More entropy from shorter experiments using polytope approximations to the quantum set

Hyejung H. Jee*[1], Florian J. Curchod[2], and Mafalda L. Almeida**[2]

[1]Quantinuum, Partnership House, Carlisle Place, London SW1P 1BX, UK
[2]Quantinuum, Terrington House, 13–15 Hills Road, Cambridge CB2 1NL, UK

arXiv:2506.09555v4 [quant-ph] 4 Mar 2026

We introduce a systematic method for constructing polytope approximations to the quantum set in a variety of device-independent quantum random number generation (DI-QRNG) protocols. Our approach relies on two general-purpose algorithms that iteratively refine an initial outer-polytope approximation, guided by typical device behaviour and cryptographic intuition. These refinements strike a balance between computational tractability and approximation effectiveness. By integrating these approximations into the probability estimation (PE) framework [Zhang et al., PRA 2018], we obtain significantly improved certified entropy bounds in the finite-size regime. We test our method on various bipartite and tripartite DI-QRNG protocols, using both simulated and experimental data. In all cases, it yields notably higher entropy rates with fewer device uses than the existing techniques. We further extend our analysis to the more demanding task of randomness amplification, demonstrating major performance gains without added complexity. These results offer an effective and ready-to-use method to prove security—with improved certified entropy rates—in the most common practical DI-QRNG protocols. Our algorithms and entropy certification with PE tools are publicly available under a non-commercial license at `https://github.com/CQCL/PE_polytope_approximation`.

1 Introduction

Device-independent randomness certification is among the key achievements of quantum cryptography. By making security claims that rely minimally on hardware characterisation, this approach enables random number generators that are secure against computationally unbounded adversaries, while minimising the risk of mismatches between the theoretical model and practical implementation. This is achieved by repeatedly challenging a quantum device and analysing its responses in what is called a multi-prover interactive proof system. The price for this uplift in security is (i) having to build more complex, expensive and/or slower devices and (ii) observing a fall in the rate of entropy generation. As a consequence, the design of DI-QRNG protocols should pay particular attention to maximising the amount of certified randomness per device use. A related requirement is to minimise the number of device uses needed to obtain a positive rate of certified entropy. Indeed, for most applications (imperfect) raw output entropy goes through randomness extraction

Hyejung H. Jee*: hailey.jee@quantinuum.com
Mafalda L. Almeida**: mafalda.almeida@quantinuum.com

algorithms which are demanding in computational resources, both in time and memory. In order to avoid this post-processing bottleneck[1]—that easily becomes a roadblock in practical applications—one needs to minimise the input size of these algorithms and thus minimise the number of device uses, n, in the protocol.

Standard techniques for lower-bounding the output entropy in DI protocols include the method described in [3–5] for quantum adversaries classically correlated with the device and the entropy accumulation theorem (EAT) introduced in [6] for quantum side information. Note that although classical side information is a well-justified assumption in QRNG protocols (see e.g. [4]), assuming quantum side information is necessary for most quantum key distribution (QKD) protocols. While these techniques are proven to be optimal in the asymptotic limit of very large n, their performance deteriorates significantly in the finite-size regime compatible with real-world applications. This limitation is addressed by the probability estimation (PE) framework for classical side information [7, 8], which derives entropy bounds optimised for a given finite n.

Despite considerable success in improving the finite-size performance of several DI-QRNG implementations [7–9], a limitation of the PE technique is that it requires an optimisation to be performed over sets of allowed behaviours that must be described by convex polytopes. Allowed behaviours are any device input-output probability distributions compatible with a quantum realisation (through the Born rule) and, in the case of DI-QRNG protocols proposed so far, with the device being composed of separated non-communicating components where measurements take place. Given that quantum theory imposes non-linear constraints in this setup, any practical applications of the PE framework require polytope approximations that contain the (non-polytope) convex set of quantum behaviours.

Finding good polytope approximations, however, remains a significant challenge. On one hand, coarse outer-approximations to the quantum set tend to greatly overestimate the strategies available to an adversary, leading to unnecessarily weak entropy bounds. On the other hand, achieving fine-grained approximations in the high-dimensional spaces that characterise these sets quickly becomes computationally intractable. So far, only basic approximations in the simplest Bell scenario[2] have been proposed: in [7, 8], the authors consider the polytope defined by the subset of non-signalling behaviours satisfying Tsirelson's bound for CHSH (i.e., that do not exceed its maximum quantum violation); while in [10] the authors go a step further by excluding from this polytope all the behaviours violating a chosen asymmetric CHSH inequality [11] above its quantum bound.

1.1 Contributions

Our main contribution is to introduce a systematic method for constructing polytope approximations to the quantum set across a variety of DI-QRNG setups. To this end, we propose two general-purpose algorithms that balance computational tractability and approximation effectiveness. The key lies in designing the polytopes based both on the typical behaviour of the device, and on educated guesses of possible adversarial strategies.

More precisely, our approach begins with any initial polytope that contains the quantum set and proceeds iteratively by removing exclusively non-quantum regions of this polytope. As a result, we construct a sequence of polytopes that approximate the quantum set with

[1] For an excellent discussion of this bottleneck refer to, e.g., Appendix E.C of [1] or the concrete examples in Section 5 of [2].

[2] The so-called CHSH scenario, consisting of two non-communicating devices with two measurement choices and outputs each.

increasing accuracy. Since the complexity of computing successive approximations grows rapidly, our algorithms carefully select the non-quantum behaviours that significantly contribute to the adversary's guessing power. This is achieved by identifying suitable quantum Bell inequalities according to the typical behaviour of the device and cryptographic intuition about potential adversarial strategies. We identify two effective strategies, each giving rise to a different polytope approximation algorithm.

We illustrate the performance of our approach by integrating it with the PE framework to derive new certified entropy bounds for a variety of practical DI-QRNG protocols. For this purpose, we consider setups based on bipartite and tripartite Bell tests involving two dichotomic observables per party. We analyse both theoretical noisy behaviours that resemble those that could be obtained in experimental implementations, as well as data from real-world loophole-free CHSH-Bell tests. In all cases studied, our method yields significantly higher entropy bounds with fewer device uses compared to previous analyses.

In addition to standard protocols where the inputs are independent of the devices (e.g., randomness expansion or QKD), we apply our method to a bipartite scenario in which the device's internal state may be correlated with the inputs, typically referred to as randomness amplification protocols. These are particularly challenging to analyse, which often leads to suboptimal entropy rates. Nonetheless, we demonstrate through examples that—with no more effort than required for protocols assuming independent sources—our method achieves improvements of several orders of magnitude over existing alternatives.

Our construction can readily be applied to any practical DI-QRNG (based on bi- or tripartite Bell tests with two inputs and outputs per party), providing optimised entropy rates in the finite n regime. To this end, we provide a software implementation (in Python) of both our algorithms for polytope approximations and to obtain entropy bounds using the PE framework. The codes are available at `https://github.com/CQCL/PE_polytope_approximation`.

Although we have not tested the effectiveness of the polytope approximations for protocols with more parties, our ideas extend to these more complex scenarios. A similar approach could be considered for semi-DI-QRNGs where the set of allowed behaviours can be bounded using semidefinite constraints (see [12] for a survey).

This paper is structured as follows. In section 2 we provide a concise overview of DI entropy certification protocols and the PE framework, along with a description of how this can be applied in practice. In Section 3, we describe our algorithms for constructing polytope approximations to the set of quantum correlations. This section is self-contained and may be of independent interest. Section 4 showcases our technique across a variety of DI-QRNG scenarios. Finally, we present our conclusions in Section 5.

2 The PE framework

The probability estimation framework for randomness certification with classical side information was introduced by Zhang et al. [7] and a more thorough description of the framework can be found in the follow-up paper [8]. The goal of this section is to provide a summary of the essential steps of the construction along with some simplified proofs.

2.1 Protocol basics and notation

Consider a user who can query a physical device that takes inputs represented by a random variable Z and returns outputs C. Over an n-round protocol, the sequences of inputs

and outputs are described by $\mathbf{Z} = Z_1 \dots Z_n$ and $\mathbf{C} = C_1 \dots C_n$, respectively. The user is interested in lower-bounding the uncertainty in $\mathbf{C}$ from the perspective of a computationally unbounded adversary ('Eve'), having access to a complete description of the device and holding classical correlations E with it. The random variables $\mathbf{CZ}E$ of the process follow some distribution μ. Although the adversary's side information could be represented by the sequence $E_1, \dots, E_n$, here we consider that all this information is merged into a single random variable E available to the adversary before the protocol starts. While in most cases this implies an overestimation of Eve's information, it allows the n-round behaviour of the device to be conditioned on a fixed realisation $E = e$, which considerably simplifies the security analysis.

Inputs $\mathbf{Z}$ may be public, meaning that they can be known to Eve once generated, and follow a distribution $\mu(\mathbf{Z}|e)$ known to Eve. Inputs Z_i are not required to be independent amongst themselves or even from the quantum device, given that they satisfy the Markov condition:

$$\mu(Z_{i+1}|\mathbf{C}_{\leq i}, \mathbf{Z}_{\leq i}, e) = \mu(Z_{i+1}|\mathbf{Z}_{\leq i}, e)\,, \qquad \forall i\,. \tag{1}$$

This is essential to prevent information on past outputs $\mathbf{C}_{\leq i} = C_1 \dots C_i$ from being leaked through inputs Z_{i+1} for any e.

To certify entropy in the demanding DI scenario where the user sees the device as a black-box—i.e., can only rely on its input-output statistics—the setup must incorporate physical constraints that limit the set of allowed behaviours $\mu(\mathbf{C}, \mathbf{Z}|e)$. In this context, we consider the standard scenario of a physical device composed of separate, non-communicating sub-units, whose non-communicating nature can be verified without accessing their internal mechanisms. This structure enables the user to identify a set $\mathcal{S}$ of allowed behaviours $\mu(C_i Z_i|e)$ at each round i. Take for instance the simplest protocols considered here, based on a bipartite Bell scenario where the physical device is composed of two non-communicating units, A and B, with inputs $Z = XY$ and outputs $C = AB$. As a result, any allowed distributions $\mu(A_i B_i X_i Y_i|e)$ must be non-signalling [13], i.e. $\mu(A_i|X_i Y_i e) = \mu(A_i|X_i e)$ and $\mu(B_i|X_i Y_i e) = \mu(B_i|Y_i e)$.

Given our focus on practical applications, the set of allowed behaviours is further constrained by quantum theory—specifically, any $\mu(C, Z|e)$ must be compatible with a quantum realisation. This means that conditional behaviours $\mu(C|Z, e)$ must be describable by Born's rule; that is, $\mu(C|Z, e) = \mathrm{tr}\left(\rho M_C^Z\right)$, where the quantum state ρ is a positive semi-definite Hermitian operator with unit trace, acting on the Hilbert space $\mathcal{H}$ of the system. The measurement operators M_C^Z may be taken as projectors on $\mathcal{H}$, satisfying $\sum_c M_c^Z = \mathbb{1}$. In the bipartite example—comprising two non-communicating sub-units—the measurement operators take the form of operators $M_A^X \otimes M_B^Y$ acting on $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$.

The PE framework allows us to lower-bound the entropy of $\mathbf{C} = C_1 \dots C_n$, or more generally any sequence $\mathbf{D} = D_1 \dots D_n$ where each D_i is determined by the raw output C_i [3]. In particular, it shows how to design entropy witnesses $W(\mathbf{c}, \mathbf{z})$ that are used to check if $\mathbf{D}$ has entropy above a certain threshold (see Figure 1), from the point of view of an adversary knowing the inputs $\mathbf{z}$ and the side information e. In this scheme, both the witness and its threshold are defined prior to the entropy certification stage and should be optimised for the *typical behaviour* of the device. This behaviour can be estimated by querying the device over many rounds during a characterisation step taking place before the entropy certification stage (the latter is depicted in Figure 1). If desired, the witness can be redesigned in subsequent runs taking into account the observed behaviour over

[3] For instance, in the bipartite Bell scenario we could be interested in the output entropy of a single party, say A, implying setting $D = A$.

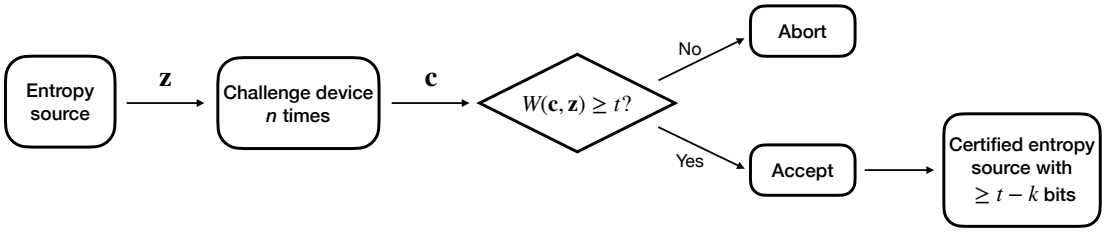


Figure 1: **Schematic of DI randomness certification protocol**. An entropy source $\mathbf{Z}$ is used to sequentially challenge n times a quantum device, composed of non-communicating sub-units, which for each challenge z_i return an answer c_i. The data $(\mathbf{c}, \mathbf{z})$ is evaluated by a pre-defined linear entropy witness W. If an entropy larger than a (pre-defined) threshold t is witnessed, the protocol produces a certified entropy source with at least $t - k$ bits. The constant k is typically a small number that depends on the witness design and on a chosen security parameter ε (see for instance (9)).

previous runs. Notice that if the behaviour of the device deviates significantly from the previously estimated typical behaviour, the protocol may abort with greater likelihood, but its security is never compromised.

