VI B of the main text. For each $\mathbf{z}$, there exists a factorization $\mathcal{H}(\mathsf{E}) = \bigoplus_i \mathcal{H}(\mathsf{E}_{1,i}) \otimes \mathcal{H}(\mathsf{E}_{2,i})$ such that for each $\mathbf{c}$ and z, $\rho_{\mathsf{E}}(\mathbf{cz}z) = \bigoplus_i \sigma_{\mathsf{E}_{1,i}}(\mathbf{c}) \otimes \zeta_{\mathsf{E}_{2,i}}(z)$ for some $\sigma_{\mathsf{E}_{1,i}}(\mathbf{c}) \in \mathcal{H}(\mathsf{E}_{1,i})$ and $\zeta_{\mathsf{E}_{2,i}}(z) \in \mathcal{H}(\mathsf{E}_{2,i})$ that depend implicitly on $\mathbf{z}$. This implies that for each $\mathbf{z}$ and z, $\rho_{\mathsf{E}}(\mathbf{z}z) = \bigoplus_i \sigma_{\mathsf{E}_{1,i}} \otimes \zeta_{\mathsf{E}_{2,i}}(z)$ with $\sigma_{\mathsf{E}_{1,i}} = \sum_{\mathbf{c}} \sigma_{\mathsf{E}_{1,i}}(\mathbf{c})$. Then, according to Eq. (D14) the un-normalized marginal state of E given u and z becomes

$$\xi_{\mathsf{E}}(uz) = \bigoplus_i \left(\sigma_{\mathsf{E}_{1,i}}(\mathbf{c})[\![u=0]\!] + \sigma_{\mathsf{E}_{1,i}}[\![u=1]\!]\right) \otimes \zeta_{\mathsf{E}_{2,i}}(z),$$

where $[\![x=y]\!]$ takes value 1 when x is equal to y and 0 otherwise. The above equation implies $\xi_{UZ\mathsf{E}} \in U \leftrightarrow \mathsf{E} \leftrightarrow Z$ for each $\mathbf{cz}$. The membership condition of lemma 8 is also satisfied since for each $\mathbf{cz}$ the model $\mathcal{C}_{\mathbf{cz}}(CZ)$ is assumed to be pCP-closed. Hence we can apply lemma 8 to obtain Eq. (D13). ■

APPENDIX E: PROOFS OF QEF PROPERTIES

Proof of property 1. Consider an arbitrary state $\rho_{\mathbf{CZ}\mathsf{E}}$ in an arbitrary model $\mathcal{C}(\mathbf{CZ})$. It suffices to verify Eq. (27) in the

main text as follows:

$$\begin{aligned}
&\sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad= \sum_{\mathbf{cz}} \mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad= \sum_{\mathbf{z}}\sum_{\mathbf{c}} \mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad\leqslant \sum_{\mathbf{z}}\sum_{\mathbf{c}} \mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{cz})) \\
&\quad= \sum_{\mathbf{z}}\sum_{\mathbf{c}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz})) = \mathrm{tr}(\rho_{\mathbf{CZE}}),
\end{aligned}$$

where for the inequality in the fourth line we used the following dominance property of Rényi powers: $\mathcal{R}_\alpha(\rho|\sigma') \leqslant \mathcal{R}_\alpha(\rho|\sigma)$ for $0 \leqslant \rho \ll \sigma \leqslant \sigma'$ (see Sec. 4.1.2 of Ref. [28]).

Proof of property 2. It suffices to check that if the QEF inequality holds at $\rho_{\mathbf{CZE},i} \in \mathcal{C}(\mathbf{CZ})$ for each $i \in \mathrm{Rng}(I)$, then it holds at every convex combination $\rho_{\mathbf{CZE}} = \sum_i \lambda_i \rho_{\mathbf{CZE},i} \in \mathrm{Cone}(\mathcal{C}(\mathbf{CZ}))$, where $\lambda_i \geqslant 0$ and $\sum_i \lambda_i = 1$. By the joint convexity of sandwiched Rényi powers (Prop. 3 of Ref. [56]), for all $\mathbf{cz}$ we have

$$\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \leqslant \sum_i \lambda_i \mathcal{R}_\alpha(\rho_{\mathsf{E},i}(\mathbf{cz})|\rho_{\mathsf{E},i}(\mathbf{z})).$$

Considering that $F(\mathbf{cz}) \geqslant 0$ for all $\mathbf{cz}$, we obtain

$$\begin{aligned}
&\sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad\leqslant \sum_{\mathbf{cz}} F(\mathbf{cz}) \sum_i \lambda_i \mathcal{R}_\alpha(\rho_{\mathsf{E},i}(\mathbf{cz})|\rho_{\mathsf{E},i}(\mathbf{z})) \\
&\quad= \sum_i \lambda_i \sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E},i}(\mathbf{cz})|\rho_{\mathsf{E},i}(\mathbf{z})) \\
&\quad\leqslant \sum_i \lambda_i \mathrm{tr}(\rho_{\mathbf{CZE},i}) \\
&\quad= \mathrm{tr}(\rho_{\mathbf{CZE}}).
\end{aligned}$$

Proof of property 3. This property follows from the data-processing inequality for Rényi powers: $\mathcal{R}_\alpha(\mathcal{E}(\rho)|\mathcal{E}(\sigma)) \leqslant \mathcal{R}_\alpha(\rho|\sigma)$ for any CPTP map $\mathcal{E}$ and $0 \leqslant \rho \ll \sigma$ (see Refs. [56,57] for the proof).

It suffices to check that if the QEF inequality holds at $\rho_{\mathbf{CZE}} \in \mathcal{C}(\mathbf{CZ})$, then it holds at $\sigma_{\mathbf{CZE}} = \sum_{\mathbf{cz}} |\mathbf{cz}\rangle\langle\mathbf{cz}| \otimes \mathcal{E}_{\mathbf{z}}(\rho_{\mathsf{E}}(\mathbf{cz})) \in \mathcal{E}_{\mathbf{Z}}(\mathcal{C}(\mathbf{CZ}))$ as follows:

$$\begin{aligned}
&\sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\sigma_{\mathsf{E}}(\mathbf{cz})|\sigma_{\mathsf{E}}(\mathbf{z})) \\
&\quad= \sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\mathcal{E}_{\mathbf{z}}(\rho_{\mathsf{E}}(\mathbf{cz}))|\mathcal{E}_{\mathbf{z}}(\rho_{\mathsf{E}}(\mathbf{z}))) \\
&\quad\leqslant \sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad\leqslant \mathrm{tr}(\rho_{\mathbf{CZE}}) = \sum_{\mathbf{z}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad= \sum_{\mathbf{z}} \mathrm{tr}(\mathcal{E}_{\mathbf{z}}(\rho_{\mathsf{E}}(\mathbf{z}))) = \mathrm{tr}(\sigma_{\mathbf{CZE}}).
\end{aligned}$$

The inequality in the third line follows from the data-processing inequality for Rényi powers, and the equality in the fifth line follows from the fact that each $\mathcal{E}_{\mathbf{z}}$ is trace-preserving.

Proof of property 4. For $0 \leqslant \rho \ll \sigma$, define the quantity $\tilde{D}_\alpha(\rho\|\sigma) = \frac{1}{\beta}\log_2(\hat{\mathcal{R}}_\alpha(\rho|\sigma))$, which is the sandwiched Rényi divergence of order α of ρ conditional on σ as introduced in Refs. [34,35]. Without loss of generality, consider a normalized state $\rho_{\mathbf{CZE}} \in \mathcal{C}(\mathbf{CZ})$. According to the QEF inequality,

$$\begin{aligned}
1 &\geqslant \sum_{\mathbf{cz}} F(\mathbf{cz})\mathcal{R}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&= \sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))F(\mathbf{cz})\hat{\mathcal{R}}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&= \sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))2^{\log_2(F(\mathbf{cz}))+\beta\tilde{D}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})\|\rho_{\mathsf{E}}(\mathbf{z}))}, \\
&\geqslant 2^{\sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))(\log_2(F(\mathbf{cz}))+\beta\tilde{D}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})\|\rho_{\mathsf{E}}(\mathbf{z})))},
\end{aligned}$$

where the last line is due to the convexity of the function $g(x) = 2^x$ with $x \in \mathbb{R}$. In view of the above inequality and the monotonicity of the function $g(x) = 2^x$, we have

$$0 \geqslant \sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))(\log_2(F(\mathbf{cz})) + \beta\tilde{D}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})\|\rho_{\mathsf{E}}(\mathbf{z}))).$$

Equivalently,

$$\begin{aligned}
&\sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))\log_2(F(\mathbf{cz}))/\beta \\
&\quad\leqslant -\sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))\tilde{D}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})\|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad\leqslant -\sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))\big(\lim_{\beta\to 0}\tilde{D}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})\|\rho_{\mathsf{E}}(\mathbf{z}))\big) \\
&\quad= -\sum_{\mathbf{cz}} \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz})(\log_2(\rho_{\mathsf{E}}(\mathbf{cz})) - \log_2(\rho_{\mathsf{E}}(\mathbf{z})))) \\
&\quad= H_1(\mathbf{C}|\mathbf{ZE})_\rho, \qquad \text{(E1)}
\end{aligned}$$

where the inequality in the third line is due to the fact that $\tilde{D}_\alpha(\rho\|\sigma)$ is monotonically increasing in α (see Cor. 4.2, p. 56 of Ref. [28]), and the equality in the fourth line follows from Prop. 4.5, p. 57 of Ref. [28].

