npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-024-00879-w

Secure and robust randomness with sequential quantum measurements

Check for updates

Matteo Padovan [1,2], Giulio Foletto [1,5], Lorenzo Coccia [1], Marco Avesani [1], Paolo Villoresi [1,3] & Giuseppe Vallone [1,3,4]

Quantum correlations between measurements of separated observers are crucial for applications like randomness generation and key distribution. Although device-independent security can be certified with minimal assumptions, current protocols have limited performance. Here, we exploit sequential measurements, defined with a precise temporal order, to enhance performance by reusing quantum states. We provide a geometric perspective and a general mathematical framework, analytically proving a Tsirelson-like boundary for sequential quantum correlations, which represents a trade-off in nonlocality shared by sequential users. This boundary is advantageous for secure quantum randomness generation, certifying maximum bits per state with one remote and two sequential parties, even if one sequential user shares no nonlocality. Our simple qubit protocol reaches this boundary, and numerical analysis shows improved robustness under realistic noise. A photonic implementation confirms feasibility and robustness. This study advances the understanding of sequential quantum correlations and offers insights for efficient device-independent protocols.

The effectiveness of information security protocols, whether quantum or classical, relies on specific assumptions. Classical protocols typically make considerations about the computational capabilities of adversaries. On the contrary, the security of quantum protocols is based solely on the validity of quantum theory. However, to leverage this validity in practice, certain assumptions about the implementation are necessary, making the protocol device-dependent. Efforts towards minimizing assumptions for enhanced security evaluation give rise to the device-independent approach in quantum information. A protocol is deemed device-independent when its security remains guaranteed without assumptions about the internal workings of the devices used in its implementation. In these schemes, a physical system prepared in an entangled state is shared and measured by different users, who choose their measurements randomly. Entanglement is necessary to produce correlations that are not reproducible by any local hidden variable theory and are hence referred to as nonlocal. The outcomes serve the dual purpose of manifesting nonlocality and providing a useful classical resource, such as a key or random bit. In principle, the security of this resource is guaranteed by nonlocality even if the devices implementing the protocols are entirely untrusted or controlled by adversaries.

A major drawback of these schemes is the low rate of resource extraction. This is mainly due to the challenges of creating and preserving entanglement, which is degraded by the coupling of the system with the environment. Instead of relying on faster entanglement generation, which may be feasible in the future, we study how to optimize the extraction of useful resources from each single entangled system. A way of doing so proposed in the scientific literature uses weak measurements to realize sequential protocols, in which each quantum system is measured more times[1–9]. Often, they are direct extensions of schemes that use projective measurements, adding further intermediate measurements, and improving the performance in terms of resources extracted from the same quantum system. With the strategy proposed in ref. 4, it is even possible, in principle, to produce an unlimited amount of device-independent randomness for each generated bipartite entangled state. However, the robustness to noise of this protocol is limited and therefore requires great accuracy of realization[9].

At the same time, the appeal of sequential protocols lies in the correlations they can create, for instance, for the possibility of sharing nonlocality among multiple users[10–12]. A geometric approach is useful for characterizing quantum correlations. However, although the geometry of quantum correlations has been the subject of several studies[13–15], its extension to the sequential setting is little known. Most previous analyses focus only on the correlations between each sequential user and the remote one, finding a monogamy trade-off: stronger correlations for one user imply weaker ones for the others[1,4,7,8]. A detailed investigation of the trade-off, its geometry, and its implications could help formulate better quantum protocols that could

[1]Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italy. [2]Centro di Ateneo di Studi e Attività Spaziali Giuseppe Colombo, Università di Padova, Padova, Italy. [3]Padua Quantum Technologies Research Center, Università degli Studi di Padova, Padova, Italy. [4]Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, Padova, Italy. [5]Present address: KTH Royal Institute of Technology, Stockholm, Sweden e-mail: vallone@dei.unipd.it

overcome this compromise[16,17]. Moreover, the literature lacks a general mathematical framework that is useful for characterizing sequential quantum correlations.