Basic entropy measures. In this paper, we will use measures of entropy tailored for our specific setup that build on a few basic definitions. Throughout, we adopt the convention where entropies are measured in bits; accordingly all logarithms are taken to base 2.

The first entropy measure is the *min-entropy*, which captures the minimum uncertainty of a random variable X distributed according to a probability distribution μ. It is defined as

$$H_{\min}(X) = -\log P_{\text{guess}}(X)\,, \tag{2}$$

where

$$P_{\text{guess}}(X) := \max_x \mu(X = x) \tag{3}$$

is the *guessing probability* of X. When necessary, we will explicitly write $H_{\min,\mu}(X)$ to indicate the underlying distribution. The *conditional min-entropy* of X given a fixed value $Y = y$ (hereafter denoted simply by y) is defined as

$$H_{\min}(X|y) = -\log \max_x \mu(x|y)\,. \tag{4}$$

The second measure we consider is the *Shannon entropy*, which quantifies the average uncertainty of X,

$$H(X) = \mathbb{E}(-\log \mu(X))\,, \tag{5}$$

where the expectation operator is given by $\mathbb{E}(Y) = \sum_y \mu(y)y$. When needed, we will explicitly write $\mathbb{E}_\mu$ as a reminder of the distribution being considered.

2.2 Probability estimation factors (PEFs)

Let us start by introducing the building block of the probability estimation technique[4].

Definition 1. *Let $\beta > 0$, and let $\mathcal{S}$ be the set of allowed behaviours. A* probability estimation factor (PEF) *with power β for $D|Z$ is a random variable $F = F(C, Z)$ such that*

1. $F(C, Z) \geq 0$,
2. $\mathbb{E}\left(F(C, Z)\mu(D|Z)^{\beta}\right) \leq 1\,, \qquad \forall \mu(C, Z) \in \mathcal{S}\,.$

Notice that F can be evaluated using only the information available to the user.

Corollary 1. *If F is a PEF with power β, then it is necessarily a PEF for any power $\beta' \geq \beta$.*

A key property of PEFs is that a product of sequential PEFs defines a new PEF, as we will see in the following theorem. This result requires the side information e to be fixed throughout the process, so, for clarity, we explicitly include this dependency on e:

Theorem 1 (Theorem 23 in [8])**.** *Let $\mathcal{S}^n$ be the set of allowed behaviours in a sequential n-round protocol. Define the product of single round PEFs with power β as $T_n = \Pi_{i=1}^{n} F_i$. If the Markov condition (1) holds, T_n is a PEF with power β for $\mathbf{D}|\mathbf{Z}$, i.e.*

1. $T_n(\mathbf{C}, \mathbf{Z}) \geq 0$,
2. $\mathbb{E}\left(T_n(\mathbf{C}, \mathbf{Z})\mu(\mathbf{D}|\mathbf{Z}, e)^{\beta}\right) \leq 1\,, \qquad \forall \mu(\mathbf{C}, \mathbf{Z}|e) \in \mathcal{S}^n.$

Note that according to Corollary 1, we can compose sequences of individual PEFs with different powers β_i by choosing $\beta = \max_i \beta_i$.

Using Theorem 1 and Markov's inequality, we can now obtain a high-confidence lower-bound on the conditional probability of $\mathbf{D}$:

$$\Pr\left(T_n(\mathbf{C}, \mathbf{Z})\mu(\mathbf{D}|\mathbf{Z}, e)^{\beta} \geq \frac{1}{\kappa}\right) \leq \kappa\mathbb{E}\left(T_n(\mathbf{C}, \mathbf{Z})\mu(\mathbf{D}|\mathbf{Z}, e)^{\beta}\right) \leq \kappa\,, \tag{6}$$

where $\kappa > 0$ is a chosen security parameter. This implies a confidence bound on any $\mu(\mathbf{D}|\mathbf{Z}, e)$ that belongs to $\mathcal{S}^n$:

$$\Pr\left(-\log \mu(\mathbf{D}|\mathbf{Z}, e) \geq \frac{\log T_n(\mathbf{C}, \mathbf{Z})}{\beta} - \frac{\log 1/\kappa}{\beta}\right) \geq 1 - \kappa\,, \quad \forall e. \tag{7}$$

Given that $\log T_n(\mathbf{C}, \mathbf{Z}) = \sum_{i=1}^{n} \log F_i(C_i, Z_i)$, this multi-round bound reduces to a function of the single round PEFs and the confidence level κ.

[4] In [8], a more general building block, known as the *soft*-PEF, is introduced. This generalization differs from the standard PEF when $\mathbf{C} \neq \mathbf{D}$. However, we do not include this extension here, as it is more cumbersome to work with and unnecessary for our purposes—particularly since every PEF is also a soft-PEF (see Lemma 25 in [8]).

2.3 From PEFs to extractable entropy

Here we will see how the confidence bound (7) allows us to establish a lower bound on the randomness of $\mathbf{D}$. To identify the relevant measure of entropy in our context, recall that the goal of a QRNG protocol is to output a string of near-perfect random bits independent from any other variables. This can be achieved by processing $\mathbf{D}$ through a randomness extraction algorithm [14]. The length of the near-perfect random bit string that is generated as a result will depend on the chosen algorithm and on the amount of *extractable entropy* in $\mathbf{D}$. The latter can be quantified by smooth min-entropies, which were proposed by [15] for the general case of adversaries holding quantum side information. Since we restrict our attention to adversaries classically correlated to the device, we will now introduce a lower bound on the (classical) smooth conditional min-entropy and from there, find a bound on the extractable entropy of $\mathbf{D}$.

Definition 2. *Let random variables* $\mathbf{DZ}E$ *be jointly distributed with* μ. $\mathbf{D}$ *has* ϵ-smooth $\mathbf{Z}$E-conditional min-entropy $H^{\epsilon}_{\min}(\mathbf{D}|\mathbf{Z},E) \geq h$ *if there exists a distribution* ν*, defined on the same domain as* μ*, such that*

1. $\|\mu - \nu\| \leq \epsilon\,,$
2. $H_{\min,\nu}(\mathbf{D}|z,e) \geq h\,, \qquad \forall z, e\,,$

where $\|\mu(X) - \nu(X)\| = \frac{1}{2}\sum_x |\mu(x) - \nu(x)|$ *is the* total variation distance.

The next theorem establishes a relationship between the confidence bound (7) and a lower bound on the smooth conditional min-entropy.

Theorem 2. *If, for all* e, $\Pr\left(-\log \mu(\mathbf{D}|\mathbf{Z},e) \geq h\right) \geq 1-\epsilon$ *then* $H^{\epsilon}_{\min}(\mathbf{D}|\mathbf{Z},E) \geq h$.

Proof. See Appendix A. □

To identify the extractable entropy in our protocols, recall that they include an acceptance step, where the sequence of n inputs and outputs is evaluated by some entropy estimator W. In our case, it is defined as

$$W := \frac{1}{\beta}\sum_i \log F_i\,. \tag{8}$$

Having chosen a set of PEFs $\{F_i\}_i$ with power β and an acceptance threshold t, the output sequence $\mathbf{d}$ is accepted and proceeds to extraction if $W(\mathbf{c},\mathbf{z}) \geq t$; otherwise, the protocol aborts (Figure 1). The following result finally establishes a lower bound on the extractable entropy of $\mathbf{D}$.

Theorem 3. *Consider the event* $\texttt{Accept} = \{W \geq t\}$ *and its probability* $p_{Acc} = \Pr(W \geq t)$. *If, for all* e, $\Pr\left(-\log \mu(\mathbf{D}|\mathbf{Z},e) \geq W\right) \geq 1-\kappa$ *and* $p_{Acc} = \Pr(W \geq t)$, *then the* extractable entropy *of* $\mathbf{D}$, *defined by* $H^{\varepsilon/p_{Acc}}_{\min}(\mathbf{D}|\mathbf{Z},E,\texttt{Accept})$, *is lower-bounded by*

$$H^{\varepsilon/p_{Acc}}_{\min}(\mathbf{D}|\mathbf{Z},E,\texttt{Accept}) \geq t + \frac{\log\kappa}{\beta} + \log(\varepsilon-\kappa)\,, \tag{9}$$

where $\varepsilon > \kappa$ *is the chosen security parameter.*

Proof. See Appendix A. □

Note that the threshold t can be chosen according to

$$t = \mathbb{E}_{\mu_{\text{typ}}}(W) - \delta\,, \tag{10}$$

where the expected value of W is evaluated on the typical behaviour of the device μ_{typ} (see discussion in Section 2), and δ is a parameter that allows us to tune the acceptance rate of the protocol. The extractable entropy (9) then takes the form

$$H_{\min}^{\varepsilon/p_{Acc}}(\mathbf{D}|\mathbf{Z}, E, \texttt{Accept}) \geq \sum_i \frac{\mathbb{E}_{\mu_{\text{typ}}}[\log F_i]}{\beta} - \frac{1}{\beta}\log\frac{1}{\kappa} - \log\frac{1}{\varepsilon-\kappa} - \delta\,, \tag{11}$$

where $\sum_i \mathbb{E}_{\mu_{\text{typ}}}\left(\frac{\log F_i}{\beta}\right)$ represents the asymptotic entropy for very large n, while the remaining terms do not depend on n. Although practical protocols typically use $\delta > 0$, hereafter we set $\delta = 0$ for simplicity. The PE approach then offers a trade-off between the asymptotic entropy term and the finite size/non-IID (independent and identically-distributed) penalty term $(\log 1/\kappa)/\beta$, that is known to be advantageous for small n [7, 8]. With other standard approaches, such as [4] for classical and [6] for quantum side information, the extractable entropy contains a penalty term that scales with $\sqrt{n}$ (see Appendix C), which becomes negligible for very large n but is significant for lower numbers of rounds.

2.4 Finding good PEFs

At this point, we aim at designing PEFs that maximise the amount of extractable entropy (11) in our protocols for a typical behaviour μ_{typ}. This means finding the set of $\{F_i\}_i$ with power β that maximises

$$\max_{\beta,\{F_i\}_i,\kappa} \mathbb{E}_{\mu_{\text{typ}}}(W) - \frac{1}{\beta}\left(\log\frac{1}{\kappa}\right) - \log\frac{1}{\varepsilon-\kappa}\,, \tag{12}$$

where $\mathbb{E}_{\mu_{\text{typ}}}(W) = \sum_i \mathbb{E}_{\mu_{\text{typ}}}(\log F_i)/\beta$ according to (8), ε is the chosen security parameter, and κ is a free optimisation parameter such that $\varepsilon > \kappa > 0$. Note that the user has no means of finding a meaningful estimate of $\mu_{\text{typ}}(C_i, Z_i|e)$ at every single round. A reasonable approach is to optimise W for data collected over many rounds and perform an estimate of μ_{typ} assuming an IID behaviour of the device, i.e. where inputs (outputs) are described by the same random variable $Z_i = Z$ ($C_i = C$) at every round. This entropy estimator will be suboptimal for the real, non-IID, experimental conditions but is, by definition, a valid estimator for any μ in the allowed set of behaviours.

Performing an optimisation for the IID behaviour greatly simplifies our problem. The probability distributions at every round can now be represented by a single distribution

$$p(C, Z) = \mu_{\text{typ}}(C_i, Z_i|e)\,, \tag{13}$$

while the set of PEFs is reduced to a single function $F = F_i$. Consequently, the entropy witness (8) now becomes

$$W = \frac{n}{\beta}\log F\,. \tag{14}$$

As a result, optimisation (12) is performed over a much simpler set, and the expected value in the objective function simplifies to

$$\mathbb{E}_{\mu_{\text{typ}}}(W) = n\frac{\mathbb{E}_p(\log F)}{\beta}\,. \tag{15}$$

Distribution p can be estimated by the frequencies of data collected either in a characterisation stage of the protocol or in previous certification stages (see Section 1), according to

$$\hat{p}(c,z) = \frac{1}{n}\sum_{i=1}^{n} \chi(c_i = c, z_i = z)\,, \tag{16}$$

where χ is an indicator function such that $\chi(\texttt{True}) = 1$ and $\chi(\texttt{False}) = 0$.

Testing the entropy of data $(\mathbf{c},\mathbf{z})$ collected during a randomness certification stage (as depicted in Figure 1) corresponds to computing

$$W(\mathbf{c},\mathbf{z}) = n\sum_{c,z} p_{\text{obs}}(c,z)\frac{\log F(c,z)}{\beta}\,, \tag{17}$$

where $p_{\text{obs}}(c,z)$ are the frequencies in $(\mathbf{c},\mathbf{z})$ also using (16).

Finally, we can express the bound (11) on the extractable entropy in the more recognisable form,

$$H_{\min}^{\varepsilon/p_{Acc}}(\mathbf{D}|\mathbf{Z}, E, \texttt{Accept}) \geq nt' - \frac{1}{\beta}\left(\log\frac{1}{\kappa}\right) - \log\frac{1}{\varepsilon-\kappa}\ , \tag{18}$$

where the asymptotically dominating term is the amount of entropy defined by the acceptance threshold t—which can also be interpreted as the product of the number of rounds n by the single round entropy $t' = \mathbb{E}_p\left(\frac{\log F}{\beta}\right)$—and the penalty terms are due to memory and finite size statistics. The single round entropy estimator $(\log F)/\beta$ is a suboptimal estimator for the average Shannon entropy (refer to [8] and also Appendix B). Moreover, in the asymptotic limit of very large n, it is proven that this estimator converges to optimality [8].