The property follows from the fact that $\rho_{\mathbf{CZE}}$ is an arbitrary normalized state in the model $\mathcal{C}(\mathbf{CZ})$ and the definition of entropy estimators in Eq. (28).

Proof of property 5. Consider an arbitrary normalized state $\rho_{\mathbf{CZE}} \in \mathcal{C}(\mathbf{CZ})$. In view of the QEF inequality in Eq. (7) of the main text, it suffices to show that $g_{\mathbf{cz}}(\alpha) \doteq \mathcal{R}_\alpha(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z}))$ is a nonincreasing function of α for all $\mathbf{cz}$. For this, we consider the following two cases. (1) For the $\mathbf{cz}$ with $\rho_{\mathsf{E}}(\mathbf{cz}) = 0$, we have $g_{\mathbf{cz}}(\alpha) = 0$ for all α, and so $g_{\mathbf{cz}}(\alpha)$ is nonincreasing. (2) For the $\mathbf{cz}$ with $\rho_{\mathsf{E}}(\mathbf{cz}) > 0$, since $\sum_{\mathbf{c'z'}} g_{\mathbf{c'z'}}(\alpha) \leqslant 1$ (by property 1) and since the summands are non-negative, we have $g_{\mathbf{cz}}(\alpha) \leqslant 1$. Therefore the value of $\log_{10}(g_{\mathbf{cz}}(\alpha))$ is nonpositive. Log-convexity of sandwiched Rényi powers as functions of α (see the first half of Cor. 4.2, p. 56 of Ref. [28]) implies that the slope of $\log_{10}(g_{\mathbf{cz}}(\alpha))$ as a function of α is nondecreasing. In view of $-\infty < \log_{10}(g_{\mathbf{cz}}(\alpha)) \leqslant 0$, the slope of the function $\log_{10}(g_{\mathbf{cz}}(\alpha))$ at any α cannot become positive, otherwise when $\alpha \nearrow \infty$ the value of $\log_{10}(g_{\mathbf{cz}}(\alpha))$ would become positive. Thus $\log_{10}(g_{\mathbf{cz}}(\alpha))$ is a nonincreasing

function of α. Moreover, since the function $\log_{10}(x)$ is order-preserving, $g_{\mathbf{cz}}(\alpha)$ is also a nonincreasing function of α.

Proof of property 6. Consider a normalized state $\rho_{\mathbf{CZE}} \in \mathcal{C}(\mathbf{CZ})$. Define the probability distribution $\mu(\mathbf{CZ})$ by $\mu(\mathbf{cz}) = \mathrm{tr}(\rho_{\mathsf{E}}(\mathbf{cz}))$. We check the QEF inequality with power $\gamma\beta$ at $\rho_{\mathbf{CZE}}$ as follows:

$$\begin{aligned}
&\sum_{\mathbf{cz}} F(\mathbf{cz})^{\gamma} \mathcal{R}_{1+\gamma\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad = \sum_{\mathbf{cz}} F(\mathbf{cz})^{\gamma} \mu(\mathbf{cz}) \hat{\mathcal{R}}_{1+\gamma\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad = \sum_{\mathbf{cz}} \mu(\mathbf{cz}) (F(\mathbf{cz}) \hat{\mathcal{R}}_{1+\gamma\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z}))^{1/\gamma})^{\gamma} \\
&\quad \leqslant \left(\sum_{\mathbf{cz}} \mu(\mathbf{cz}) F(\mathbf{cz}) \hat{\mathcal{R}}_{1+\gamma\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z}))^{1/\gamma} \right)^{\gamma},
\end{aligned}$$

since for $\gamma \in (0, 1]$ the function $g(x) = x^{\gamma}$ is concave and the sums are expectations with respect to $\mu(\mathbf{CZ})$. By the fact that the quantity $\hat{\mathcal{R}}_{\alpha}(\rho|\sigma)^{1/(\alpha-1)}$ is a nondecreasing function of α (see the second half of Cor. 4.2, p. 56 of Ref. [28]), we have $\hat{\mathcal{R}}_{1+\gamma\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z}))^{1/(\beta\gamma)} \leqslant \hat{\mathcal{R}}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z}))^{1/\beta}$. So we can continue where we left off to get

$$\begin{aligned}
&\sum_{\mathbf{cz}} F(\mathbf{cz})^{\gamma} \mathcal{R}_{1+\gamma\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \\
&\quad \leqslant \left(\sum_{\mathbf{cz}} \mu(\mathbf{cz}) F(\mathbf{cz}) \hat{\mathcal{R}}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \right)^{\gamma} \\
&\quad = \left(\sum_{\mathbf{cz}} F(\mathbf{cz}) \mathcal{R}_{1+\beta}(\rho_{\mathsf{E}}(\mathbf{cz})|\rho_{\mathsf{E}}(\mathbf{z})) \right)^{\gamma} \leqslant 1,
\end{aligned}$$

since $F(\mathbf{CZ})$ is assumed to be a QEF with power β.

The property follows from the fact that $\rho_{\mathbf{CZE}}$ is an arbitrary normalized state in the model $\mathcal{C}(\mathbf{CZ})$.

APPENDIX F: PROOF OF THEOREM 6

Proof. We first apply the lemma of Ref. [46] or lemma 2 of Ref. [48]. Accordingly, there exists an orthonormal basis in $\mathcal{H}(\mathsf{D}) = \mathcal{H}(\mathsf{D_A}) \otimes \mathcal{H}(\mathsf{D_B})$ such that for all inputs x (or y) and outputs a (or b) the POVM elements have the direct-sum structure

$$\begin{aligned}
P_{\mathsf{D_A},x}(a) \otimes \mathbb{1}_{\mathsf{D_B}} &= \left(\oplus_i P_{\mathsf{D}_{\mathsf{A}}^{(i)},x}(a)\right) \otimes \mathbb{1}_{\mathsf{D_B}}, \\
\mathbb{1}_{\mathsf{D_A}} \otimes P_{\mathsf{D_B},y}(b) &= \mathbb{1}_{\mathsf{D_A}} \otimes \left(\oplus_j P_{\mathsf{D}_{\mathsf{B}}^{(j)},y}(b)\right),
\end{aligned}$$

where $P_{\mathsf{D}_{\mathsf{A}}^{(i)},x}(a)$ and $P_{\mathsf{D}_{\mathsf{b}}^{(j)},y}(b)$ are projective and of dimension 1×1 or 2×2. On the one-dimensional summands, each $P_{\mathsf{D}_{\mathsf{A}}^{(i)},x}(a)$ and $P_{\mathsf{D}_{\mathsf{B}}^{(j)},y}(b)$ is equal to 0 or 1. We can add a second dimension on which the state has no support and extend the measurements to the added dimension such that each $P_{\mathsf{D}_{\mathsf{A}}^{(i)},x}(a)$ and $P_{\mathsf{D}_{\mathsf{B}}^{(j)},y}(b)$ becomes of the form $Q_{0;\theta}(s)$ in Eq. (36) of the main text. Therefore, for all summands ij and for all inputs xy and outputs ab, these exist orthonormal bases in $\mathcal{H}(\mathsf{D_A})$ and $\mathcal{H}(\mathsf{D_B})$ such that $P_{\mathsf{D}_{\mathsf{A}}^{(i)},x}(a)$ and $P_{\mathsf{D}_{\mathsf{B}}^{(j)},y}(b)$ can be written as $Q_{x;\theta_{\mathsf{A},i}}(a)$ and $Q_{y;\theta_{\mathsf{B},j}}(b)$ for some $\theta_{\mathsf{A},i}, \theta_{\mathsf{B},j} \in (-\pi, \pi]$.