In this paper, we characterize sequential quantum correlations with a geometric approach. First, we provide a general mathematical framework useful for describing any sequential quantum scenario. Then, we extend the common two-user, two-measurement, two-outcome scenario with a sequential user on one side and study the geometry of the obtainable correlations, identifying a Tsirelson-like quantum boundary that also serves as monogamy trade-off. This trade-off provides further insights about the sharing of nonlocality between sequential users.

Furthermore, we show that the correlations on the boundary can be used to certify the maximum amount of local randomness obtainable for our scenario, that is, two bits. This is possible regardless of how nonlocality, quantified as violation of a given Bell inequality, is divided between the sequential pairs, meaning that the trade-off for nonlocality is not a trade-off for randomness. Contrary to intuition, the maximal number of bits is attained even if the correlations generated by one of the pairs are entirely local. This is in contrast to previous results in which randomness was generated from nonlocal pairwise correlations[4], and offers a perspective for future works. We also propose an explicit protocol that can generate boundary correlations using states and measurements similar to those that maximally violate the CHSH inequality. Compared to the protocol of ref. 4, which can also achieve two bits of randomness with two dichotomic measurements, ours is simpler as it requires fewer different settings. Furthermore, we show numerically through semidefinite programming techniques that it is more robust to noise, because it is insensitive to the nonlocality trade-off. Our protocol is also simpler than the two proposals of ref. 18, which can also certify two bits of randomness, since it requires fewer measurements, allowing for easier experimental implementation.

Finally, to demonstrate the feasibility and noise resilience of our protocol, we performed a proof-of-concept experimental test based on polarization-entangled photon pairs that generate the correlations required by the protocol. From these correlations, we could certify 39% more random bits than those obtainable with standard non-sequential CHSH protocols in the same noise conditions.

The paper is structured as follows. In the sequential scenario, we introduce a convenient formalism to describe the sequential quantum scenario. In Bounds on the sequential quantum correlations, we show some inequalities in the values of the correlations. In Sequential-CHSH protocol, we propose a protocol to saturate these inequalities: This will lead us to identify part of the boundary of the sequential quantum correlation. In Randomness from correlations, we show how the saturation of the inequalities can be used to certify randomness, supporting the discussion with numerical simulations for some non-ideal cases. Finally, in Experiment, we describe a proof-of-concept sequential quantum experiment based on quantum optics.

Methods

The sequential scenario

We work in the sequential scenario defined in ref. 16, and specifically in a scenario that includes three users: Alice, Bob$_1$, Bob$_2$. A scheme is depicted in Fig. 1. A common source prepares an unknown physical system that is shared and then measured by the untrusted devices operated by the three users. Each user randomly chooses a measurement identified by a binary input $x, y_1, y_2 \in \{0, 1\}$ and obtains as a result a binary output $a, b_1, b_2 \in \{\pm 1\}$. We assume all inputs to be independent of one another, and forbid any communication during data collection between Alice and the Bobs, but we allow unidirectional communication from Bob$_1$ to Bob$_2$ between the production of their respective outputs: This characterizes the sequential correlation scenario that we formally define below.

The main goal of this work is to study the properties of the correlations between inputs and outputs $p(a, \mathbf{b}|x, \mathbf{y}) = p(a, b_1, b_2|x, y_1, y_2)$ that can be generated in this scenario and to see how they can be used to produce device-independent random numbers from the Bobs outputs. We assume that after sufficiently many independent and identically distributed runs, the correlations are known perfectly, neglecting the effects of finite statistics. Moreover, we do not have requirements on the probabilities of the inputs, as long as they allow for the entire reconstruction of the correlations $p(a, \mathbf{b}|x, \mathbf{y})$.