Tackling the optimisation problem. In order to find the optimal W for an IID behaviour, we now have to solve the optimisation problem described in (12):

$$\begin{aligned}
\max_{F,\beta,\kappa}\quad & \frac{1}{\beta}\left(n\sum_{c,z} p(c,z)\log F(c,z) + \log(\kappa)\right) + \log(\varepsilon-\kappa)\\
\text{s.t.}\quad & F \geq 0\\
& \beta > 0\\
& \varepsilon > \kappa > 0\\
& \sum_{c,z}\mu(c,z|e)F(c,z)\mu(d|z,e)^{\beta} \leq 1\,,\quad \forall\mu(C,Z|e)\in\mathcal{S}\,.
\end{aligned} \tag{19}$$

Due to the non-linear objective and constraint, directly solving the full optimisation is intractable, and we therefore consider a relaxation of the above problem. Specifically, for fixed values of (β,κ), we optimise over F by solving:

$$\begin{aligned}
\max_{F}\quad & \sum_{c,z} p(c,z)\log F(c,z)\\
\text{s.t.}\quad & F \geq 0\,,\\
& \sum_{c,z}\mu(c,z|e)F(c,z)\mu(d|z,e)^{\beta} \leq 1\,,\quad \forall\mu(C,Z|e)\in\mathcal{S}\,.
\end{aligned} \tag{20}$$

We perform optimisation for a large number of (β,κ) pairs to generate a collection of feasible solutions to the original problem (19). Each such solution provides a lower bound on the true optimum. Finally, we select the tuple (F,β,κ) from this set that maximises

the objective in (19). Although this strategy brings us closer to finding a good entropy estimator (15) for the typical device behaviour, whether we can actually have a practical method to tackle the optimisation (20) depends on the characterisation of $\mathcal{S}$.

In this work, we consider two distinct device-independent scenarios. In the first, the inputs $\mathbf{Z}$ are chosen independently of the device's behaviour and therefore also independently of the adversary: $\mu(Z|e) = \mu(Z)$. In the second scenario, $\mathbf{Z}$ may share correlations with the device, restricted by a parameter known to the user. Each setting defines a different and characteristic set of allowed behaviours $\mathcal{S}$. However, as we will discuss in detail in Section 4.2, both scenarios ultimately require an optimisation over conditional quantum behaviours $\mu(C|Z)$. We begin by analysing the first, simpler scenario, which provides the foundational tools necessary to address the more general case.

We then turn our attention to the set of conditional quantum behaviours, denoted by $\mathcal{Q}$. While this set is known to be convex [16], no general explicit characterisation is currently available. Nonetheless, it can be efficiently approximated from the outside by a converging hierarchy of semidefinite programs, known as the Navascués-Pironio-Acín (NPA) hierarchy [17, 18]. In this work, we use the NPA hierarchy as a relaxation of the problem of characterising $\mathcal{Q}$. For simplicity, we will henceforth (somewhat abusively) identify $\mathcal{Q}$ with a fixed level of the NPA hierarchy. Note that using this relaxation to find the optimal PEF provides a lower bound on the solution of (20), since the new feasible set is a subset of the original one. This coincides with the intuition that giving the adversary a larger set of allowed behaviours still provides a valid, most likely suboptimal, entropy bound.

Despite our efforts, this relaxation of optimisation (20) is still challenging. It consists of optimising a logarithmic function over a convex domain of F. This domain is nonlinearly dependent on a variable μ which must belong to a chosen level of the NPA hierarchy (defined by semidefinite constraints). It is not known if one can directly incorporate the NPA constraints into (20) in such a way that the resulting problem is solvable. Therefore, we follow the approach in [7, 8] to further relax this problem. We approximate the set $\mathcal{Q}$ from the outside by a convex polytope $\mathcal{P}_Q$. Then, due to convexity, it suffices to impose the PEF constraint on all the extreme points of this polytope, which we denote by the set $\mathrm{Extr}(\mathcal{P}_Q)$. In the measurement independent scenario, this leads to the following relaxation of (20):

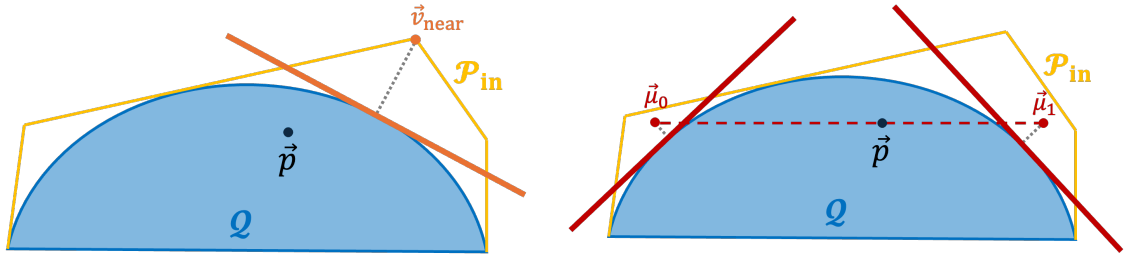
$$\begin{aligned} \max_F \quad & \sum_{c,z} p(c,z) \log F(c,z) \\ \text{s.t.} \quad & F \geq 0 \\ & \sum_{c,z} F(c,z)\mu(c|z,e)p(z)\mu(d|z,e)^\beta \leq 1, \quad \forall \mu \in \mathrm{Extr}(\mathcal{P}_\mathcal{Q}) \,, \end{aligned} \tag{21}$$

where $p(z) = \mu(z)$ is assumed to be known or estimated by the user.

3 Outer polytope approximations to the quantum set

We have seen in the last section that finding appropriate outer polytope approximations $\mathcal{P}_Q$ is a step toward obtaining effective entropy estimators (15). But what makes a good approximation? Ideally, polytopes $\mathcal{P}_Q$ should:

1. Closely approximate the original quantum set $\mathcal{Q}$. This avoids the gross overestimation of the adversary's allowed behaviours, which can lead to unnecessarily suboptimal entropy estimators;



(a) Algorithm 1 using near non-quantum vertices

(b) Algorithm 2 using optimal guessing strategies

Figure 2: **Illustrations of algorithms NearV (1) and MaxGP (2).** The blue region represents an approximation to the quantum set $\mathcal{Q}$ given by some level of the NPA hierarchy while the yellow lines represent the boundaries of a polytope $\mathcal{P}_{\text{in}}$ containing $\mathcal{Q}$. Our aim is to generate a finer outer-polytope approximation $\mathcal{P}_Q$ to $\mathcal{Q}$ taking into account the typical conditional behaviour $\vec{p}$ (black dot). (a) NearV (Algorithm 1): Randomly choose one vertex $\vec{v}_{\text{near}}$ from the set of m nearest non-quantum vertices to $\vec{p}$ and generate a quantum Bell inequality $(\vec{b}, \beta)$ (half-space delimited by the orange line, tangent to $\mathcal{Q}$) defined by the vector between $\vec{v}_{\text{near}}$ and its closest $\vec{q} \in \mathcal{Q}$ (the grey dotted line). The output polytope $\mathcal{P}_Q$ is the intersection of $\mathcal{P}_{\text{in}}$ with the quantum Bell inequality $(\vec{b}, \beta)$. (b) MaxGP (Algorithm 2): Solve optimisation (27) for $\vec{p}$ and a set of allowed behaviours $\mathcal{P}_{\text{in}}$ and obtains the optimal adversarial guessing strategies $\{\vec{\mu}_\lambda\}_\lambda$ (in the illustration, red points with $|E| = 2$). The algorithm uses each $\vec{\mu}_\lambda$ to generate a quantum Bell inequality (delimited by a red line) in a similar method to Algorithm 1. The new polytope $\mathcal{P}_Q$ is the intersection of $\mathcal{P}_{\text{in}}$ with at least one quantum Bell inequality.

2. Be simple enough such that *(i)* it is possible to find all its extreme points and *(ii)* the number of extreme points is not excessively large, allowing us to solve (21) in a reasonable amount of time.

Here we propose a method for designing polytopes $\mathcal{P}_Q$ that explicitly takes into account the typical conditional behaviour $p(C|Z)$, which allows these approximations to be effective and tractable. Our starting point is a polytope $\mathcal{P}_{\text{in}}$ that contains $\mathcal{Q}$, for instance the set of non-signalling behaviours $\mathcal{NS}$ [13, 19]. We then obtain refined polytopes $\mathcal{P}_Q$ by iteratively eliminating supra-quantum behaviours[5] that could significantly enhance the adversary's predictive power. For this, at each iteration, we tighten the approximation by imposing additional quantum Bell inequalities chosen to be tangent to $\mathcal{Q}$. The two main algorithms described in the following lead to PEFs that perform well in a variety of scenarios, as illustrated in the next section.

3.1 Polytope approximations using nearest non-quantum vertices

The first algorithm, NearV, aims at building an approximation $\mathcal{P}_Q$ by excluding the regions of $\mathcal{P}_{\text{in}}$ nearest to selected supra-quantum vertices (see Figure 2). To understand the intuition behind this approach, recall that while the user observes a behaviour $p(C|Z)$, an adversary having access to classical correlations may know any possible convex decomposition of this point into any behaviours of $\mathcal{P}_{\text{in}}$. In particular, writing this polytope in its vertex (or V)-representation, $V = \{v_k(C|Z)\}_k$, we have

$$p(C|Z) = \sum_k \omega(k) v_k(C|Z)\,, \tag{22}$$

where $\omega(k) \geq 0$ and $\sum_k \omega(k) = 1$. On one hand, we would like to identify and eliminate the non-quantum vertices v_k that appear in the decomposition (22), i.e., that can be part

[5] A behaviour is supra-quantum if it does not have a quantum realisation (see Section 1).

of an adversary's strategy. These vertices are intuitively in the vicinity of $p(C|Z)$. On the other hand, removing supra-quantum extremal behaviours associated with smaller weights $\omega(k)$ (i.e., larger distances from $p(C|Z)$) avoids decompositions that contain a significant contribution of local vertices, which are always deterministic. Empirically, we find that an effective approach is to randomly select a vertex from the subset of the m vertices closest to $p(C|Z)$ and then eliminate the supra-quantum region between this vertex and the quantum set $\mathcal{Q}$. This strategy has proven effective in reducing the adversary's predictive power. The parameter m is user-defined and depends on the setup.

We present the NearV algorithm using a vectorial representation of the space of behaviours, meaning that $\mu(C|Z)$ will be represented by a vector $\vec{\mu}$ with components μ_{cz}. A half-space $(\vec{h}, \eta)$ is the set of vectors $\vec{\mu}$ such that

$$\vec{h} \cdot \vec{\mu} \leq \eta \,. \tag{23}$$

A quantum Bell inequality $(\vec{b}, \beta)$ is a half-space which contains the quantum set $\mathcal{Q}$

$$\vec{b} \cdot \vec{\mu} \leq \beta \,, \qquad \forall \vec{\mu} \in \mathcal{Q} \,. \tag{24}$$

Algorithm 1 NearV: Generates a new polytope $\mathcal{P}_Q$ using the nearest non-quantum vertices to $p(C|Z)$.

Input: $\vec{p}$ - typical conditional behaviour; $H = \{(\vec{h}_j, \eta_j)\}_j$ - $\mathcal{P}_{\text{in}}$ polytope in H-representation; I - number of iterations; m - size of list of nearest vertices

Output: $\mathcal{P}_Q$ in V-representation

1: **for** $i \leftarrow 1$ to I **do**
2: Express the polytope H in its V-representation $V \leftarrow \{\vec{v}_k\}_k$;
3: Identify all the vertices $\{\vec{v}_{k'}\}_{k'}$ that are also in $\mathcal{Q}$ and define the list of quantum vertices $V_Q \leftarrow \{\vec{v}_{k'}\}_{k'}$;
4: Define the list of non-quantum vertices $V_{NQ} \leftarrow V \backslash V_Q$;
5: Compute the distance $d_k = ||\vec{v}_k - \vec{p}||$ for every $\vec{v}_k \in V_{NQ}$ and define the list of the m nearest vertices $D \leftarrow \{(\vec{v}_l, d_l)\}_{l=1}^m$;
6: Select $\vec{v}_l \in D$ with probability $d_l^{-1}/(\sum_{k=1}^m d_k^{-1})$ and set $\vec{v}_{\text{near}} \leftarrow \vec{v}_l$;
7: Find the behaviour $\vec{q} \in \mathcal{Q}$ that minimises $||\vec{v}_{\text{near}} - \vec{q}||$;
8: Define the Bell coefficients $\vec{b} \leftarrow \vec{v}_{\text{near}} - \vec{q}$;
9: Find the quantum bound $\beta \leftarrow \max_{\vec{\mu} \in \mathcal{Q}} \vec{b} \cdot \vec{\mu}$;
10: Define the tighter polytope approximation $H \leftarrow [H, (\vec{b}, \beta)]$;
11: **end for**
12: Express the polytope H in its V-representation $V \leftarrow \{\vec{v}_l\}_l$;
13: Output V

Note that the NearV algorithm can easily be modified to take an input polytope $\mathcal{P}_{\text{in}}$ in its V-representation. A possible choice for $\mathcal{P}_{\text{in}}$ is the non-signalling set $\mathcal{NS}$, or any known polytope containing $\mathcal{Q}$. A method for finding the H-representation of $\mathcal{NS}$ can be found, for instance, in [19] and references therein. Vertex enumeration algorithms to find the V-representation of a convex polytope given its H-representation are widely available. We have arbitrarily chosen the total variation distance in our implementations, but this could be replaced by another efficiently computable distance. Likewise, one can use different probability distributions to choose $\vec{v}_{\text{near}}$ in Step 5. For instance, the uniform distribution also gave good results in some of our simulations. Finally, Steps 3, 7 and 9 require the use of the NPA relaxation algorithm.