The direct-sum structure of POVMs implies that for all inputs xy and outputs ab

$$\begin{aligned}
&\mathrm{tr}_{\mathsf{D}}\left(\rho_{\mathsf{DE}}\left(P_{\mathsf{D_A},x}(a) \otimes P_{\mathsf{D_B},y}(b) \otimes \mathbb{1}_{\mathsf{E}}\right)\right) \\
&\quad = \sum_{ij} \mathrm{tr}_{\mathsf{D}_{\mathsf{A}}^{(i)}\mathsf{D}_{\mathsf{B}}^{(j)}}\left(\rho_{\mathsf{D}_{\mathsf{A}}^{(i)}\mathsf{D}_{\mathsf{B}}^{(j)}\mathsf{E}}\left(Q_{x;\theta_{\mathsf{A},i}}(a) \otimes Q_{y;\theta_{\mathsf{B},j}}(b) \otimes \mathbb{1}_{\mathsf{E}}\right)\right),
\end{aligned}$$

where the state $\rho_{\mathsf{D}_{\mathsf{A}}^{(i)}\mathsf{D}_{\mathsf{B}}^{(j)}\mathsf{E}} \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{H}(\mathsf{E})$ is the projection of ρ_{DE} onto the joint support of the operators $Q_{x;\theta_{\mathsf{A},i}}(a) \otimes Q_{y;\theta_{\mathsf{B},j}}(b) \otimes \mathbb{1}_{\mathsf{E}}$ with all $abxy$. By the above equation and considering that extremal states are pure, all members of the induced model $\mathcal{M}(\mathcal{P}_{\mathsf{D},xy}(AB); \mathsf{E})$ for each xy are positive combinations of the states $\rho_{AB\mathsf{E}|xy}$ in the form

$$\rho_{AB\mathsf{E}|xy} = \sum_{ab} |ab\rangle\langle ab| \otimes \mathrm{tr}_{\mathsf{D}}(|\psi\rangle_{\mathsf{DE}}\langle\psi|(\Pi_{ab|xy} \otimes \mathbb{1}_{\mathsf{E}})) \quad \text{(F1)}$$

with a pure state $|\psi\rangle_{\mathsf{DE}} \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{H}(\mathsf{E})$ and $\Pi_{ab|xy}$ as given in the statement of theorem 6 of the main text. Note that here and in the following of the proof we abbreviate $\Pi_{ab|xy}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}})$ as $\Pi_{ab|xy}$.

Without loss of generality, the dimension of $\mathcal{H}(\mathsf{E})$ is not less than 4, the dimension of $\mathbb{C}^2 \otimes \mathbb{C}^2$. Then, according to the Schmidt decomposition there exist an orthonormal basis $\{|v\rangle_{\mathsf{D}}\}_{v \in \mathrm{Rng}(V)}$ of $\mathbb{C}^2 \otimes \mathbb{C}^2$ and a partial orthonormal basis $\{|v\rangle_{\mathsf{E}}\}_{v \in \mathrm{Rng}(V)}$ of $\mathcal{H}(\mathsf{E})$ with $|\mathrm{Rng}(V)| = 4$ such that the state $|\psi\rangle_{\mathsf{DE}}$ can be written as

$$|\psi\rangle_{\mathsf{DE}} = \sum_{v} \lambda_v |v\rangle_{\mathsf{D}} \otimes |v\rangle_{\mathsf{E}}, \quad \text{(F2)}$$

where the Schmidt coefficients satisfy $\lambda_v \geqslant 0$ for all $v \in \mathrm{Rng}(V)$. Define the positive semidefinite operator $\tau' = \sum_v \lambda_v^2 |v\rangle\langle v|$, which describes the marginal state of either D or E according to $|\psi\rangle_{\mathsf{DE}}$ in Eq. (F2). Then we have

$$|\psi\rangle_{\mathsf{DE}} = \mathbb{1}_{\mathsf{D}} \otimes (\tau')^{1/2} \left(\sum_{v} |v\rangle_{\mathsf{D}} \otimes |v\rangle_{\mathsf{E}} \right). \quad \text{(F3)}$$

Now suppose that the measurement operators $\{\Pi_{ab|xy}\}_{abxy}$ in Eq. (F1) are represented in another orthonormal basis $\{|w\rangle_{\mathsf{D}}\}_{w \in \mathrm{Rng}(W)}$ of $\mathbb{C}^2 \otimes \mathbb{C}^2$ with $|\mathrm{Rng}(W)| = 4$. By the invariance of the (un-normalized) maximally entangled state $\sum_v |v\rangle_{\mathsf{D}} \otimes |v\rangle_{\mathsf{E}}$ under a unitary transformation, there exists a partial orthonormal basis $\{|w\rangle_{\mathsf{E}}\}_{w \in \mathrm{Rng}(W)}$ of $\mathcal{H}(\mathsf{E})$ such that $\sum_v |v\rangle_{\mathsf{D}} \otimes |v\rangle_{\mathsf{E}} = \sum_w |w\rangle_{\mathsf{D}} \otimes |w\rangle_{\mathsf{E}}$. Therefore, if the marginal state of D or E is τ in the basis $\{|w\rangle\}_{w \in W}$, then the state in Eq. (F3) can be written in the new basis as

$$|\psi\rangle_{\mathsf{DE}} = \mathbb{1}_{\mathsf{D}} \otimes \tau^{1/2} \left(\sum_{w} |w\rangle_{\mathsf{D}} \otimes |w\rangle_{\mathsf{E}} \right). \quad \text{(F4)}$$

We emphasize that in the above equation the state $|\psi\rangle_{\mathsf{DE}}$ is represented in a partial orthonormal basis $\{|w\rangle_{\mathsf{E}}\}_{w \in \mathrm{Rng}(W)}$ of $\mathcal{H}(\mathsf{E})$, which can be extended to a complete orthonormal basis of $\mathcal{H}(\mathsf{E})$ by an isometry U from $\mathbb{C}^2 \otimes \mathbb{C}^2$ to $\mathcal{H}(\mathsf{E})$. Then in the complete basis the state becomes

$$|\psi\rangle_{\mathsf{DE}} = \mathbb{1}_{\mathsf{D}} \otimes (U\tau^{1/2}) \left(\sum_{w} |w\rangle_{\mathsf{D}} \otimes |w\rangle_{\mathsf{E}} \right). \quad \text{(F5)}$$

Define $|\Phi\rangle_{\mathsf{DE}} = \sum_w |w\rangle_{\mathsf{D}} \otimes |w\rangle_{\mathsf{E}}$. By combining Eqs. (F1) and (F5), we get that for each xy,

$$\begin{aligned}\rho_{AB\mathsf{E}|xy} &= \sum_{ab} |ab\rangle\langle ab| \otimes \mathrm{tr}_{\mathsf{D}}((\mathbb{1}_{\mathsf{D}} \otimes (U\tau^{1/2}))|\Phi\rangle_{\mathsf{DE}}\langle\Phi| \\ &\quad \times (\mathbb{1}_{\mathsf{D}} \otimes (\tau^{1/2}U^\dagger))(\Pi_{ab|xy} \otimes \mathbb{1}_{\mathsf{E}})) \\ &= \sum_{ab} |ab\rangle\langle ab| \otimes ((U\tau^{1/2})\mathrm{tr}_{\mathsf{D}}(|\Phi\rangle_{\mathsf{DE}}\langle\Phi| \\ &\quad \times (\Pi_{ab|xy} \otimes \mathbb{1}_{\mathsf{E}}))(\tau^{1/2}U^\dagger)). \end{aligned} \tag{F6}$$

Since each $\Pi_{ab|xy}$ is a rank-1 projector, direct calculation shows that

$$\mathrm{tr}_{\mathsf{D}}(|\Phi\rangle_{\mathsf{DE}}\langle\Phi|(\Pi_{ab|xy} \otimes \mathbb{1}_{\mathsf{E}})) = (\Pi_{ab|xy})^T,$$

where for a matrix M the notation M^T denotes its transpose. Further, considering that each $\Pi_{ab|xy}$ is real and symmetric, the state in Eq. (F6) is simplified to the desired form in the statement of theorem 6 of the main text. ■

APPENDIX G: METHOD FOR QEF VERIFICATION

Let us first provide several observations, which help to simplify the QEF verification in Eq. (42) of the main text, as follows.