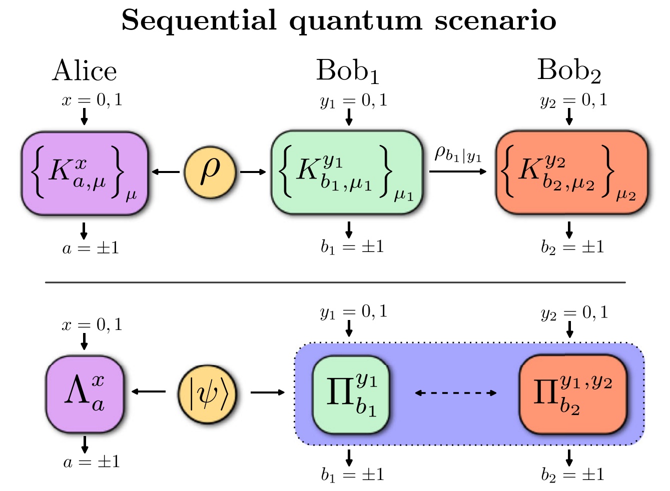

Fig. 1 | Schematic of the sequential scenario. Above, the framework with Kraus operators. Bottom, the projective framework with the operators introduced in the sequential scenario.

The absence of communication means that Alice's marginal probabilities are independent of Bobs' inputs and vice versa. Formally, the correlations must satisfy the no-signaling conditions[13]:

$$\begin{aligned} \sum_a p(a, \mathbf{b}|x, \mathbf{y}) &= \sum_a p(a, \mathbf{b}|x', \mathbf{y}) \quad \forall \mathbf{b}, x, x', \mathbf{y} \\ \sum_{\mathbf{b}} p(a, \mathbf{b}|x, \mathbf{y}) &= \sum_{\mathbf{b}} p(a, \mathbf{b}|x, \mathbf{y}') \quad \forall a, x, \mathbf{y}, \mathbf{y}' \end{aligned} \tag{1}$$

Furthermore, sequentiality implies that Bob$_2$'s input cannot influence Bob$_1$[16]:

$$\sum_{b_2} p(a, b_1, b_2|x, y_1, y_2) = \sum_{b_2} p(a, b_1, b_2|x, y_1, y_2') \quad \forall a, b_1, x, y_1, y_2, y_2' \tag{2}$$

As is common in the context of device-independent protocols, we focus on the set of sequential quantum correlations Q_{SEQ}, i.e. those sequential correlations that can be written using Born rule as

$$p(a, \mathbf{b}|x, \mathbf{y}) = \sum_{\mu,\mu_1,\mu_2} \mathrm{Tr}\left[(K^x_{a,\mu} \otimes K^{y_2}_{b_2,\mu_2} K^{y_1}_{b_1,\mu_1})\rho(K^x_{a,\mu} \otimes K^{y_2}_{b_2,\mu_2} K^{y_1}_{b_1,\mu_1})^\dagger\right] \tag{3}$$

where we have imposed the standard tensor product form to separate Alice and the Bobs[19], and the measurements are described in terms of Kraus operators such that $\sum_{a,\mu} K^x_{a,\mu}{}^\dagger K^x_{a,\mu} = \sum_{b_1,\mu_1} K^{y_1}_{b_1,\mu_1}{}^\dagger K^{y_1}_{b_1,\mu_1} = \sum_{b_2,\mu_2} K^{y_2}_{b_2,\mu_2}{}^\dagger K^{y_2}_{b_2,\mu_2} = \mathbb{1}$ for any input[17]. We note that the sequentiality is reflected in the order of the Kraus operators.

Expression (3) considers that a real implementation of a protocol can be generally described in terms of mixed states and non-projective measurements. However, the shared state can be assumed to be pure because even if the actual is not, it is always possible to consider its purification in a larger Hilbert space without changing the correlations. Similarly, through the Stinespring[20] dilation, the right-hand side of (3) can be rewritten in terms of orthogonal projective measurements satisfying additional constraints in order to guarantee (2) (see Supplementary Methods A and refs. 17,21 for details).