3.2 Polytope approximations using optimal guessing strategies

Our second algorithm uses a more elaborate method to identify supra-quantum strategies that might significantly contribute to the predictive power of an adversary. The basic idea is to use an algorithm that finds the behaviours that maximise the adversary's probability of guessing D for a typical distribution $p(C|Z)$. These optimal strategies are then used to define quantum Bell inequalities in a similar way to the NearV algorithm (see Figure 2). Note that the adversarial strategies that maximise the guessing probability—equivalently minimise the min-entropy of D, see (2) and (3)—are in general different from the adversarial strategies that minimise our single round entropy estimator from $(\log F)/\beta$ (15) [6]. Nevertheless, as we will see later, removing the sets of supra-quantum behaviours identified by this approach significantly increases the amount of verifiable entropy using PEFs in various examples.

Algorithm to find optimal guessing strategies. We start by reviewing the algorithm introduced by Nieto *et al* [20]. It relies on the description of a general adversarial strategy to guess D, given that a particular input z has been chosen. The adversary uses its side information Λ to make a guess on D and is successful whenever $\lambda = d$. This implies that it is enough to consider the number of strategies to be $|\Lambda| = |D|$ and the guessing probability can be written as

$$P_{\text{guess}}(D|z,\Lambda) = \max_{q_\Lambda, \{\mu_\lambda(C|Z)\}_\lambda} \left(\sum_d q_\Lambda(d)\mu_d(d|z) \right) , \tag{25}$$

where q_Λ is the probability distribution of Λ. Strategies $\mu_d(C|Z) = \mu(C|Z, \Lambda = d)$ belong to the set of allowed behaviours $\mathcal{S}$ and must be compatible with the behaviour $p(C|Z)$. We can absorb the normalisation factor $q_\Lambda(d)$ and define sub-normalised strategies $\tilde{\mu}_d$ as

$$\tilde{\mu}_d(C|Z) = q_\Lambda(d)\mu_d(C|Z) . \tag{26}$$

The guessing probability can then be expressed as the following optimisation problem

$$\begin{aligned} P_{\text{guess}}(D|z,\Lambda) = \max_{\{\tilde{\mu}_\lambda\}_\lambda} & \sum_d \tilde{\mu}_d(d|z) \\ \text{s.t.} \ & \sum_d \tilde{\mu}_d(C|Z) = p(C|Z) , \quad \forall \tilde{\mu}_d(C|Z) \in \widetilde{\mathcal{S}} , \end{aligned} \tag{27}$$

where $\widetilde{\mathcal{S}}$ is the set of sub-normalised allowed behaviours. The solution to this problem gives us also the set of optimal strategies $\{\mu_d(C|Z)\}_d$ for the chosen input z.

We are now in position to introduce our second algorithm to approximate the quantum set.

[6] We show in Appendix B that the expected value of this estimator defines a min-trade-off function for the average conditional Shannon entropy.

Algorithm 2 *MaxGP*: Generates a polytope $\mathcal{P}_Q$ using the supra-quantum behaviours that maximise the guessing probability of D.

Input: $\vec{p}$ - typical conditional behaviour; $p(Z)$ - input distribution; $H = \{(\vec{h}_j, \eta_j)\}_j$ - $\mathcal{P}_{\text{in}}$ polytope in H-representation; I - number of iterations

Output: $\mathcal{P}_Q$ in V-representation

```
for i ← 1 to I do
    Randomly pick a setting z according to p(Z);
    Obtain the behaviours {μ⃗_λ}_λ that maximise P_guess(D|z, Λ) for the set of allowed behaviours H;
    for λ ← 1 to |Λ| do
        if μ⃗_λ ∉ Q then
            Find the behaviour q⃗ ∈ Q that minimises ||μ⃗_λ − q⃗||;
            Define the Bell coefficients b⃗ ← μ⃗_λ − q⃗;
            Find the quantum bound β ← max_{μ⃗∈Q} b⃗ · μ⃗;
            Define the refined polytope approximation H ← [H, (b⃗, β)];
        end if
    end for
end for
Express the polytope H in its V-representation V ← {v⃗_l}_l;
Output V
```

Note that we have chosen here to randomly pick the setting z to compute the optimal strategies at every iteration of the algorithm. Other choices are possible, for instance picking z that gives the highest $P_{\text{guess}}(D|z, \Lambda)$, finding the strategies that maximise the guessing probability averaged over the inputs z (see the approach in [21]), or simply choosing a fixed setting z.

4 Randomness certification using new polytope approximations

In this section, we consider a variety of device-independent protocols for randomness certification and compute the amount of extractable entropy (9) using the PE approach combined with polytope approximations $\mathcal{P}_Q$ generated by the algorithms introduced in the previous section.

First, we consider the most standard protocols in which the entropy source $\mathbf{Z}$ is independent from the side information E, therefore relying on Bell tests. In the bipartite case, we analysed the global output entropy in noisy standard [22] and asymmetric [11] CHSH correlations, and in experimental data obtained from running loophole-free CHSH-Bell tests [23, 24]. For the tripartite case, we studied the two-party output entropy in noisy Mermin correlations obtained through real experiments on a commercially available quantum computer (H1 from Quantinuum). Our results are compared with the extractable entropy obtained in previous analyses with PE or with other commonly used methods, namely:

- The PE approach using the original polytope approximations [8] and approximations introduced in [10];
- The randomness certification method for classical side information described in [4, 20, 25]. This is one of the first approaches to successfully certify entropy in a non-IID setting;

- The EAT method, as introduced in [6], which considers quantum side information. This result (and its variations) is the most commonly used method to certify entropy under coherent attacks.

We also consider protocols where the input entropy source might be correlated with the side information E, meaning that inputs may be correlated to the state of the device in a manner known to the adversary. These are commonly referred to as *randomness amplification* protocols. We analyse the correlations arising in a practical protocol proposed in [26] and compare with their results.

Note that when analysing theoretical noisy correlations or experimental data with no prior calibration data, we consider the typical behaviour p to coincide with the observed p_{obs}.

4.1 Protocols using an independent entropy source

When the inputs $\mathbf{Z}$ are chosen independently of the state of the device, finding a PEF adapted to the typical behaviour $p(C, Z)$ involves solving the optimisation problem (21) for a set of allowed conditional behaviours, as described in Section 2.4. In this section, inputs are therefore independent of the side information $p(Z) := \mu(Z|e) = \mu(Z)$. We have chosen uniformly distributed inputs $p(Z) = 1/|Z|$ for simplicity, but other choices would be possible (for instance, we could have chosen distributions biased towards a particular input, like in spot-checking protocols).

4.1.1 Standard and asymmetric noisy CHSH correlations

Consider the bipartite Bell scenario, with $C = AB$ and $Z = XY$, and the asymmetric CHSH inequality [11, 22]

$$\text{CHSH}_\alpha := \alpha\langle \mathsf{A}_0\mathsf{B}_0\rangle + \alpha\langle \mathsf{A}_0\mathsf{B}_1\rangle + \langle \mathsf{A}_1\mathsf{B}_0\rangle - \langle \mathsf{A}_1\mathsf{B}_1\rangle \leq 2\alpha\,, \tag{28}$$

where the local observables A_x and B_y can take values ± 1, $\langle\cdot\rangle$ represents their expected value, for instance $\langle \mathsf{A}_x\rangle = \sum_a ap(a|x)$, and 2α is the classical bound of the expression. For $\alpha = 1$, we recover the standard CHSH Bell inequality while $\alpha > 1$ corresponds to the asymmetric case. The maximum quantum Bell violation of (28) is achieved when

$$\begin{gathered}\langle \mathsf{A}_x\rangle = \langle \mathsf{B}_y\rangle = 0\,,\\ \langle \mathsf{A}_0\mathsf{B}_y\rangle = \frac{\alpha}{\sqrt{1+\alpha^2}}\,, \qquad \langle \mathsf{A}_1\mathsf{B}_y\rangle = \frac{(-1)^y}{\sqrt{1+\alpha^2}}\,,\end{gathered} \tag{29}$$

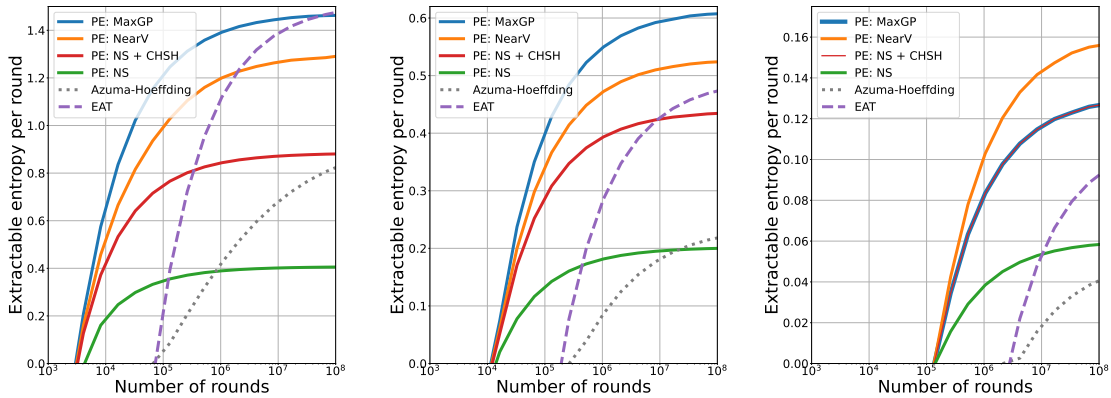
which corresponds to the conditional behaviour $p^*_\alpha(A, B|X, Y)$ via $p(a, b|x, y) = 1/4(1 + \langle \mathsf{A}_x\rangle + \langle \mathsf{B}_y\rangle + ab\langle \mathsf{A}_x\mathsf{B}_y\rangle)$.

Here we analyse protocols with typical conditional behaviours that are convex mixtures of the optimal behaviour (29) and white noise

$$p_{\alpha,w}(A, B|X, Y) = (1 - w)p^*_\alpha(A, B|X, Y) + w\frac{1}{4}\,, \tag{30}$$

for $\alpha = 1$ (standard CHSH) and $\alpha = 8$, and a variety of noise levels $w \in [0, 1]$.

Obtained results. Figures 3a-4c depict lower bounds on the extractable entropy per round $\frac{1}{n}H_{\min}^{\varepsilon/p_{Acc}}(\mathbf{AB}|\mathbf{XY}, E)$ (18) as a function of the number of rounds n of the protocol. We considered acceptance thresholds (10) with $\delta = 0$ and security parameter $\varepsilon = 2^{-128}$.



(a) w=0.5% (b) w=15% (c) w=25%

Figure 3: **Extractable entropy rates from noisy CHSH correlations for different levels of white noise.** Solid lines are obtained through the PE technique using different sets of allowed conditional behaviours: (orange) $\mathcal{P}_Q$ from 10 iterations of NearV (Algorithm 1 with $m = 10$); (blue) $\mathcal{P}_Q$ from 10 iterations of MaxGP (Algorithm 2); (green) $\mathcal{P}_Q = \mathcal{NS}$; and (red) $\mathcal{P}_Q = \mathcal{NS} \cap \mathrm{CHSH} \leq 2\sqrt{2}$, which coincides with set used in [8]. The purple dashed line is obtained using the EAT approach [27] and the grey dotted line represents the method [4, 20] using the Azuma-Hoeffding inequality. The figure is produced using level 2 of the NPA hierarchy.

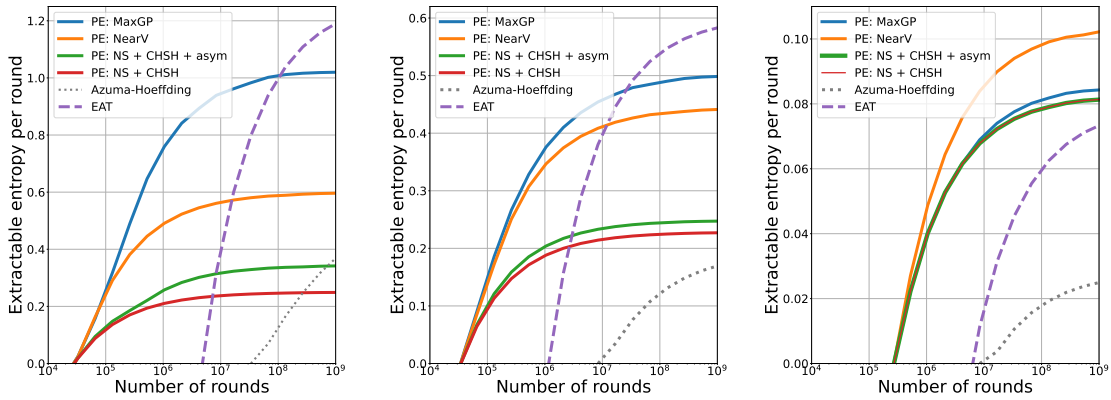
Note that we used $\mathcal{P}_{\text{in}} = \mathcal{NS} \cap \mathrm{CHSH} \leq 2\sqrt{2}$, i.e. the intersection between $\mathcal{NS}$ and the behaviours that do not violate CHSH beyond its quantum bound, as the input for the NearV and MaxGP algorithms, which corresponds to the set of allowed behaviours used in [8].