Observation 1. The function $W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, \tau)$ in Eq. (41) of the main text is a concave function of τ. This follows from the general fact that given a positive semidefinite operator $P \geqslant 0$, a square matrix H of the same dimension as P, and $\alpha \geqslant 1$, $\mathrm{tr}((H^\dagger P^{1/\alpha} H)^\alpha)$ is a concave function in P, see theorem 7.2 of Ref. [58]. Setting $H = H^\dagger = \Pi_{ab|xy}$ and $P = \tau$ we obtain the concavity in τ of $\mathrm{tr}((\Pi_{ab|xy}\tau^{1/\alpha}\Pi_{ab|xy})^\alpha)$, which is equal to $(\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}))^\alpha$ since $\Pi_{ab|xy}$ is a rank-1 projector and the trace is invariant under cyclic permutations. It follows that $W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, \tau)$ is a positive linear combination of concave functions of τ and is therefore itself concave.

Observation 2. Concavity in τ implies that the set of τ over which $W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, \tau)$ needs to be maximized can be restricted to real matrices. This follows from the equality $W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, \tau) = W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, \tau^\dagger)$, which is a consequence of the projector $\Pi_{ab|xy}$ being real. So, by concavity $W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, (\tau + \tau^\dagger)/2) \geqslant W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, \tau)$ with $(\tau + \tau^\dagger)/2$ being a real matrix.

Observation 3. The feasible region of each θ_{A} and θ_{B} in Eq. (42) can be restricted to $[0, \pi]$. Without loss of generality, consider the case of θ_{A}. Let the Pauli matrix $\sigma_{z,\mathsf{A}}$ act on the Hilbert space $\mathbb{C}^2$ held by A, and let $\mathbb{1}_{\mathsf{B}}$ be the identity operator on the Hilbert space $\mathbb{C}^2$ of B. We notice that $\sigma_{z,\mathsf{A}} Q_{x;-\theta_{\mathsf{A}}}(a)\sigma_{z,\mathsf{A}} = Q_{x;\theta_{\mathsf{A}}}(a)$ for all θ_{A}, x and a. Therefore

$$\begin{aligned}&\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}})) \\ &= \mathrm{tr}(\tau^{1/\alpha}(Q_{x;\theta_{\mathsf{A}}}(a) \otimes Q_{y;\theta_{\mathsf{B}}}(b))) \\ &= \mathrm{tr}(\tau^{1/\alpha}((\sigma_{z,\mathsf{A}}Q_{x;-\theta_{\mathsf{A}}}(a)\sigma_{z,\mathsf{A}}) \otimes Q_{y;\theta_{\mathsf{B}}}(b))) \\ &= \mathrm{tr}((\sigma_{z,\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}})\tau^{1/\alpha}(\sigma_{z,\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}})(Q_{x;-\theta_{\mathsf{A}}}(a) \otimes Q_{y;\theta_{\mathsf{B}}}(b))) \\ &= \mathrm{tr}(((\sigma_{z,\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}})\tau(\sigma_{z,\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}}))^{1/\alpha}(Q_{x;-\theta_{\mathsf{A}}}(a) \otimes Q_{y;\theta_{\mathsf{B}}}(b))), \end{aligned}$$

where to obtain the equality in the fourth line we used the community between $\sigma_{z,\mathsf{A}}$ and $Q_{y;\theta_{\mathsf{B}}}(b)$ and the invariance of the trace under cyclic permutations. Since the function that maps τ to $(\sigma_{z,\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}})\tau(\sigma_{z,\mathsf{A}} \otimes \mathbb{1}_{\mathsf{B}})$ is a bijection, the maximum over τ of the above expression does not change when θ_{A} is changed to $-\theta_{\mathsf{A}}$. It follows that for the optimization problem in Eq. (42) with the objective function expressed in Eq. (41) of the main text, if $\theta_{\mathsf{A}} \in (-\pi, 0)$, we can replace it with $\theta'_{\mathsf{A}} = -\theta_{\mathsf{A}}$ and at the same time keep the maximum f_k unchanged.

Now we can solve the QEF verification in Eq. (42) of the main text by two steps, which are summarized below and detailed in Appendices G 1 and G 2, respectively.

Step 1. We fix the values of θ_{A} and θ_{B} and solve the problem:

$$\begin{aligned} f_k(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}) \doteq \mathrm{Max}: &W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, \tau) \\ \text{Subject to: } &\tau \geqslant 0 \text{ and } \mathrm{tr}(\tau) = 1. \end{aligned} \tag{G1}$$

In view of observation 3, we only need to consider the fixed values of θ_{A} and θ_{B} in the interval $[0, \pi]$, and in view of observation 2, we can restrict the feasible region of τ to be the set $\mathcal{S}_1$ of real normalized states of dimension 4, which is a convex set. Furthermore, since the objective function $W_{F',\alpha,k}(\theta_{\mathsf{A}}, \theta_{\mathsf{B}}, \tau)$ is concave in τ (see observation 1), the problem in Eq. (G1) is a convex-optimization problem. We provide a method to obtain both upper and lower bounds on $f_k(\theta_{\mathsf{A}}, \theta_{\mathsf{B}})$ in Appendix G 1.

Step 2. Given the values of $f_k(\theta_{\mathsf{A}}, \theta_{\mathsf{B}})$ for a finite number of θ_{A} and θ_{B} sampled from the interval $[0, \pi]$, we provide a method in Appendix G 2 to bound $\max_{\theta_{\mathsf{A}},\theta_{\mathsf{B}}\in[0,\pi]} f_k(\theta_{\mathsf{A}}, \theta_{\mathsf{B}})$, which is equal to the maximum f_k of Eq. (42) in view of observation 3.

1. Upper and lower bounds of $f_k(\theta_{\mathsf{A}}, \theta_{\mathsf{B}})$

To simplify notation and clarify the function considered, in this section we denote the objective function of the optimization problem in Eq. (G1) by $W(\tau)$. The optimization problem considered becomes $\max_{\tau\in\mathcal{S}_1} W(\tau)$, where $\mathcal{S}_1$ is the set of real normalized states of dimension 4.

Given a real normalized state $\tau_0 \in \mathcal{S}_1$, let $\nabla W|_{\tau_0}$ be a gradient matrix of the function W at τ_0 satisfying that $W(\tau_0 + \epsilon\Delta) = W(\tau_0) + \epsilon\mathrm{tr}(\nabla W|_{\tau_0}\Delta) + o(\epsilon)$ for every Hermitian matrix Δ and an arbitrarily small parameter $\epsilon > 0$, where $o()$ is the little-o notation. We observe that $\nabla W|_{\tau_0}$ can be chosen to be a Hermitian matrix. To see this, suppose that $M \doteq \nabla W|_{\tau_0}$ is a complex but not Hermitian matrix. Then, as the function $W(\tau_0 + \epsilon\Delta)$ is real, so is $\mathrm{tr}(M\Delta)$ for every Hermitian matrix Δ. Moreover, $\mathrm{tr}(M^\dagger\Delta)$ is real, as it is equal to $\mathrm{tr}(M\Delta)$. Now we can set the gradient $\nabla W|_{\tau_0}$ to be $(M + M^\dagger)/2$, which is a Hermitian matrix. In a similar way, we can further choose $\nabla W|_{\tau_0}$ to be a real symmetric matrix.

Since the function $W(\tau)$ is concave, for any $\tau \geqslant 0$ we have $W(\tau) \leqslant W(\tau_0) + \mathrm{tr}(\nabla W|_{\tau_0}(\tau - \tau_0))$. Considering that the function W is positively homogeneous of degree 1 in τ, $\mathrm{tr}(\nabla W|_{\tau_0}\tau_0) = W(\tau_0)$. Therefore $W(\tau) \leqslant \mathrm{tr}(\nabla W|_{\tau_0}\tau)$. So we have $\max_{\tau\in\mathcal{S}_1} W(\tau) \leqslant \max_{\tau\in\mathcal{S}_1} \mathrm{tr}(\nabla W|_{\tau_0}\tau)$. As $\mathcal{S}_1$ is the set of all real normalized states of dimension 4 and $\nabla W|_{\tau_0}$ is a real symmetric matrix, $\max_{\tau\in\mathcal{S}_1} \mathrm{tr}(\nabla W|_{\tau_0}\tau) = \lambda_{\max}(\nabla W|_{\tau_0})$, where $\lambda_{\max}(\nabla W|_{\tau_0})$ is the maximal eigenvalue of the gradient matrix $\nabla W|_{\tau_0}$. As τ_0 is feasible, we also have $\max_{\tau\in\mathcal{S}_1} W(\tau) \geqslant W(\tau_0)$. Hence, any feasible solution τ_0 provides both an upper and a lower bound on $\max_{\tau\in\mathcal{S}_1} W(\tau)$.