The description in terms of pure states and projective measurements is more convenient for studying the geometry of sequential quantum correlations and we will adopt it in the following. Moreover, as shown in Supplementary Methods A, it can also be rephrased in terms of unitary and hermitian operators (namely measurement operators with only ± 1 eigenvalues) B_{y_1} and B_{y_1,y_2} that satisfy the following constraints:

$$\begin{aligned} &[B_{y_1}, B_{y_1,y_2}] = 0 \\ &B^{\dagger}_{y_1} = B_{y_1},\, B^{\dagger}_{y_1,y_2} = B_{y_1,y_2} \qquad \forall y_1, y_2 \\ &B^{\dagger}_{y_1} B_{y_1} = B^{\dagger}_{y_1,y_2} B_{y_1,y_2} = \mathbb{1}\,. \end{aligned} \tag{4}$$

They can be understood as the observables measured by Bob$_1$ and Bob$_2$. Indeed, the operators B_{y_1} reproduce the statistics of Bob$_1$, while the operators B_{y_1,y_2} reproduce the statistics of Bob$_2$ given that Bob$_1$ has chosen the input y_1. See Fig. 1 for a schematic of the scenario. Similar considerations can be applied to Alice's side to define two unitary and hermitian operators A_x. Without the sequentiality requirement, Alice has no commutation relation analogue to that of (4).

With these definitions, the correlations in the sequential scenario can always be written as

$$p(a, \mathbf{b}|x, \mathbf{y}) = \langle \psi | \Lambda^x_a \otimes \Pi^{y_1}_{b_1} \Pi^{y_1,y_2}_{b_2} | \psi \rangle \tag{5}$$

where Λ^x_a, $\Pi^{y_1}_{b_1}$ and $\Pi^{y_1,y_2}_{b_2}$ are the projectors on the eigenspaces of hermitian operators A_x, B_{y_1} and B_{y_1,y_2} respectively (i.e., $B_{y_1} = \Pi^{y_1}_{+} - \Pi^{y_1}_{-}$ and similarly for Alice and Bob$_2$). The commutation relation in (4) guarantees that the product of the Bobs' projectors can be used to compute a well-defined probability.

Results

Bounds on the sequential quantum correlations

Having introduced the notation, we now present a Tsirelson-like bound satisfied by the sequential quantum correlations.

In our specific case, we are not interested in the operations of Bob$_2$ after Bob$_1$ has chosen the input $y_1 = 1$. This means that we will only consider the marginal probability distribution $p(a, b_1|x, y_1 = 1) = \sum_{b_2} p(a, b_1, b_2|x, y_1 = 1, y_2)$. We are allowed to do this because of sequentiality: Bob$_2$ cannot influence Bob$_1$ and hence $p(a, b_1|x, y_1 = 1)$ is well-defined and does not depend on y_2. Our results are valid regardless of what Bob$_2$ does in this case, we can even think that he does not perform any measurement at all. With this simplification, the association of inputs and measurements is as follows:

$$\begin{array}{cc} \textit{Input sequence} & \textit{Measurements} \\ y_1, y_2 = 0, 0 & B_0 \text{ and } \mathrm{B}_{0,0} \\ y_1, y_2 = 0, 1 & B_0 \text{ and } \mathrm{B}_{0,1} \\ y_1, y_2 = 1, 0 \text{ or } 1, 1 & B_1\,. \end{array} \tag{6}$$

Consequently, we consider the following operators:

$$\begin{aligned} S_1 &\equiv (A_0 + A_1)B_0 + (A_0 - A_1)B_1 \\ S_2 &\equiv (A_0 + A_1)B_{0,0} + (A_0 - A_1)B_{0,1}\,. \end{aligned} \tag{7}$$

These are two CHSH-like operators relative to Alice-Bob$_1$ and Alice-Bob$_2$, respectively, and their mean values can be measured in our scenario from the correlations $p(a, \mathbf{b}|x, \mathbf{y})$ by selecting the values of the inputs that correspond to the relevant observables. Hence, the usual results about CHSH operators also apply, so that in a quantum setting $\langle S_i \rangle \leq 2\sqrt{2}$. Moreover, from conceptually similar results in the literature[1,4,8], one can expect a trade-off between $\langle S_1 \rangle$ and $\langle S_2 \rangle$, therefore it is meaningful to consider an expression that combines the two:

$$S_\theta \equiv \cos 2\theta (S_1 - \sqrt{2}\mathbb{1}) + \sin 2\theta (S_2 - \sqrt{2}\mathbb{1})\,. \tag{8}$$