4.1.2 Noisy correlations from loophole-free CHSH-Bell tests

We report here in Table 2 the improvements on the extractable entropy rates for data from loophole-free CHSH-Bell tests reported in [23, 24]. In particular, note that we obtained almost twice the entropy from the data in [24], while previous attempts with refined polytopes [10] only achieved a marginal improvement.

Data set		n	$\mathrm{CHSH}_{\alpha=1}$	ε	Extractable entropy rate before*	Extractable entropy rate with our methods
[8, Table I], [23]		27,683	2.1756226	2^{-32}	0.04119278	0.05010119
[24]	Instance 1	23,194,880	2.0011386	2^{-64}	0.00033189	0.00056707
	Instance 2	37,649,791	2.0011957	2^{-64}	0.00021068	0.00047694
	Instance 3	28,537,805	2.0010692	2^{-64}	0.00030063	0.00052014
	Instance 4	28,319,978	2.0010454	2^{-64}	0.00030474	0.00050788
	Instance 5	27,219,887	2.0011109	2^{-64}	0.00028706	0.00050131

Table 1: Extractable entropy rates from loophole-free CHSH-Bell tests [23, 24]. Our method improves the extractable entropy rates compared to those previously reported. 10 iterations of NearV (Algorithm 1 with $m = 10$) is used to obtain the result for [8, Table I][23], and MaxGP (Algorithm 2) is used to obtain the results for [24]. *For [24] these entropy rates are calculated with the optimal PEFs reported in their Table IV, Appendix IV, and for [8, Table I] we obtain the rate with $\mathcal{P}_Q = \mathcal{NS} \cap \mathrm{CHSH} \leq 2\sqrt{2}$ which was used in their analysis.



(a) w=0.1% (b) w=1% (c) w=7%

Figure 4: **Extractable entropy rates from noisy asymmetric CHSH correlations ($\alpha = 8$) for different levels of white noise.** Solid lines are obtained through the PE technique using sets of allowed conditional behaviours: (orange) $\mathcal{P}_Q$ from 10 iterations of NearV (Algorithm 1 with $m = 10$); (blue) $\mathcal{P}_Q$ from 10 iterations of MaxPG (Algorithm 2); (red) - $\mathcal{P}_Q = \mathcal{NS} \cap \mathrm{CHSH} \leq 2\sqrt{2}$ (set defined according to the approach in [8]); and (green) - $\mathcal{P}_Q = \mathcal{NS} \cap \mathrm{CHSH} \leq 2\sqrt{2} \cap \mathrm{CHSH}_{\alpha=8} \leq TB$ (Tsirelson's bound) (set used in [10]). The purple dashed line is obtained using the EAT approach [27], and the grey dotted line uses the method in [4, 20], which uses the Azuma-Hoeffding inequality. The figure is produced using level 2 of the NPA hierarchy.

4.1.3 Noisy Mermin correlations

A well-studied Bell inequality in the tripartite scenario is the Mermin inequality

$$\mathrm{M} = \langle \mathsf{A}_0\mathsf{B}_0\mathsf{C}_0\rangle - \langle \mathsf{A}_0\mathsf{B}_1\mathsf{C}_1\rangle - \langle \mathsf{A}_1\mathsf{B}_0\mathsf{C}_1\rangle - \langle \mathsf{A}_1\mathsf{B}_1\mathsf{C}_0\rangle \leq 2 \tag{31}$$

where local observables A_x, B_y and C_z can take values ± 1. The maximum quantum violation (and algebraic bound) of this inequality is $\mathrm{M} = 4$, which can be achieved by measuring the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ with the Pauli operators $\mathsf{A}_0 = \mathsf{B}_0 = \mathsf{C}_0 = \sigma_x$ and $\mathsf{A}_1 = \mathsf{B}_1 = \mathsf{C}_1 = \sigma_y$.

To showcase our method and the effectiveness of our algorithms, we have implemented the Mermin-Bell test on an ion-trap quantum computer (H1 from Quantinuum [28])[7] with $n = 4 \times 10^4$ rounds, from which we obtained a behaviour achieving $\mathrm{M} = 3.928$ shown in Table 2. We then analyse the extractable entropy of outputs $\mathbf{D} = \mathbf{AB}$ using the typical behaviour estimated by (16) and regularised according to [29]. The results depicted in Figure 5 include the extractable entropy from the same behaviour as if it were obtained with a different n.

4.2 Protocols using an entropy source correlated with the device

Randomness amplification protocols allow one to obtain certified output entropy even if inputs are chosen from a weakly random source that is partly correlated with the quantum device. However, this comes at the price of more complex security analysis and lower

[7] While one cannot guarantee the non-signalling condition in experiments performed on a single quantum computer, the negligible levels of cross-talk in H1 support the assumption that local measurements are indeed independent across different locations.

abc \ xyz	000	001	010	011	100	101	110	111
000	0.0044	0.1258	0.1302	0.2514	0.1282	0.2414	0.2484	0.1236
001	0.247	0.129	0.127	0.0034	0.1254	0.0024	0.0024	0.1358
010	0.244	0.1252	0.115	0.0014	0.124	0.0018	0.0016	0.1242
011	0.002	0.126	0.125	0.248	0.1194	0.2546	0.2468	0.1292
100	0.2536	0.1204	0.1252	0.002	0.1264	0.003	0.0024	0.125
101	0.0014	0.1256	0.1232	0.2352	0.1202	0.2472	0.2518	0.119
110	0.0018	0.1228	0.1304	0.2556	0.1318	0.2486	0.2446	0.1208
111	0.2458	0.1252	0.124	0.003	0.1246	0.001	0.002	0.1224

Table 2: Estimated probabilities $p(A, B, C|X, Y, Z)$ from running the Mermin game in H1 from Quantinuum, with $n = 4 \times 10^4$. Raw data before regularisation, achieving $\mathrm{M} = 3.928$.

output entropy rates. While one would expect sacrificing efficiency to achieve higher levels of security, how much entropy remains uncertified due to a suboptimal security analysis?

In this section, we show how to use the PE framework to lower-bound the extractable entropy of randomness amplification protocols that use a Santa Vazirani (SV)-source [32] as an input. These entropy sources produce bits S_i that, at every round, deviate from being perfectly random up to some bias parameter $0 \leq \delta < 1/2$,

$$\frac{1}{2} - \delta \leq \mu(S_i|S_{i-1}, \ldots, S_1, e) \leq \frac{1}{2} + \delta\,, \quad \forall i\,. \tag{32}$$

We illustrate our method by analysing the correlations arising in the bipartite protocol in [26] based on the Hardy paradox [33].

4.2.1 Algorithm to find PEFs for correlated input source

In the general case where the input randomness can be correlated with the quantum device, $\mu(Z|e)$ is no longer known to the user and the simplified optimisation (21) to find a PEF no longer holds. We must then go back to (20), which we reproduce here:

$$\max_F \quad \sum_{c,z} p(c,z) \log F(c,z) \tag{33}$$

$$\text{s.t.} \quad F \geq 0 \tag{34}$$

$$\sum_{c,z} \mu(c,z|e) F(c,z) \mu(d|z,e)^\beta \leq 1\,, \quad \forall \mu(C,Z|e) \in \mathcal{S}\,. \tag{35}$$

As before, solving this optimisation requires the set $\mathcal{S}$ to be a polytope, in which case it is sufficient to impose the constraint (35) only on the extreme points of this set. Given that we consider quantum adversaries, $\mathcal{S}$ is in general not a polytope, and we must find an outer-polytope approximation $\mathcal{P}_\mathcal{S}$ of $\mathcal{S}$. Although the allowed behaviours are now joint input-output distributions, this task will use the methods introduced in Section 3 as a sub-routine.

We consider here a bipartite protocol where, at each round, the inputs of A and B are defined by two samples of a SV-source (32)[8]. Therefore, the distribution of Alice's input

[8] We still require that the input of each party is not leaked to the other party; otherwise any distribution can be reproduced by classical strategies.

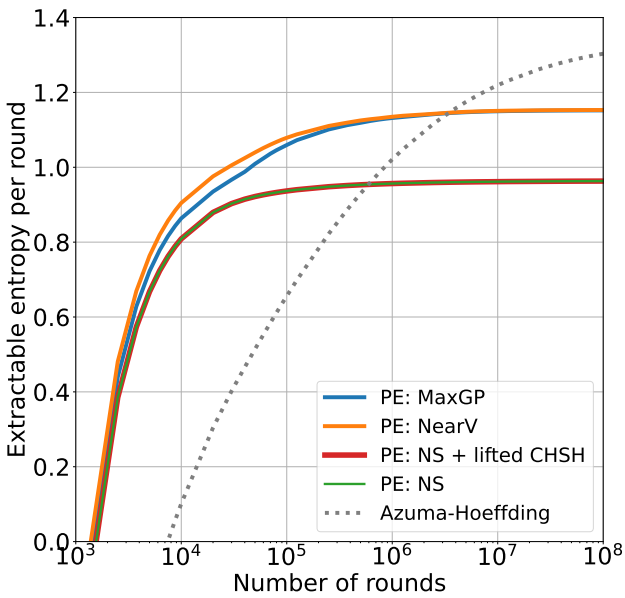


Figure 5: **Extractable entropy rates from noisy Mermin correlations obtained from Table 2 as a function of the number of rounds n.** Solid lines correspond to lower bounds computed with the PE technique using $\mathcal{P}_Q$ obtained through: (orange) NearV algorithm (Algorithm 1 with $m = 1$); (blue) MaxGP algorithm (Algorithm 2); (green) $\mathcal{P}_Q = \mathcal{NS}$; (red) $\mathcal{P}_Q = \mathcal{NS} \cap (\text{lifted-CHSH} \leq 2\sqrt{2})$, where the lifted-CHSH is a generalisation of CHSH for 3 parties [30]. The grey dotted line is obtained by approach [4] using analytical optimal P_{guess} as a function of the Mermin value [31]. The figure is produced using level 2 of the NPA hierarchy.

X at any round belongs to the polytope $\mathcal{SV}_\delta$ defined by

$$\frac{1}{2} - \delta \leq \mu(X|\lambda) \leq \frac{1}{2} + \delta\,, \tag{36}$$

where λ represents all the side information available to the adversary in that round, i.e., the information of past samples of the SV-source and any additional information e available. In full generality, we assume that Bob's input Y is generated after X. The probability distribution of Y also belongs to the polytope $\mathcal{SV}_\delta$ given by

$$\frac{1}{2} - \delta \leq \mu(Y|\lambda') \leq \frac{1}{2} + \delta\,, \tag{37}$$

where the information λ' contains both λ and x. The following theorem allows us to combine the sets of allowed input distributions for each party into a single convex polytope[9].

Theorem 4. *Consider two sets of inputs X and Y modelled by two samples of a δ-SV-source (32), i.e., each following probability distributions belonging to a convex polytope $\mathcal{SV}_\delta$ according to (36) and (37), respectively. Assume, without loss of generality, that X is sampled before Y. Then the set of allowed joint input distributions $\mathcal{SV}_\delta^2$ for both inputs is a polytope with vertices $u_{kk'}(X,Y) = v_k(X)v'_{k'}(Y)$, for $k, k' = 0, 1$, where $v_k(X) = \frac{1}{2}\left(1 + (-1)^{k+X}\delta\right)$ are vertices of $\mathcal{SV}_\delta$ for party* A*, and analogously for party* B*.*

[9]We could have also considered an SV-source where at each round the condition $l \leq \mu(X,Y|\lambda) \leq h$ holds. The vertices of this polytope are described in Lemma 1 of [34].

Proof. By construction, the set of joint input distributions is

$$\mathcal{SV}_\delta^2 = \{\mu(X,Y|\lambda) : \mu(X,Y|\lambda) = \mu(X|\lambda)\mu(Y|X,\lambda), \mu(X|\lambda) \in \mathcal{SV}_\delta, \mu(Y|x,\lambda) \in \mathcal{SV}_\delta, \forall x\}\,, \tag{38}$$

where $\mu(Y|x,\lambda) \in \mathcal{SV}_\delta$ following (37).