It is desirable to make the upper and lower bounds as tight as possible. For this we use an iterative method. Given a feasible solution τ_0, we can apply line search to find another feasible solution τ_1 such that $W(\tau_1) \geqslant W(\tau_0)$ as follows. Let Π_0 be the projector onto the span of the eigenvectors of the gradient matrix $\nabla W|_{\tau_0}$ with eigenvalues larger than or equal to $W(\tau_0)$. Then, the line segment $L = \{(1-\epsilon)\tau_0 + \epsilon\Pi_0/\mathrm{tr}(\Pi_0) : 0 \leqslant \epsilon < 1\}$ constitutes a subset of feasible solutions. By line search, we can find $\tau_1 = \mathrm{argmax}_{\tau\in L} W(\tau)$. We thus have $W(\tau_1) \geqslant W(\tau_0)$. By iteration, we can obtain a sequence of feasible solutions $\{\tau_i : i = 0, 1, 2, \ldots\}$ such that $W(\tau_i) \leqslant W(\tau_{i+1})$ for all i. At each feasible solution, we have $W(\tau_i) \leqslant \max_{\tau\in\mathcal{S}_1} W(\tau) \leqslant \lambda_{\max}(\nabla W|_{\tau_i})$ following the argument of the above paragraph. We can stop the iteration as long as the gap between the least upper bound and the greatest lower bound obtained so far is smaller than a prespecified precision. We remark that the convergence of the obtained upper bounds $\{\lambda_{\max}(\nabla W|_{\tau_i}), i = 0, 1, 2, \ldots\}$ is not promised. However, we emphasize that a *certified but not necessarily tight* upper bound is sufficient for QEF verification.

In order to implement the above iterative method, we need to compute the gradient matrix ∇W. Considering the explicit expression of W as in Eq. (41) of the main text, it suffices to compute the gradients of functions in the form $W_\Pi(\tau) = (\mathrm{tr}(\tau^{1/\alpha}\Pi))^\alpha$, where Π is a rank-1 projector. We can write the gradient in the form

$$\nabla W_\Pi(\tau) = \alpha(\mathrm{tr}(\tau^{1/\alpha}\Pi))^\beta X, \tag{G2}$$

where $X \doteq \nabla \mathrm{tr}(\tau^{1/\alpha}\Pi)$. Note that if the initial solution τ_0 is positive definite (which is true as usual), so is each τ_i obtained by the iterative method. Therefore, for practical implementation, we only need to know the gradient ∇W_Π at arbitrary positive τ in $\mathcal{S}_1$. For this case, the matrix X is derived in Appendix H.

2. Upper and lower bounds of f_k

Recall that $f_k = \max_{\theta_\mathsf{A},\theta_\mathsf{B}\in[0,\pi]} f_k(\theta_\mathsf{A}, \theta_\mathsf{B})$. For each θ_A and θ_B, we can obtain both an upper and a lower bound on $f_k(\theta_\mathsf{A}, \theta_\mathsf{B})$. In order to bound f_k, we first solve the following problem: Given the values of $f_k(\theta_{\mathsf{A},i}, \theta_\mathsf{B})$ and $f_k(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B})$ with $\theta_{\mathsf{A},i}, \theta_{\mathsf{A},i+1}, \theta_\mathsf{B} \in [0, \pi]$ and $\theta_{\mathsf{A},i} < \theta_{\mathsf{A},i+1}$, compute bounds on $f_k(I_{\mathsf{A},i}, \theta_\mathsf{B}) \doteq \max_{\theta_\mathsf{A}\in I_{\mathsf{A},i}} f_k(\theta_\mathsf{A}, \theta_\mathsf{B})$ where $I_{\mathsf{A},i}$ denotes the interval $[\theta_{\mathsf{A},i}, \theta_{\mathsf{A},i+1}]$. A lower bound $\max(f_k(\theta_{\mathsf{A},i}, \theta_\mathsf{B}), f_k(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B}))$ is immediately available; while an upper bound can be derived from lemma 9 in Appendix I.

According to lemma 9, for all $\theta_\mathsf{A} \in I_{\mathsf{A},i}$ we have

$$f_k(\theta_\mathsf{A}, \theta_\mathsf{B}) \leqslant (\lambda f_k(\theta_{\mathsf{A},i}, \theta_\mathsf{B}) + (1-\lambda) f_k(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B}))/l^\alpha, \tag{G3}$$

where both l and λ depend on $\phi = \theta_{\mathsf{A},i+1} - \theta_{\mathsf{A},i}$ and $\varphi = \theta_\mathsf{A} - \theta_{\mathsf{A},i}$. The explicit expressions of l and λ are given in Eq. (I2). Since the upper bound in Eq. (G3) is an analytic function of ϕ and φ, whose maximum can be easily bounded from above. Consequently, we can obtain an upper bound on $f_k(I_{\mathsf{A},i}, \theta_\mathsf{B})$.

In the same way as above, given $\theta_\mathsf{A}, \theta_{\mathsf{B},j}, \theta_{\mathsf{B},j+1} \in [0, \pi]$ and $\theta_{\mathsf{B},j} < \theta_{\mathsf{B},j+1}$, for all $\theta_\mathsf{B} \in I_{\mathsf{B},j} \doteq [\theta_{\mathsf{B},j}, \theta_{\mathsf{B},j+1}]$, we have

$$f_k(\theta_\mathsf{A}, \theta_\mathsf{B}) \leqslant (\lambda f_k(\theta_\mathsf{A}, \theta_{\mathsf{B},j}) + (1-\lambda) f_k(\theta_\mathsf{A}, \theta_{\mathsf{B},j+1}))/l^\alpha, \tag{G4}$$

where l and λ are as given in Eq. (I2) with the replacement of $\phi = \theta_{\mathsf{B},j+1} - \theta_{\mathsf{B},j}$ and $\varphi = \theta_\mathsf{B} - \theta_{\mathsf{B},j}$. Since $f_k(\theta_\mathsf{A}, \theta_{\mathsf{B},j}) \leqslant f_k(I_{\mathsf{A},i}, \theta_{\mathsf{B},j})$, $f_k(\theta_\mathsf{A}, \theta_{\mathsf{B},j+1}) \leqslant f_k(I_{\mathsf{A},i}, \theta_{\mathsf{B},j+1})$ for all $\theta_\mathsf{A} \in I_{\mathsf{A},i}$ and $1 \geqslant \lambda \geqslant 0, l > 0$ [see Eq. (I2)], the inequality in Eq. (G4) implies

$$f_k(\theta_\mathsf{A}, \theta_\mathsf{B}) \leqslant (\lambda f_k(I_{\mathsf{A},i}, \theta_{\mathsf{B},j}) + (1-\lambda) f_k(I_{\mathsf{A},i}, \theta_{\mathsf{B},j+1}))/l^\alpha, \tag{G5}$$

for all $\theta_\mathsf{A} \in I_{\mathsf{A},i}$ and $\theta_\mathsf{B} \in I_{\mathsf{B},j}$. Hence we are able to bound the maximum $f_k(I_{\mathsf{A},i}, I_{\mathsf{B},j}) \doteq \max_{\theta_\mathsf{A}\in I_{\mathsf{A},i}, \theta_\mathsf{B}\in I_{\mathsf{B},j}} f_k(\theta_\mathsf{A}, \theta_\mathsf{B})$ from the above. As $f_k(I_{\mathsf{A},i}, I_{\mathsf{B},j})$ cannot be less than the largest of $f_k(\theta_\mathsf{A}, \theta_\mathsf{B})$ with $\theta_\mathsf{A} = \theta_{\mathsf{A},i}$ or $\theta_{\mathsf{A},i+1}$ and $\theta_\mathsf{B} = \theta_{\mathsf{B},j}$ or $\theta_{\mathsf{B},j+1}$, a lower bound is also available.