Furthermore, we introduce the operator

$$S_c \equiv (A_0 + A_1)B_{0,0} + (A_0 - A_1)B_1 \tag{9}$$

whose expected value is a function of part of the statistic of Alice-Bob$_1$ and part of the statistic of Alice-Bob$_2$. This is a well-defined CHSH-like operator, as the relevant observables on the Bobs' side are measured with different inputs: $y_1, y_2 = 1, 0$ or $1, 1$ for B_1 and $y_1, y_2 = 0, 0$ for $B_{0,0}$. Therefore, in a quantum experiment $\langle S_c \rangle \leq 2\sqrt{2}$.

We can express now our main result (proven in Supplementary Methods B) on the geometry of the sequential correlations, which is a bound on $\langle S_1 \rangle$ and $\langle S_2 \rangle$ in the specific case in which $\langle S_c \rangle$ takes its maximum value $2\sqrt{2}$.

Result 1. For any sequential quantum correlation in our scenario, it holds that

$$\langle S_c \rangle = 2\sqrt{2} \quad \Rightarrow \quad \langle S_\theta \rangle \leq \sqrt{2}\,, \quad \forall \theta\,, \tag{10}$$

and there exist correlations that saturate the inequality.

This upper bound on $\langle S_\theta \rangle$ can be interpreted as a monogamy relation between the correlations of Alice-Bob$_1$ and Alice-Bob$_2$. This is different from the trade-offs already present in the literature because S_2 considers Bob$_1$'s input, since $B_{0,0}$ and $B_{0,1}$ are measured only if $y_1 = 0$. Instead, in ref. 1, the quantity similar to S_2 is calculated ignoring the actions of Bob$_1$, while the protocols of refs. 4,8 calculate separate CHSH quantities for each of Bob$_1$'s outputs, adapting Alice's measurements to obtain the highest values.

Sequential-CHSH protocol

In the following, we will provide state and operators that generate correlations for which $\langle S_c \rangle = 2\sqrt{2}$ and $S_\theta = \sqrt{2}$ for any given value of θ, proving that the inequality (10) is tight and identifies a boundary of Q_{SEQ} in our scenario.

In the scheme, Alice and Bob$_1$ share the maximally entangled Bell state $|\phi^+\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ are the eigenstates of the σ_z Pauli matrix.

Alice randomly chooses between two inputs $x \in \{0, 1\}$, corresponding to the two observables

$$A_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}\,, \quad A_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}\,. \tag{11}$$

Bob$_1$ randomly chooses between two inputs $y_1 \in \{0, 1\}$, the latter corresponding to a projective measurement of σ_x and the former to the non-projective measurement realized by the two Kraus operators depending on the parameter θ:

$$\begin{aligned} K_+(\theta) &= \cos\theta |0\rangle\langle 0| + \sin\theta |1\rangle\langle 1|\,, \\ K_-(\theta) &= \cos\theta |1\rangle\langle 1| + \sin\theta |0\rangle\langle 0|\,. \end{aligned} \tag{12}$$

In this expression, the parameter θ is taken to be the same as the one appearing in (8) in order to achieve correlations that saturate the inequality in (10). Its value has a clear physical meaning: it controls the strength of the measurement, in the sense that $\theta = n\frac{\pi}{2}$ leads to a projective measurement of $\pm\sigma_z$, while for $\theta = \frac{\pi}{4} + n\pi$ correspond to a non-interactive measurement. At $\theta = \frac{\pi}{4} + n\frac{\pi}{2}$ the two Kraus operators are equal, up to a sign.

After these operations, if $y_1 = 1$, the protocol ends. Otherwise, for $y_1 = 0$, Bob$_1$ sends the post-measurement state to Bob$_2$, who randomly chooses between the projective measurements of σ_z or σ_x, each corresponding to one of the two inputs $y_2 \in \{0, 1\}$.