Recall that a point μ belongs to a polytope $\mathcal{P}$ if and only if it can be written as a convex combination of its vertices v_i,

$$\mu = \sum_i \omega(i) v_i\,, \tag{39}$$

where $\omega \geq 0$ and $\sum_i \omega(i) = 1$. Then we can express (38) as

$$\begin{aligned}\mathcal{SV}_\delta^2 = \{\mu(X,Y|\lambda) :& \mu(X,Y|\lambda) = \sum_{k,k'} \omega(k)\omega'(k') v_k(X) v'_{k'}(Y)\,,\\ & \omega,\omega' \geq 0\,, \sum_k \omega(k) = \sum_{k'} \omega'(k') = 1\}\,.\end{aligned} \tag{40}$$

Since $\omega(k)\omega'(k') \geq 0$ and $\sum_{k,k'} \omega(k)\omega(k') = 1$, we have that $\mathcal{SV}_\delta^2$ is a convex polytope with vertices $v_k(X)v'_{k'}(Y)$. □

As before, we approximate the set of conditional behaviours $\mathcal{Q}$ by a polytope $\mathcal{P}_Q$. This implies that the set $\mathcal{P}_\mathcal{S}$ of allowed behaviours is also a polytope with vertices $u_{ij}(CZ) = v_i(C|Z)v'_j(Z)$, where $\{v_i(C|Z)\}_i = \mathrm{Extr}(\mathcal{P}_Q)$ and $\{v'_j(Z)\}_j = \mathrm{Extr}(\mathcal{SV}_\delta^2)$. This result is analogous to the previous theorem and its proof is based on the decomposition $\mu(CZ|e) = \mu(C|Ze)\mu(Z|e)$.

We can then replace the constraint (35) by the condition[10]

$$\sum_{cz} \mu(c|z)\mu(z)F(c,z)\mu(d|z)^\beta \leq 1\,, \quad \forall \left(\mu(C|Z) \in \mathrm{Extr}(\mathcal{P}_Q) \wedge \mu(Z) \in \mathrm{Extr}(\mathcal{SV}_\delta^2)\right)\,, \tag{41}$$

which is analogous to the last constraint in (21), except that now it unfolds as a condition for each vertex of $\mathcal{P}_Q$ and $\mathcal{SV}_\delta^2$.

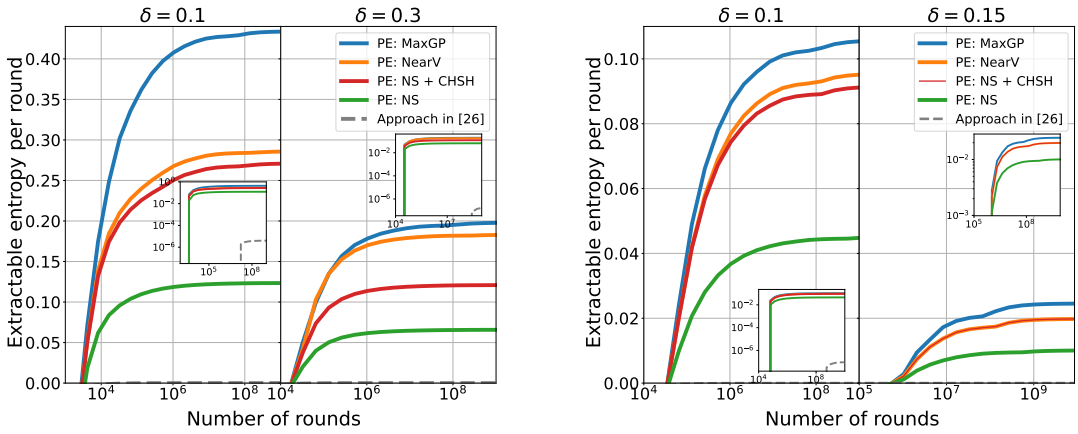
4.2.2 Noisy Hardy correlations

In the scenario where inputs are correlated to the device, Bell inequalities are replaced by measurement dependent locality (MDL) inequalities, introduced in [34], as tests of non-locality. A protocol for randomness amplification will then require correlations that violate some MDL inequality. In [26], the authors use a bipartite Hardy paradox [33] together with SV-sources (36) to select the inputs for each party, and build the following MDL inequality on distributions $p(A,B,X,Y)$:

$$h = p(0000)\left(\frac{1}{2} - \delta\right)^2 - (p(0101) + p(1010) + p(0011))\left(\frac{1}{2} + \delta\right)^2 \leq 0\,. \tag{42}$$

Assuming a non-signalling adversary classically correlated with the input source and the device, the amount of violation h is then related to an upper bound on $p(A,B|X,Y)$, from which a lower bound on the min-entropy of outputs AB is established, and consequently

[10] We omitted conditioning on e for simplicity.



(a) 0.1% white noise

(b) 5% white noise

Figure 6: **Randomness amplification of a SV-source.** Extractable entropy rates from noisy Hardy correlations (43) for different number of rounds: (a) 0.1% white noise with SV parameter $\delta = 0.1$ and $\delta = 0.3$; and (b) 5% white noise with SV parameter $\delta = 0.1$ and $\delta = 0.15$. Lines corresponding to lower bounds computed with the PEF approach using $\mathcal{P}_Q$ obtained through: (orange) 3 iterations of NearV (Algorithm 1 with $m = 15$); (blue) 3 iterations of MaxGP (Algorithm 2); (green) $\mathcal{P}_Q = \mathcal{NS}$; (red) $\mathcal{P}_Q = \mathcal{NS} \cap \mathrm{CHSH} \leq 2\sqrt{2}$. The grey dashed line represents the extractable entropy using the approach in [26] against NS adversaries (see Appendix C). The figure is produced using level 2 of the NPA hierarchy.

the extractable entropy[11] after n uses of the device. Here we will lower bound this entropy by directly using our approach on noisy Hardy correlations, i.e., mixtures of behaviours that maximise the violation h and white noise,

$$p_{\mathrm{Hardy},w}(A,B,X,Y) = (1-w)p^*_{\mathrm{Hardy}}(A,B,X,Y) + w\frac{1}{16}\,. \tag{43}$$

where we assumed $p(X,Y) = 1/4$. The ideal correlations $p^*_{\mathrm{Hardy}}(A,B,X,Y)$ are obtained by measuring the two-qubit state $|\phi_\theta\rangle = \frac{1}{\sqrt{1+\cos^2\theta}}\left(\cos\theta\left(|01\rangle + |10\rangle\right) + \sin\theta\,|11\rangle\right)$ in the basis $\{\sin\theta\,|0\rangle - \cos\theta\,|1\rangle\,, \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\}$ when $X,Y = 0$ and $\{|0\rangle\,,|1\rangle\}$ if $X,Y = 1$, for $\theta = \arccos\sqrt{\frac{\sqrt{5}-1}{2}}$. Figure 6 shows the extractable entropy rates obtained from $p_{\mathrm{Hardy},w}(A,B,X,Y)$ for different white noise and SV parameters with security parameter $\varepsilon = 2^{-32}$.

5 Discussion and conclusion

Our approach yields a significant improvement in the rates of extractable entropy across all scenarios we have examined. Additionally, when compared to analyses based on the original EAT [6] or the Azuma-Hoeffding inequality as in [4], our method requires far fewer device uses to achieve positive rates.

As discussed, a key advantage of PE is its better penalty factor—scaling as $O(\frac{1}{n})$, versus $O(\frac{1}{\sqrt{n}})$ for other approaches—compensating for suboptimal single round bounds. Another

[11] The extractable entropy is actually not computed in [26], where the chosen figure of merit is the number of ε-perfect random bits at the end of the protocol, meaning after randomness extraction. In Appendix A, we use their approach to obtain an expression for the extractable entropy that we can use to compare with our results.

interesting observation is the distinct asymptotic behaviour of the three approaches and how this impacts their performance. In the PE approach, extractable entropy rates converge to the conditional Shannon entropy. In contrast, the method in [4] yields convergence to the conditional min-entropy, which is a lower bound on the conditional Shannon entropy. This difference contributes to the superior performance of PE-based methods unless the polytope approximation used is too coarse (as is the case in the tripartite scenario analysed). On the other hand, entropy extracted using the EAT converges to the conditional von Neumann entropy, which is generally lower than the conditional Shannon entropy. However, in the large n regime and for correlations with low noise levels, the EAT approach sometimes outperforms the PE method. We believe this is primarily due to a smaller set of allowed behaviours (defined directly by the NPA hierarchy) being considered in the EAT framework.

Regarding the scalability of our approach, it is important to highlight that both algorithms fundamentally rely on the ability to perform vertex enumeration—a computationally intensive task that constitutes a clear bottleneck. For example, computing the vertices of the non-signalling polytope $\mathcal{NS}$ in Bell scenarios involving more than three parties becomes infeasible with standard computational resources. As a result, applying our methods to more complex scenarios would require initialising the algorithms with significantly coarser approximations of the quantum set—such as polytopes that may include signalling behaviours. This possibility could be explored if these more complex scenarios become relevant at the experimental level.

Going beyond the framework analysed here, we could immediately use our construction to prove security against quantum side information, in specific scenarios, by following the method proposed in [35]. Further, it would be interesting to investigate how our approach can be used for the security analysis of semi-DI-QRNG/QKD protocols where the set of allowed behaviours can be approximated by semidefinite constraints; refer to [12] for relevant examples of such protocols.

Acknowledgements The authors thank Cameron Foreman, Erik Woodhead and Victoria Wright for helpful discussions and feedback on an earlier version of the manuscript.

References

[1] Masahito Hayashi and Toyohiro Tsurumaru. "More efficient privacy amplification with less random seeds via dual universal hash function". IEEE Transactions on Information Theory **62**, 2213–2232 (2016).

[2] Cameron Foreman, Richie Yeung, Alec Edgington, and Florian J. Curchod. "Cryptomite: A versatile and user-friendly library of randomness extractors". Quantum **9**, 1584 (2025).

[3] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N. Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, Timothy A. Manning, et al. "Random numbers certified by Bell's theorem". Nature **464**, 1021–1024 (2010).

[4] Stefano Pironio and Serge Massar. "Security of practical private randomness generation". Physical Review A **87**, 012336 (2013).

[5] Serge Fehr, Ran Gelles, and Christian Schaffner. "Security and composability of randomness expansion from Bell inequalities". Physical Review A **87**, 012335 (2013).

[6] Frédéric Dupuis, Omar Fawzi, and Renato Renner. "Entropy accumulation". Communications in Mathematical Physics **379**, 867–913 (2020).

[7] Yanbao Zhang, Emanuel Knill, and Peter Bierhorst. "Certifying quantum randomness by probability estimation". Physical Review A **98**, 040304 (2018).
[8] Emanuel Knill, Yanbao Zhang, and Peter Bierhorst. "Generation of quantum randomness by probability estimation with classical side information". Physical Review Research **2**, 033465 (2020).
[9] Lynden K. Shalm, Yanbao Zhang, Joshua C. Bienfang, Collin Schlager, Martin J. Stevens, Michael D. Mazurek, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Mohammad A. Alhejji, Honghao Fu, Joel Ornstein, Richard P. Mirin, Sae Woo Nam, and Emanuel Knill. "Device-independent randomness expansion with entangled photons". Nature Physics **17**, 452–456 (2021).
[10] Peter Bierhorst and Yanbao Zhang. "Tsirelson polytopes and randomness generation". New Journal of Physics **22**, 083036 (2020).
[11] Antonio Acín, Serge Massar, and Stefano Pironio. "Randomness versus nonlocality and entanglement". Physical Review Letters **108**, 100402 (2012).
[12] Armin Tavakoli, Alejandro Pozas-Kerstjens, Peter Brown, and Mateus Araújo. "Semidefinite programming relaxations for quantum correlations". Reviews of Modern Physics **96**, 045006 (2024).
[13] Sandu Popescu and Daniel Rohrlich. "Quantum nonlocality as an axiom". Foundations of Physics **24**, 379–385 (1994).
[14] Robert T. Konig and Barbara M. Terhal. "The bounded-storage model in the presence of a quantum adversary". IEEE Transactions on Information Theory **54**, 749–762 (2008).
[15] Renato Renner and Stefan Wolf. "Smooth Renyi entropy and applications". In IEEE International Symposium on Information Theory — ISIT 2004. Page 233. IEEE (2004).
[16] Boris S. Tsirelson. "Some results and problems on quantum Bell-type inequalities". Hadronic Journal Supplement **8**, 329–345 (1993).
[17] Miguel Navascués, Stefano Pironio, and Antonio Acín. "Bounding the set of quantum correlations". Physical Review Letters **98**, 010401 (2007).
[18] Miguel Navascués, Stefano Pironio, and Antonio Acín. "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations". New Journal of Physics **10**, 073013 (2008).
[19] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. "Bell nonlocality". Reviews of Modern Physics **86**, 419–478 (2014).
[20] Olmo Nieto-Silleras, Stefano Pironio, and Jonathan Silman. "Using complete measurement statistics for optimal device-independent randomness evaluation". New Journal of Physics **16**, 013035 (2014).
[21] Jean-Daniel Bancal, Lana Sheridan, and Valerio Scarani. "More randomness from the same data". New Journal of Physics **16**, 033011 (2014).
[22] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. "Proposed experiment to test local hidden-variable theories". Physical Review Letters **23**, 880 (1969).
[23] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau, and Harald Weinfurter. "Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes". Physical Review Letters **119**, 010402 (2017).
[24] Yanbao Zhang, Lynden K. Shalm, Joshua C. Bienfang, Martin J. Stevens, Michael D. Mazurek, Sae Woo Nam, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell,

Honghao Fu, et al. “Experimental low-latency device-independent quantum randomness”. Physical Review Letters **124**, 010505 (2020).