We can now determine bounds on f_k. Let $m \geqslant 2$ be a positive integer, and let $\theta_{\mathsf{A},i} = i\pi/m$ and $\theta_{\mathsf{B},j} = j\pi/m$ with $i, j = 0, 1, \ldots, m$. Denote the subregion $\{(\theta_\mathsf{A}, \theta_\mathsf{B}) : \theta_{\mathsf{A},i} \leqslant \theta_\mathsf{A} \leqslant \theta_{\mathsf{A},i+1}, \theta_{\mathsf{B},j} \leqslant \theta_\mathsf{B} \leqslant \theta_{\mathsf{B},j+1}\}$ by $I_{\mathsf{AB},ij}$ with $i, j = 0, 1, \ldots, (m-1)$. According to the results in the above paragraph, we can determine both an upper and a lower bound on $f_k(I_{\mathsf{AB},ij}) \doteq \max_{(\theta_\mathsf{A},\theta_\mathsf{B})\in I_{\mathsf{AB},ij}} f_k(\theta_\mathsf{A}, \theta_\mathsf{B})$ for each $I_{\mathsf{AB},ij}$. Suppose that $l_{k,ij} \leqslant f_k(I_{\mathsf{AB},ij}) \leqslant u_{k,ij}$. Since the union of the subregions $I_{\mathsf{AB},ij}$ with all ij is the feasible region of $(\theta_\mathsf{A}, \theta_\mathsf{B})$ (see observation 3), we have $f_k = \max_{ij} f_k(I_{\mathsf{AB},ij})$. Thus we have $\max_{ij} l_{k,ij} \leqslant f_k \leqslant \max_{ij} u_{k,ij}$.

We remark that m is a free parameter, characterizing the resolution in the division of the feasible region of $(\theta_\mathsf{A}, \theta_\mathsf{B})$. With the increase of m, we expect that the upper and lower bounds on f_k obtained converge. In our implementation of the above method, we start dividing the feasible region at a low resolution, and refine the subregions $I_{\mathsf{AB},ij}$ if the gap between the upper and lower bounds on f_k is too large. However, not all subregions $I_{\mathsf{AB},ij}$ need to be refined. We refine the subregions $I_{\mathsf{AB},ij}$ in the order of priority. The priority is determined by the obtained upper bounds $u_{k,ij}$ on $f_k(I_{\mathsf{AB},ij})$. The subregion $I_{\mathsf{AB},ij}$ with the highest upper bound $u_{k,ij}$ will be refined with the highest priority. A possible refinement strategy is to divide the region $I_{\mathsf{AB},ij}$ into four subregions. We determine the upper and lower bounds on each refined subregion. We then update both the upper and the lower bounds on f_k obtained so far. We continue the refinement until the gap between these two bounds is smaller than a prespecified precision.

APPENDIX H: DERIVATION OF THE MATRIX X IN EQ. (G2)

To compute X at $\tau > 0$, we use perturbation techniques. Let $\tau' = \tau + \epsilon\Delta$, where $\epsilon > 0$ is sufficiently small and Δ is a real symmetric matrix. The matrix τ can be decomposed in terms of its eigenspace projectors as $\tau = \sum_i \lambda_i \Lambda_i$, where $\lambda_i > 0$ and $\Lambda_i\Lambda_j = \Lambda_i\delta_{ij}$. Since $\sum_i \Lambda_i = \mathbb{1}$, we have

$$\Delta = \left(\sum_i \Lambda_i\right)\Delta\left(\sum_j \Lambda_j\right) = \sum_i \Delta_{ii} + \sum_{i\neq j} \Delta_{ij},$$

where $\Delta_{ij} = \Lambda_i\Delta\Lambda_j$ for all ij. By introducing $S = \sum_{i\neq j} S_{ij}$ with $S_{ij} = \Delta_{ij}/(\lambda_j - \lambda_i)$ and noting that $\tau\Lambda_i = \Lambda_i\tau = \lambda_i\Lambda_i$, we can write Δ as

$$\Delta = \sum_i \Delta_{ii} + [S, \tau]. \tag{H1}$$

One can see that the support of Δ_{ii} is in Λ_i and S is skew-symmetric (that is, $S^T = -S$) with $\Lambda_i S \Lambda_i = 0$ for each i.

Let $U = e^{\epsilon S}$. Since S is skew-symmetric, we have $U^T U = e^{\epsilon S^T} e^{\epsilon S} = \mathbb{1}$. That is, $U = e^{\epsilon S}$ is orthogonal. Therefore, for any $\gamma > 0$ and any $\rho \geqslant 0$, we have

$$(U \rho U^T)^\gamma = U \rho^\gamma U^T. \tag{H2}$$

Moreover, we claim that

$$\begin{aligned} &U \left(\tau + \sum_i \epsilon \Delta_{ii} \right)^\gamma U^T \\ &\quad = \tau^\gamma + \epsilon \gamma \tau^{\gamma-1} \left(\sum_i \Delta_{ii} \right) + \epsilon [S, \tau^\gamma] + O(\epsilon^2), \end{aligned} \tag{H3}$$

where $\gamma > 0$ and $O()$ is the big-O notation.

To prove the equality in Eq. (H3), we first set $Y = \sum_i \Delta_{ii}$, and note that Y and τ commute with each other. So, Y can be written as $Y = \sum_i y_i \Lambda_i$, and

$$\begin{aligned} &(\tau + \epsilon Y)^\gamma \\ &\quad = \left(\sum_i (\lambda_i + \epsilon y_i) \Lambda_i \right)^\gamma \\ &\quad = \sum_i (\lambda_i + \epsilon y_i)^\gamma \Lambda_i \\ &\quad = \sum_i \left(\lambda_i^\gamma + \epsilon \gamma \lambda_i^{\gamma-1} y_i + O(\epsilon^2) \right) \Lambda_i \\ &\quad = \tau^\gamma + \epsilon \gamma \tau^{\gamma-1} Y + O(\epsilon^2), \end{aligned} \tag{H4}$$

where for the equalities in the third and last lines we used the orthonormality conditions $\Lambda_i \Lambda_j = \Lambda_i \delta_{ij}$, and for the equality in the forth line we used the fact that all $\lambda_i > 0$ and the Taylor-series approximation of $(\lambda_i + \epsilon y_i)^\gamma$. Second, we combine Eq. (H4) with the Taylor-series approximation $U = e^{\epsilon S} = \mathbb{1} + \epsilon S + O(\epsilon^2)$. Then considering that $S^T = -S$, direct calculation establishes the desired equality in Eq. (H3).

Now we obtain

$$\begin{aligned} &(\tau + \epsilon \Delta)^{1/\alpha} \\ &\quad = \left(\tau + \sum_i \epsilon \Delta_{ii} + \epsilon [S, \tau] \right)^{1/\alpha} \\ &\quad = \left(U \left(\tau + \sum_i \epsilon \Delta_{ii} \right) U^T + O(\epsilon^2) \right)^{1/\alpha} \\ &\quad = \left(U \left(\tau + \sum_i \epsilon \Delta_{ii} + O(\epsilon^2) \right) U^T \right)^{1/\alpha} \\ &\quad = U \left(\tau + \sum_i \epsilon \Delta_{ii} + O(\epsilon^2) \right)^{1/\alpha} U^T \\ &\quad = U \left(\left(\tau + \sum_i \epsilon \Delta_{ii} \right)^{1/\alpha} + O(\epsilon^2) \right) U^T \\ &\quad = \tau^{1/\alpha} + \epsilon \frac{1}{\alpha} \tau^{-\beta/\alpha} \left(\sum_i \Delta_{ii} \right) + \epsilon [S, \tau^{1/\alpha}] + O(\epsilon^2). \end{aligned} \tag{H5}$$

Here, for the equality in the second line, we used Eq. (H1), for the equality in the third line we used Eq. (H3) with $\gamma = 1$, for the equality in the fifth line we used Eq. (H2) with $\gamma = 1/\alpha$, and for the equality in the last line we used Eq. (H3) with $\gamma = 1/\alpha$.