[25] Olmo Nieto-Silleras, Cédric Bamps, Jonathan Silman, and Stefano Pironio. “Device-independent randomness generation from several Bell estimators”. New Journal of Physics **20**, 023049 (2018).

[26] Ravishankar Ramanathan, Michał Horodecki, Hammad Anwer, Stefano Pironio, Karol Horodecki, Marcus Grünfeld, Sadiq Muhammad, Mohamed Bourennane, and Paweł Horodecki. “Practical no-signalling proof randomness amplification using Hardy paradoxes and its experimental implementation”. arXiv preprint arXiv:1810.11648 (2018).

[27] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. “Practical device-independent quantum cryptography via entropy accumulation”. Nature Communications **9**, 459 (2018).

[28] “Quantinuum H1-1. https://www.quantinuum.com/, May, 2023.”.

[29] Pei-Sheng Lin, Denis Rosset, Yanbao Zhang, Jean-Daniel Bancal, and Yeong-Cherng Liang. “Device-independent point estimation from finite data and its application to device-independent property estimation”. Physical Review A **97**, 032309 (2018).

[30] Stefano Pironio. “Lifting Bell inequalities”. Journal of Mathematical Physics**46** (2005).

[31] Erik Woodhead, Boris Bourdoncle, and Antonio Acín. “Randomness versus nonlocality in the Mermin-Bell experiment with three parties”. Quantum **2**, 82 (2018).

[32] Miklos Santha and Umesh V. Vazirani. “Generating quasi-random sequences from semi-random sources”. Journal of Computer and System Sciences **33**, 75–87 (1986).

[33] Lucien Hardy. “Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories”. Physical Review Letters **68**, 2981–2984 (1992).

[34] Gilles Pütz and Nicolas Gisin. “Measurement dependent locality”. New Journal of Physics **18**, 055006 (2016).

[35] Yanbao Zhang, Honghao Fu, and Emanuel Knill. “Efficient randomness certification by quantum probability estimation”. Physical Review Research **2**, 013016 (2020).

[36] Thomas Van Himbeeck and Stefano Pironio. “Correlations and randomness generation based on energy constraints”. arXiv preprint arXiv:1905.09117 (2019).

[37] Wassily Hoeffding. “Probability inequalities for sums of bounded random variables”. The collected works of Wassily HoeffdingPages 409–426 (1994).

[38] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. “Generalised entropy accumulation”. In 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS). Pages 844–850. (2022).

[39] Peter Brown, Hamza Fawzi, and Omar Fawzi. “Device-independent lower bounds on the conditional von Neumann entropy”. Quantum **8**, 1445 (2024).

[40] Fernando G. S. L. Brandão, Ravishankar Ramanathan, Andrzej Grudka, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Tomasz Szarek, and Hanna Wojewódka. “Realistic noise-tolerant randomness amplification using finite number of devices”. Nature Communications **7**, 11345 (2016).

Appendices

A Bounds on smooth min-entropies

A useful tool to bound the total variation distance between two probability distributions of X is the notion of *sub-probability distribution* $\tilde{\nu}(X)$. This is a sub-normalised probability distribution, i.e $\tilde{\nu}(x) \geq 0, \forall x$, and the weight of $\tilde{\nu}$ satisfies $\omega(\tilde{\nu}) := \sum_x \tilde{\nu}(x) \leq 1$. The following lemma is the generalisation of Lemma 1 in [8].

Lemma 3. *Let ν and ν' be probability distributions of X. Then $\|\nu - \nu'\| \leq \epsilon$ if and only if there exists a sub-probability distribution $\tilde{\nu}$ of X, with weight $\omega \geq 1-\epsilon$, satisfying $\tilde{\nu} \leq \nu$ and $\tilde{\nu} \leq \nu'$.*[12]

Proof. If there is $\tilde{\nu}$ such that $\tilde{\nu} \leq \nu$ and $\tilde{\nu} \leq \nu'$, with weight $\omega \geq 1-\epsilon$, we can directly check that $\|\nu - \nu'\| \leq \epsilon$. Start by expressing the total variation as

$$\|\nu - \nu'\| = \sum_x \left(\nu(x) - \nu'(x)\right) \Theta(\nu(x) - \nu'(x)) \,, \tag{44}$$

where $\Theta(y) = 1$ if $y \geq 0$ and $\Theta(y) = 0$ otherwise. Then,

$$\begin{aligned} \|\nu - \nu'\| &= \sum_x \left(\nu(x) - \nu'(x)\right) \Theta(\nu(x) - \nu'(x)) \\ &\leq \sum_x \left(\nu(x) - \tilde{\nu}(x)\right) \leq 1 - \omega \leq \epsilon \,. \end{aligned} \tag{45}$$

In the other direction, if $\|\nu - \nu'\| \leq \epsilon$, we can define a sub-probability distribution as $\tilde{\nu}(x) := \min\{\nu(x), \nu'(x)\}$. Then $\tilde{\nu} \leq \nu$ and $\tilde{\nu} \leq \nu'$ as required. We are left with proving that the weight of $\tilde{\nu}$ is $\omega \geq 1-\epsilon$, which follows from:

$$\begin{aligned} \omega =& \sum_x \min\{\nu(x), \nu'(x)\} \\ =& \sum_x \nu(x) \Theta\left(\nu'(x) - \nu(x)\right) + \sum_x \nu'(x) \Theta\left(\nu(x) - \nu'(x)\right) \\ =& \sum_x \nu(x) \Theta\left(\nu'(x) - \nu(x)\right) + \left(1 - \sum_x \nu'(x) \Theta\left(\nu'(x) - \nu(x)\right)\right) \\ =& 1 - \|\nu - \nu'\| \geq 1 - \epsilon \,. \end{aligned} \tag{46}$$

In the third line we have used the identity

$$1 = \sum_x \nu'(x) = \sum_x \nu'(x) \left[\Theta\left(\nu'(x) - \nu(x)\right) + \Theta\left(\nu(x) - \nu'(x)\right)\right] \,. \tag{47}$$

□

We can immediately use this result to prove the following relation between high-confidence bounds on the min-entropy and the smooth min-entropy. We are using here generic variables C, D and Z, while in the main text we have explicitly represented them as sequences.

Theorem 5 (Theorem 2 in the main text)**.** *If, for all e, $\Pr\left(H_{\min}(D|Z,e) \geq h\right) \geq 1-\epsilon$ then $H^{\epsilon}_{\min}(D|Z,E) \geq h$.*

[12] We use the notation $\nu \leq \nu'$ when $\nu(x) \leq \nu'(x)$ for all x.

Proof. Assume that DZE is distributed according to μ. Define the sub-distribution $\tilde{\nu}$,

$$\tilde{\nu}(D,Z,E) = \mu(D,Z,E)\Theta\left(2^{-h} - \max_{d'} \mu(d'|Z,E)\right), \tag{48}$$

where $\Theta(x) = 1$ if $x \geq 0$ and $\Theta(x) = 0$ otherwise. The weight of $\tilde{\nu}$ is

$$\begin{aligned}\omega &= \sum_{d,z,e} \mu(z,e)\mu(d|z,e)\Theta\left(2^{-h} - \max_{d'} \mu(d'|z,e)\right) \\ &= \sum_{z,e} \mu(z,e)\Theta\left(2^{-h} - \max_{d'} \mu(d'|z,e)\right) \geq 1-\epsilon\,.\end{aligned} \tag{49}$$

Now define ν as

$$\nu(D,Z,E) = \begin{cases} \mu(D,Z,E) & \text{if } \max_{d'} \mu(d'|Z,E) \leq 2^{-h} \\ \frac{1}{|D|}\mu(Z,E) & \text{otherwise.} \end{cases} \tag{50}$$

Since $2^{-h} \geq 1/|D|$ it follows that $\max_d \nu(d|z,e) \leq 2^{-h}$, i.e. $H_{\min,\nu}(D|z,e) \geq h, \forall z,e$. Clearly $\tilde{\nu} \leq \mu$ and $\tilde{\nu} \leq \nu$, and by Lemma 3, $\|\mu - \nu\| \leq \epsilon$. Then $H^{\epsilon}_{\min,\mu}(D|Z,E) \geq h$. □

The following average notion of conditional smooth min-entropy comes in handy for some of the proofs in this paper.

Definition 4. *Let random variables DZE be jointly distributed according to μ. Then D has ϵ-*smooth average ZE-conditional min-entropy *$H^{\epsilon,\text{avg}}_{\min,\mu}(D|Z,E) \geq h$ if there exists a distribution ν such that*

1. $\|\mu - \nu\| \leq \epsilon$,
2. $\mathbb{E}(\max_d \nu(d|ZE)) \leq 2^{-h}$.

Moreover, it is convenient to find a mapping between the average conditional min-entropy and the (worst-case) version in Definition 2. While the latter clearly provides a lower bound on the average version, i.e., if $H^{\epsilon}_{\min,\mu}(D|Z,E) \geq h$ then $H^{\epsilon,\text{avg}}_{\min,\mu}(D|Z,E) \geq h$, a relationship in the opposite direction is not as straightforward. The following theorem establishes that result and is adapted from Lemma 5 in [8] to our (more general) definition of conditional smooth min-entropy in Definition 2.

Lemma 5. *Consider positive constants $p > 0$ and $\delta > 0$. If $H^{\epsilon,\text{avg}}_{\min,\mu}(D|Z,E) \geq -\log(p\delta)$, then $H^{\epsilon+\delta}_{\min,\mu}(D|Z,E) \geq -\log p$.*

Proof. By definition, there exists a distribution ν of DZE such that $\mathbb{E}(\max_d \nu(d|Z,E)) \leq p\delta$ and $\|\mu - \nu\| \leq \epsilon$. Consider the random variable $M(Z,E) = \max_d \nu(d|Z,E)$. Applying the Markov inequality, we get

$$\Pr(M \geq p) \leq \delta. \tag{51}$$

Define

$$\eta(D,Z,E) = \begin{cases} \nu(D,Z,E) & \text{if } \max_{d'} \nu(d'|Z,E) \leq p \\ \frac{1}{|D|}\nu(Z,E), & \text{otherwise.} \end{cases} \tag{52}$$

We will now prove that there exists a sub-distribution $\tilde{\nu}$ with weight $\omega \geq 1-\delta$ such that $\tilde{\nu} \leq \nu$ and $\tilde{\nu} \leq \eta$. Define $\tilde{\nu}(D,Z,E) = \nu(D,Z,E)\Theta(p - \max_{d'} \nu(d'|Z,E))$. It is clear

that $\tilde{\nu} \leq \nu$ and $\tilde{\nu} \leq \eta$ follows from the fact that $p \geq 1/|D|$. Furthermore, the weight of $\tilde{\nu}$ is

$$\begin{aligned}\omega = \sum_{d,z,e} \tilde{\nu}(d,z,e) &= \sum_{d,z,e} \nu(d|z,e)\nu(z,e)\Theta\left(p - \max_{d'} \nu(d'|z,e)\right) \\ &= \sum_{z,e} \nu(z,e)\Theta\left(p - \max_{d'} \nu(d'|z,e)\right) \geq 1-\delta\,,\end{aligned} \tag{53}$$

where the last equality comes from the fact that $\sum_d \nu(d|ze) = 1$ while in the final inequality we used the bound (51). Then, from Lemma 3, $\|\nu - \eta\| \leq \delta$. Using the triangle inequality, we get

$$\|\mu - \eta\| \leq \|\mu - \nu\| + \|\nu - \eta\| \leq \epsilon + \delta\,. \tag{54}$$

Since $\eta(d|z,e) \leq p, \forall d, z, e$, we finally conclude that $H^{\epsilon+\delta}_{\min,\mu}(D|Z,E) \geq -\log p$. □

Theorem 6 (Theorem 3 in the main text)**.** *If, for all e,* $\Pr\left(H_{\min}(D|Z,e) \geq W\right) \geq 1-\kappa$ *and* $p_{Acc} = \Pr(W \geq t)$*, then the* extractable entropy of D *is lower-bounded by*

$$H^{\varepsilon/p_{Acc}}_{\min}(D|Z,E,\texttt{Accept}) \geq t + \frac{\log\kappa}{\beta} + \log(\varepsilon - \kappa)\,. \tag{55}$$

Proof. The proof follows from Lemma 18 in [8], which states that under these conditions the average conditional smooth min-entropy satisfies

$$H^{\kappa/p_{Acc},\mathrm{avg}}_{\min}(D|Z,E,W \geq t) \geq t + \frac{\log\kappa}{\beta} + \log(p_{Acc}). \tag{56}$$

Then,

$$H^{\kappa/p_{Acc},\mathrm{avg}}_{\min}(D|Z,E,W \geq t) \geq t + \frac{\log\kappa}{\beta} + \log(\varepsilon - \kappa) - \log\left(\frac{\varepsilon-\kappa}{p_{Acc}}\right) \tag{57}$$

to which we apply Lemma 5 and finally obtain (55). □

B PEFs and min-trade-off functions

Min-trade-off functions were introduced in the entropy accumulation framework [6] and provide a convenient tool to lower-bound single round entropies. We revisit here a connection between PEFs and min-trade-off functions established in [8], which will later allow us to compare the extractable entropies calculated using both methods.