With the decomposition $\tau = \sum_i \lambda_i \Lambda_i$ and the orthogonality relations $\Lambda_i \Lambda_j = \Lambda_i \delta_{ij}$ and $\Lambda_i \Delta_{jj} = \Delta_{jj} \delta_{ij}$, we have

$$\tau^{-\beta/\alpha} \Delta_{ii} = \lambda_i^{-\beta/\alpha} \Delta_{ii}. \tag{H6}$$

Further, considering that $S = \sum_{i \neq j} \Delta_{ij} / (\lambda_j - \lambda_i)$, $\Delta_{ij} \Lambda_k = \Delta_{ij} \delta_{kj}$ and $\Lambda_k \Delta_{ij} = \Delta_{ij} \delta_{ki}$ we get

$$[S, \tau^{1/\alpha}] = \sum_{i \neq j} \frac{\lambda_j^{1/\alpha} - \lambda_i^{1/\alpha}}{\lambda_j - \lambda_i} \Delta_{ij}. \tag{H7}$$

By Eqs. (H6) and (H7) and the expressions $\Delta_{ij} = \Lambda_i \Delta \Lambda_j$ for all ij, Eq. (H5) becomes

$$\begin{aligned} &(\tau + \epsilon \Delta)^{1/\alpha} - \tau^{1/\alpha} \\ &\quad = \epsilon \left(\sum_i \frac{1}{\alpha} \lambda_i^{-\beta/\alpha} \Lambda_i \Delta \Lambda_i + \sum_{i \neq j} \frac{\lambda_j^{1/\alpha} - \lambda_i^{1/\alpha}}{\lambda_j - \lambda_i} \Lambda_i \Delta \Lambda_j \right) \\ &\qquad + O(\epsilon^2). \end{aligned} \tag{H8}$$

By Eq. (H8) and the invariance of the trace under cyclic permutations, direct calculation shows that

$$\begin{aligned} &\mathrm{tr}((\tau + \epsilon \Delta)^{1/\alpha} \Pi) - \mathrm{tr}(\tau^{1/\alpha} \Pi) \\ &\quad = \epsilon \mathrm{tr} \left(\left(\sum_i \frac{\lambda_i^{-\beta/\alpha}}{\alpha} \Pi_{ii} + \sum_{i \neq j} \frac{\lambda_j^{1/\alpha} - \lambda_i^{1/\alpha}}{\lambda_j - \lambda_i} \Pi_{ji} \right) \Delta \right) \\ &\qquad + O(\epsilon^2), \end{aligned}$$

where $\Pi_{ij} \doteq \Lambda_i \Pi \Lambda_j$ for all ij. With this equation and the definition of the gradient, we can determine that X in Eq. (G2) is given by

$$X = \sum_i \frac{\lambda_i^{-\beta/\alpha}}{\alpha} \Pi_{ii} + \sum_{i \neq j} \frac{\lambda_j^{1/\alpha} - \lambda_i^{1/\alpha}}{\lambda_j - \lambda_i} \Pi_{ji}. \tag{H9}$$

One can check that X is a real symmetric matrix (as Π is real and symmetric).

We remark that the limit of $(\lambda_j^{1/\alpha} - \lambda_i^{1/\alpha})/(\lambda_j - \lambda_i)$ as $\lambda_j \to \lambda_i$ is $\lambda_i^{-\beta/\alpha}/\alpha$, so the potentially problematic terms for near-degenerate eigenvalues can be stably computed. The simplest way to avoid precision problems with the expression of Eq. (H9) is to always collapse near-degenerate eigenvalues of τ, where λ_i and λ_j should be considered near-degenerate if $|\lambda_i^{1/\alpha} - \lambda_j^{1/\alpha}| \leqslant \sqrt{\delta}$ with δ being the machine precision. That is, we replace τ by $\tilde{\tau}$ where $\tilde{\tau}$ is derived from τ with near-degenerate eigenvalues collapsed and rescaled to satisfy the constraint $\mathrm{tr}(\tilde{\tau}) = 1$. Then with $\tilde{\tau}$ instead of τ, we implement the iterative method.

APPENDIX I: A LEMMA USED IN APPENDIX G 2

Let $f_k(\theta_\mathsf{A}, \theta_\mathsf{B})$ be the maximum of the optimization problem in Eq. (G1). Given $f_k(\theta_{\mathsf{A},i}, \theta_\mathsf{B})$ and $f_k(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B})$ with $\theta_{\mathsf{A},i} < \theta_{\mathsf{A},i+1}$ and $\theta_{\mathsf{A},i}, \theta_{\mathsf{A},i+1}, \theta_\mathsf{B} \in [0, \pi]$, the next lemma provides an upper bound on $f_k(\theta_\mathsf{A}, \theta_\mathsf{B})$ for all $\theta_\mathsf{A} \in [\theta_{\mathsf{A},i}, \theta_{\mathsf{A},i+1}]$. Below we write $\phi = \theta_{\mathsf{A},i+1} - \theta_{\mathsf{A},i}$ and $\varphi = \theta_\mathsf{A} - \theta_{\mathsf{A},i}$.

Lemma 9. For all $\theta_\mathsf{A} \in [\theta_{\mathsf{A},i}, \theta_{\mathsf{A},i+1}]$, we have

$$f_k(\theta_\mathsf{A}, \theta_\mathsf{B}) \leqslant \big(\lambda f_k(\theta_{\mathsf{A},i}, \theta_\mathsf{B}) + (1-\lambda) f_k(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B})\big)/l^\alpha, \tag{I1}$$

where

$$l = \frac{\sin(\phi)}{\sin(\varphi) + \sin(\phi - \varphi)} \in (0, 1],$$
$$\lambda = \frac{\sin(\phi - \varphi)}{\sin(\varphi) + \sin(\phi - \varphi)} \in [0, 1]. \tag{I2}$$

Proof. Let $\vec{n} = (\cos(\theta_\mathsf{A}), \sin(\theta_\mathsf{A}))$, $\vec{n}_i = (\cos(\theta_{\mathsf{A},i}), \sin(\theta_{\mathsf{A},i}))$, $\vec{n}_{i+1} = (\cos(\theta_{\mathsf{A},i+1}), \sin(\theta_{\mathsf{A},i+1}))$, and $\vec{\sigma} = (\sigma_z, \sigma_x)$. We observe that $\lambda\vec{n}_i + (1-\lambda)\vec{n}_{i+1} = l\vec{n}$, where λ and l are given in Eq. (I2). Thus $\lambda\vec{\sigma}\cdot\vec{n}_i + (1-\lambda)\vec{\sigma}\cdot\vec{n}_{i+1} = l\vec{\sigma}\cdot\vec{n}$. This implies the operator inequality

$$Q_{x;\theta_\mathsf{A}}(a) \leqslant \big(\lambda Q_{x;\theta_{\mathsf{A},i}}(a) + (1-\lambda) Q_{x;\theta_{\mathsf{A},i+1}}(a)\big)/l, \tag{I3}$$

for all $a \in \{0, 1\}$ in the case of $x = 1$, where the operators $Q_{x;\theta}(a)$ with $x = 0, 1$ and $a = 0, 1$ are defined in Eq. (36) of the main text. Note that the above operator inequality also holds for the case of $x = 0$, as in this case $Q_{x;\theta_\mathsf{A}}(a)$ is independent of θ_A and $l \in (0, 1]$.

Considering the expression of the rank-1 projector $\Pi_{ab|xy}(\theta_\mathsf{A}, \theta_\mathsf{B})$ as in the statement of theorem 6 of the main text, the operator inequality in Eq. (I3) extends to

$$\Pi_{ab|xy}(\theta_\mathsf{A}, \theta_\mathsf{B}) \leqslant (\lambda\Pi_{ab|xy}(\theta_{\mathsf{A},i}, \theta_\mathsf{B}) + (1-\lambda)\Pi_{ab|xy}(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B}))/l,$$

for each $abxy$. So, for any $\tau \geqslant 0$ and $\alpha > 1$, we have $\tau^{1/\alpha} \geqslant 0$ and

$$\begin{aligned}\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}(\theta_\mathsf{A}, \theta_\mathsf{B})) &\leqslant \lambda\,\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}(\theta_{\mathsf{A},i}, \theta_\mathsf{B})/l) \\ &\quad + (1-\lambda)\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B})/l).\end{aligned}$$

Since the function $g(x) = x^\alpha$ with $x \geqslant 0$ and $\alpha > 1$ is monotonically increasing and convex, the above inequality implies

$$\begin{aligned}(\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}(\theta_\mathsf{A}, \theta_\mathsf{B})))^\alpha &\leqslant \lambda(\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}(\theta_{\mathsf{A},i}, \theta_\mathsf{B})/l))^\alpha \\ &\quad + (1-\lambda)(\mathrm{tr}(\tau^{1/\alpha}\Pi_{ab|xy}(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B})/l))^\alpha,\end{aligned} \tag{I4}$$

for each $abxy$.