Consider the *average conditional Shannon entropy* defined as

$$H(D|Z,E) = \sum_e \mu(e)H(D|Z,e) = -\sum_{dze} \mu(e)\mu(dz|e)\log\mu(d|ze)\,, \tag{58}$$

and an affine function $f(\mu) = \sum_{cz} K(c,z)\mu(cz)$ which satisfies

$$f(\mu) \leq H(D|Z,E)\,, \qquad \forall \mu \in \mathcal{S}\,, \tag{59}$$

where $\mathcal{S}$ is the set of allowed behaviours and f is a *min-trade-off function* for $H(D|Z,E)$. The function f can be seen as the expected value of a *min-trade-off estimator* $K = K(C,Z)$

$$\mathbb{E}(K(C,Z)) = f(\mu)\,, \tag{60}$$

where $\mu = \mu(C, Z)$. As a result, the optimal K for a given behaviour p is the solution of the optimisation [36],

$$\begin{aligned} \max_K \quad & \sum_{cz} p(cz)K(c,z) \\ \text{s.t.} \quad & \sum_{cz} \mu(c,z)K(c,z) \leq \sum_{dz} \mu(d,z)(-\log \mu(d|z)) \,, \quad \forall \mu \in \mathcal{S} \,. \end{aligned} \tag{61}$$

There is clear a resemblance between (61) and the single round PEFs optimisation (20). In fact, we will see next that every PEF can be used to define a min-trade-off function (59).

Theorem 7. *Consider a PEF $F(C, Z)$ with power β. Then $\frac{1}{\beta}\log F$ is a (suboptimal) min-trade-off estimator for the average conditional Shannon entropy $H(D|Z, e)$ (58).*

Proof. Applying the log function to condition 2 in the definition of PEF, we have

$$\log \left[\mathbb{E}\left(F(C,Z)\mu(D|Z)^{\beta}\right)\right] \leq 0 \,, \qquad \forall \mu \in \mathcal{S} \,. \tag{62}$$

Since log is a concave function, we can use Jensen's inequality to write (62) as

$$\mathbb{E}\left[\log\left(F(C,Z)\mu(D|Z)^{\beta}\right)\right] + \Delta \leq 0 \,, \qquad \forall \mu \in \mathcal{S} \,, \tag{63}$$

where $\Delta := \log\left[\mathbb{E}(F(C,Z)\mu(D|Z)^{\beta})\right] - \mathbb{E}\left[\log\left(F(C,Z)\mu(D|Z)^{\beta}\right)\right] \geq 0$. From this, we can finally prove that $\log F/\beta$ is a min-trade-off estimator for the conditional Shannon entropy.

$$\mathbb{E}\left[\frac{\log F(C,Z)}{\beta}\right] + \frac{\Delta}{\beta} \leq \mathbb{E}\left[-\log \mu(D|Z)\right] = H(D|Z) \,, \quad \forall \mu \in \mathcal{S} \,. \tag{64}$$

□

Note that due to the Δ/β gap, this estimator will often be suboptimal. In [8], it is proven that in the asymptotic limit of very large n, $\beta \to 0$ and $\frac{1}{\beta}\log F$ tends to an optimal estimator of the average conditional Shannon entropy.

C Extractable entropy from alternative methods

In this section, we give a brief description of how we applied the alternative methods to bound the extractable entropy in Section 4. Since the aim is to compare this with the performance of the PEF method coupled with our proposed polytope approximations, we took the off-the-shelf results which provide the fairest comparison.

C.1 Classical side information: from single round P_{guess} and the Azuma-Hoeffding concentration inequality

The first method to successfully bound the extractable entropy for sequential processes in devices with memory and classical side information was introduced in [3–5]. Here we mainly follow the approach in [4], which derives a lower bound on the extractable entropy using a min-trade-off function for $H_{\min}(D|Z, E) := -\log(\max_{d,z,e} p(d|z, e))$ and the Azuma-Hoeffding concentration inequality [37].

The first step is to find a function that lower bounds the min-entropy for every input z. Consider the generalisation of optimisation (27) described in [25],

$$\begin{aligned} P_{\text{guess}}(D|Z,\Lambda) = \max_{\{\tilde{\mu}_\lambda\}_\lambda} & \sum_{d,z} \tilde{\mu}_{d,z}(d|z) \\ \text{s.t.} & \sum_{d,z} \tilde{\mu}_{d,z}(C|Z) = p(C|Z)\,, \quad \forall \tilde{\mu}_{d,z}(C|Z) \in \widetilde{\mathcal{S}}\,. \end{aligned} \tag{65}$$

The dual problem can be written as

$$\begin{aligned} \min_B & \sum_{c,z} p(c,z)B(c,z) \\ \text{s.t.} & \sum_{c,z} \mu(c,z)B(c,z) \geq \max_{d,z} \mu(d|z)\,, \quad \forall \mu \in \mathcal{Q}\,, \end{aligned} \tag{66}$$

where $\mu(z) = p(z)$. The optimal solution to this problem provides an estimator B, optimised for the typical behaviour p, that satisfies

$$-\log \mathbb{E}_\mu(B) \leq -\log \max_{d,z} \mu(d|z), \qquad \forall \mu \in \mathcal{Q}\,, \tag{67}$$

and therefore $h(\mu) := -\log \mathbb{E}_\mu(B)$ is a min-trade-off function for $H_{\min}(D|Z,E)$, as described in Appendix B.

Following the method described in [4], we use the single round bound (67) combined with the Azuma-Hoeffding inequality to obtain the extractable entropy

$$H_{\min}^{\varepsilon/p_{Acc}}(\mathbf{D}|\mathbf{Z},E,\texttt{Accept}) \geq nt - \gamma\left(2n\ln 1/\kappa\right)^{1/2} - \log 1/(\varepsilon-\kappa)\,, \tag{68}$$

where $h(\mu) \geq t$ is the acceptance criterion and $\gamma = \max|B - \mathbb{E}_\mu(B)|\,, \forall \mu \in \mathcal{Q}$. We obtained the optimal estimator B by solving (66) for the typical behaviours $p(C,Z)$ corresponding to noisy CHSH correlations in Section 4.1.1 and accordingly chose $t = -\log \mathbb{E}_p(B)$.

C.2 Quantum side information: EAT

The entropy accumulation theorem (EAT) introduced in [6] allows us to bound the conditional von Neumann entropy of outputs from a sequential process, and therefore include the general case where an adversary holds quantum side information. In order to treat the framework of the original EAT [6], we assume here that the entangled systems used in the protocol are shared in advance between the parties, becoming inaccessible to the adversary after this preliminary stage. A generalised EAT has been proposed [38] that allows us to relax this assumption, at the cost of lower rates of certified entropy. For this reason, we have decided to compare our results to the original EAT.

Analogously to the previous section, the initial step consists of finding a min-trade-off function f, in this case relative to the von Neumann entropy:

$$f(\mu) \leq \inf_{\sigma \in \Sigma(\mu)} H(C|Z,E)_\sigma\,, \tag{69}$$

where the set $\Sigma(\mu)$ describes all quantum states σ of the system compatible with some behaviour μ.

Although one can in principle optimise f for the typical behaviour p using the Brown-Fawzi-Fawzi (BFF) algorithm [39], this approach was too computationally demanding in all the cases analysed in this paper. We instead ran the algorithm to find min-trade-off

functions f_z for each fixed input z, and from there constructed the min-trade-off function $g(\mu) := \sum_z p(z) f_z(\mu)$, which satisfies

$$g(\mu) \leq \sum_z p(z) \inf_{\sigma \in \Sigma(\mu)} H(C|z,E)_\sigma \leq \inf_{\sigma \in \Sigma(\mu)} \left(\sum_z p(z) H(C|z,E)_\sigma \right) = \inf_{\sigma \in \Sigma(\mu)} H(C|Z,E)_\sigma \,. \tag{70}$$

By direct application of the EAT, the extractable entropy is

$$H_{\min}^{\varepsilon/p_{Acc}}(\mathbf{C}|\mathbf{Z}, E, \texttt{Accept}) \geq nt - \xi\sqrt{n}\,, \tag{71}$$

where $g(\mu) \geq t$ is the chosen acceptance condition and

$$\xi = 2(\log(1+2|C|) + \lceil \|\nabla g\|_\infty \rceil)\sqrt{1 - 2\log\varepsilon}\,, \tag{72}$$

where $\|\cdot\|_\infty$ is the infinity (or maximum) norm. In our analyses, we used the threshold $t = g(p)$.

C.3 Randomness amplification: non-signalling adversaries with classical side information for bipartite Hardy settings

In [26], the authors use the number of random bits at the end of the protocol as their figure of merit, which assumes the use of a specific randomness extractor. Here we are interested in the amount of extractable entropy, which cannot be readily obtained from this reference. We thus go back to the seminal paper [40] and derive an expression for the extractable entropy that can be fairly compared with our results.

We start by using Proposition 3 in Appendix I.E of [26] which ensures that any NS probability distribution $p(AB|XY)$, for which a value h of the MDL inequality (42) is observed, can be bounded by

$$p(A,B|X,Y) \leq 1 - \frac{h}{(\frac{1}{4} - \delta^2)^2}\,. \tag{73}$$

The following results allow us to relate the violation h to the experimentally accessible quantities. Following [26], we define the random variable

$$M^\delta = \begin{cases} -\left(\frac{1}{2}+\delta\right)^2 & \text{if } ABXY = 0101, 1010, 0011 \\ \left(\frac{1}{2}-\delta\right)^2 & \text{if } ABXY = 0000 \\ 0 & \text{otherwise}\,, \end{cases} \tag{74}$$

whose expected value corresponds to $h = \mathbb{E}(M^\delta)$ whenever inputs X and Y are each described by a δ-SV-source. An estimate for h can then be computed by assuming an IID behaviour of the device, leading to a random variable

$$L_\delta = \frac{1}{n}\sum_{i=1}^n M_i^\delta\,, \tag{75}$$

whose values correspond to the experimentally observed violation of the MDL inequality (42). However, from the point of view of an adversary knowledgeable of the memory effects of the device, the corresponding random variable should be given by

$$\overline{L}_\delta = \frac{1}{n}\sum_{i=1}^n \mathbb{E}\left(M_i^\delta | \mathbf{W}_{i-1}, e\right)\,, \tag{76}$$

where $\mathbf{W}_{i-1} = A_1B_1X_1Y_1 \dots A_{i-1}B_{i-1}X_{i-1}Y_{i-1}$ is information accumulated over the past rounds. Lemma 2 of Appendix I.B in [26] uses the Azuma-Hoeffding inequality to obtain the confidence bound

$$\Pr\Big(\overline{L}_\delta \geq L_\delta - s_{Az}\Big) \geq 1 - 2e^{-n\frac{{s_{Az}}^2}{2}} := 1 - \epsilon_{Az}\,, \tag{77}$$

where $s_{Az} \geq 0$ is a constant. The following lemma relates multi-round $\overline{L}_\delta$ to the single round quantity $\overline{M}_i^\delta := \mathbb{E}\left(M_i^\delta | \mathbf{W}_{i-1}, e\right)$.

Lemma 6 (Lemma 3 in Appendix I.B of [26])**.** *If $\overline{L}_\delta \geq l$ then $\overline{M}_i^\delta \geq k$ in, at least, $\frac{l-k}{1/16-k}n$ rounds, for $k \in [0, l]$.*

Let us now define the acceptance threshold of our protocol to be $L_\delta \geq h_{exp}$, where h_{exp} is the observed violation of the MDL inequality (42). In this case, $\overline{L}_\delta \geq h_{exp} - s_{Az}$ with probability given by (77). Moreover, using Lemma 6, we obtain

$$\mu(A_iB_i|X_iY_i, \mathbf{W}_{i-1}, E, L_\delta \geq h_{exp}) \leq 1 - \frac{h_{exp}}{(\frac{1}{4} - \delta^2)^2} =: \gamma \tag{78}$$

in at least a fraction $\alpha(k) := \frac{h_{exp} - s_{Az} - k}{1/16-k}$ of the rounds, for $k \in [0, h_{exp} - s_{Az}]$.

Going back to our concise input/output notation $C = AB$ and $Z = XY$ and using Lemmas 12, 18 and Proposition 19 in Appendix B of [40], we obtain

$$\mathbb{E}\left(\max_{\mathbf{c}} \mu(\mathbf{c}|\mathbf{Z}, E, \texttt{Accept})\right) \leq \frac{\max(\epsilon_{Az}, \gamma^{\alpha n}) + \epsilon_{Az}}{p_{Acc}} \leq \frac{\gamma^{\alpha n} + 2\epsilon_{Az}}{p_{Acc}}\,. \tag{79}$$

From Markov's inequality, we then derive the confidence bound:

$$\Pr\left(\mu(\mathbf{C}|\mathbf{Z}, E, \texttt{Accept}) \geq \frac{\gamma^{\alpha n} + 2\epsilon_{Az}}{\epsilon' + \epsilon_{Az}}\right) \leq \frac{\epsilon' + \epsilon_{Az}}{p_{Acc}}\,, \tag{80}$$

where $\epsilon' \geq 0$ is a free optimisation parameter. Using Theorem 2, we finally obtain the extractable entropy:

$$H_{\min}^{\varepsilon/p_{Acc}}(\mathbf{C}|\mathbf{Z}, E, \texttt{Accept}) \geq \max_k \left(-\log\left(\gamma^{\alpha(k)n} + 2\epsilon_{Az}\right)\right) + \log\varepsilon \tag{81}$$

where $\varepsilon = \epsilon_{Az} + \epsilon'$ is our total security parameter.