Considering the definition of $W_{F',\alpha,k}(\theta_\mathsf{A}, \theta_\mathsf{B}, \tau)$ in Eq. (41) of the main text and that all coefficients $F'(abxy)\mu_k(xy)$ in Eq. (41) are non-negative, it follows from the inequality in Eq. (I4) that

$$W_{F',\alpha,k}(\theta_\mathsf{A}, \theta_\mathsf{B}, \tau) \leqslant \big(\lambda W_{F',\alpha,k}(\theta_{\mathsf{A},i}, \theta_\mathsf{B}, \tau) + (1-\lambda) W_{F',\alpha,k}(\theta_{\mathsf{A},i+1}, \theta_\mathsf{B}, \tau)\big)/l^\alpha.$$

Hence, the maximum of the optimization problem in Eq. (G1) satisfies the bound stated in the lemma. ■

[1] B. Hayes, Randomness as a resource, Am. Sci. **89**, 300 (2001).

[2] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2006.

[3] S. Pironio, A. Acin, 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).

[4] R. Colbeck and A. Kent, Private randomness expansion with untrusted devices, J. Phys. A: Math. Theor. **44**, 095305 (2011).

[5] U. Vazirani and T. Vidick, Certifiable quantum dice - or, exponential randomness expansion, in *STOC'12 Proceedings of the 44th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2012), p. 61.

[6] S. Pironio and S. Massar, Security of practical private randomness generation, Phys. Rev. A **87**, 012336 (2013).

[7] S. Fehr, R. Gelles, and C. Schaffner, Security and composability of randomness expansion from Bell inequalities, Phys. Rev. A **87**, 012335 (2013).

[8] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, in *STOC '14 Proceedings of the 46th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2014), pp. 417–426.

[9] C. A. Miller and Y. Shi, Universal security for randomness expansion from the spot-checking protocol, SIAM J. Comput. **46**, 1304 (2017).

[10] M. Coudron and H. Yuen, Infinite randomness expansion with a constant number of devices, in *STOC'14 Proceedings of the 46th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2014), pp. 427–36.

[11] K.-M. Chung, Y. Shi, and X. Wu, Physical randomness extractors: Generating random numbers with minimal assumptions, arXiv:1402.4797 [quant-ph].

[12] O. Nieto-Silleras, C. Bamps, J. Silman, and S. Pironio, Device-independent randomness generation from several Bell estimators, New J. Phys. **20**, 023049 (2018).

[13] 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).

[14] F. Dupuis and O. Fawzi, Entropy accumulation with improved second-order, IEEE Trans. Inf. Th. **65**, 7596 (2019).

[15] P. J. Brown, S. Ragy, and R. Colbeck, An adaptive framework for quantum-secure device-independent randomness expansion, arXiv:1810.13346.

[16] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R.

Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 km, Nature (London) **526**, 682 (2015).

[17] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, Event-Ready Bell-Test Using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes, Phys. Rev. Lett. **119**, 010402 (2017).

[18] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Åke Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015).

[19] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).

[20] M.-H. Li, C. Wu, Y. Zhang, W.-Z. Liu, B. Bai, Y. Liu, W. Zhang, Q. Zhao, H. Li, Z. Wang, L. You, W. J. Munro, J. Yin, J. Zhang, C.-Z. Peng, X. Ma, Q. Zhang, J. Fan, and J.-W. Pan, Test of Local Realism Into the Past without Detection and Locality Loopholes, Phys. Rev. Lett. **121**, 080404 (2018).

[21] P. Bierhorst, E. Knill, S. Glancy, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, and L. K. Shalm, Experimentally generated random numbers certified by the impossibility of superluminal signaling (version 1), arXiv:1702.05178v1.

[22] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Experimentally generated random numbers certified by the impossibility of superluminal signaling, Nature (London) **556**, 223 (2018).

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

[24] M. J. Fischer, A public randomness service, in *SECRYPT 2011* (SciTe Press, Seville, Spain, 2011), pp. 434–438.

[25] E. Knill, Y. Zhang, and P. Bierhorst, Quantum randomness from probability estimation with classical side information, arXiv:1709.06159.

[26] Y. Zhang, E. Knill, and P. Bierhorst, Certifying quantum randomness by probability estimation, Phys. Rev. A **98**, 040304(R) (2018).

[27] R. König, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Th. **55**, 4337 (2009).

[28] M. Tomamichel, *Quantum Information Processing with Finite Resources - Mathematical Foundations*, Springer Briefs in Mathematical Physics (Springer, Verlag, 2016) (specific citations are for arXiv:1504.00233 version 3, note that definitions, lemmas, propositions, etc. are independently numbered).

[29] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, arXiv:1607.01796 (specific citations are for version 1).

[30] A. Acin, S. Massar, and S. Pironio, Randomness Versus Nonlocality and Entanglement, Phys. Rev. Lett. **108**, 100402 (2012).

[31] 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).

[32] S. Popescu and D. Rohrlich, Quantum nonlocality as an axiom, Found. Phys. **24**, 379 (1994).

[33] 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).

[34] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, On quantum Rényi entropies: A new generalization and some properties, J. Math. Phys. **54**, 122203 (2013).

[35] M. M. Wilde, A. Winter, and D. Yang, Strong converse for the classical capacity of entanglement-breaking and hadamard channels via a sandwiched Rényi relative entropy, Commun. Math. Phys. **331**, 593 (2014).

[36] Y. Zhang, S. Glancy, and E. Knill, Asymptotically optimal data analysis for rejecting local realism, Phys. Rev. A **84**, 062118 (2011).

[37] M. Tomamichel, A framework for non-asymptotic quantum information theory, Ph.D. thesis, ETH, Zürich, Switzerland, 2012 (specific citations are for arXiv:1203.2142 version 2, note that definitions, lemmas, propositions, etc. are independently numbered).

[38] L. Trevisan, Extractors and pseudorandom generators, J. ACM **48**, 860 (2001).

[39] A. De, C. Portmann, T. Vidick, and R. Renner, Trevisan's extractor in the presence of quantum side information, SIAM J. Comput. **41**, 915 (2012).

[40] W. Mauerer, C. Portmann, and V. B. Scholz, A modular framework for randomness extraction based on Trevisan's construction, arXiv:1212.0520, code available on `github`.

[41] R. Arnon-Friedman, R. Renner, and T. Vidick, Simple and tight device-independent security proofs, SIAM J. Comput. **48**, 181 (2019).

[42] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Structure of states which satisfy strong subadditivity of quantum entropy with equality, Comm. Math. Phys. **246**, 359 (2004).

[43] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink, and E. Knill, Experimental Low-Latency Device-Independent Quantum Randomness, Phys. Rev. Lett. **124**, 010505 (2020).

[44] E. Knill, Y. Zhang, and H. Fu, Quantum probability estimation for randomness with quantum side information, arXiv:1806.04553.

[45] M. Tomamichel, R. Colbeck, and R. Renner, The fully quantum asymptotic equipartition property, IEEE Trans. Inf. Theory **55**, 5840 (2009).

[46] L. Masanes, Asymptotic Violation of Bell Inequalities and Distillability, Phys. Rev. Lett. **97**, 050503 (2006).

[47] B. Tsirelson, Some results and problems on quantum Bell-type inequalities, Hadronic J. Suppl. **8**, 329 (1993).

[48] 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).

[49] B. S. Cirelśon, Quantum generalizations of Bell's inequality, Lett. Math. Phys. **4**, 93 (1980).

[50] P. H. Eberhard, Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment, Phys. Rev. A **47**, R747 (1993).

[51] W. van Dam, R. D. Gill, and P. D. Grunwald, The statistical strength of nonlocality proofs, IEEE Trans. Inf. Theory. **51**, 2812 (2005).

[52] Y. Zhang, E. Knill, and S. Glancy, Statistical strength of experiments to reject local realism with photon pairs and inefficient detectors, Phys. Rev. A **81**, 032117 (2010).

[53] R. Renner, Security of quantum key distribution, Ph.D. thesis, ETH, Zürich, Switzerland, 2005 (available as arXiv:quant-ph/0512258 version 2).

[54] J. Barrett, R. Colbeck, and A. Kent, Memory Attacks on Device-Independent Quantum Cryptography, Phys. Rev. Lett. **110**, 010503 (2013).

[55] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).

[56] R. L. Frank and E. H. Lieb, Monotonicity of a relative Rényi entropy, J. Math. Phys. **54**, 122201 (2013).

[57] S. Beigi, Sandwiche Rényi divergence satisfies data processing inequality, J. Math. Phys **54**, 122202 (2013).

[58] E. A. Carlen, Trace inequalities and quantum entropy: An introductory course, in *Entropy and the Quantum*, Contemporary Mathematics Vol. 529 (American Mathematical Society, Providence, RI, 2010), pp. 73–140.