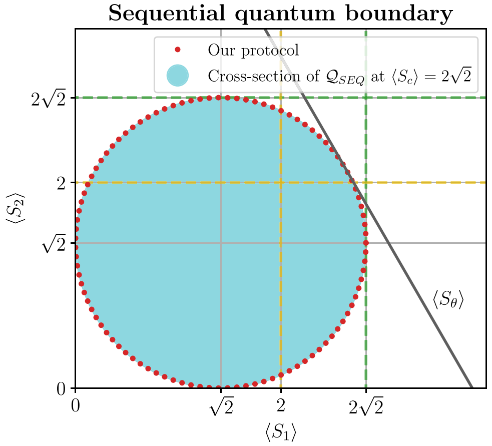

Fig. 2 | Cross-section of the set of sequential quantum correlations, $\mathcal{Q}_{SEQ}$, at $\langle S_c\rangle = 2\sqrt{2}$. The dashed lines denote the maximum values achievable by $\langle S_1\rangle$ and $\langle S_2\rangle$ in the local and non-sequential quantum scenarios, without restrictions on $\langle S_c\rangle$. The red dots mark the geometric location of the correlations achievable with the protocol explained in Sequential-CHSH protocol.

As discussed in Supplementary Methods D, in terms of projective operators, this protocol can be formulated by leaving unchanged A_0 and A_1, while introducing the operators

$$\begin{aligned} B_0 &= \sigma_z \otimes \sigma_z \\ B_1 &= \sigma_x \otimes \mathbb{1}_{B''} \\ B_{0,0} &= \sigma_z \otimes \mathbb{1}_{B''} \\ B_{0,1} &= \sigma_x \otimes \sigma_x \end{aligned} \tag{13}$$

on the Bobs' side. These act on an Hilbert space $\mathcal{H}_{B'} \otimes \mathcal{H}_{B''} = \mathbb{C}^2 \otimes \mathbb{C}^2$. The shared state is now

$$|\psi\rangle = |\phi^+\rangle_{AB'}\left[\cos\theta|0\rangle_{B''} + \sin\theta|1\rangle_{B''}\right] \tag{14}$$

One can verify, using Eqs. (3) and (5), that the sequential and projective formulations give the same correlations, and that the operators B_{y_1} and B_{y_1,y_2} respect all the constraints in Eq. (4). Moreover the relations $\langle S_c\rangle = 2\sqrt{2}$ and $\langle S_\theta\rangle = \sqrt{2}$ hold with the above defined state and operators, proving that the inequality on S_θ is tight and define a boundary, as claimed.

A geometric depiction of this boundary is shown in Fig. 2 and can be deduced by Eq. (8): For each θ, when $\langle S_\theta\rangle = \sqrt{2}$, this equation describe the tangent to a circumference in the $\langle S_1\rangle\langle S_2\rangle$ plane, centered at $(\sqrt{2}, \sqrt{2})$ and of radius $\sqrt{2}$. The points on the circumference are spanned by the protocol just discussed, while the interior of the circle is filled with sequential quantum correlations satisfying $\langle S_c\rangle = 2\sqrt{2}$ and $\langle S_\theta\rangle < \sqrt{2}$.

Randomness from correlations

We can now move to our second main result, which is a statement on the randomness that can be obtained from correlations on the aforementioned boundary of Q_{SEQ}. In this work, we consider only local randomness, originating solely from the side of the Bobs. Given a sequential probability distribution that is observed experimentally $P_{exp}(a, \mathbf{b}|x, \mathbf{y})$, the quantity of device-independent random numbers that can be extracted from the outcomes corresponding to a specific input sequence $\mathbf{y_r}$ can be measured by the (quantum conditional) min-entropy $H_{\min} = -\log_2 G$[22], where G is the maximum guessing probability that an adversary Eve has on the Bobs' outcomes when the input sequence is $\mathbf{y_r}$:

$$G = \max_{p_{ABE}} \sum_{\mathbf{b}} p_{BE}(\mathbf{b}, \mathbf{b}|\mathbf{y_r}) \tag{15}$$

$$\text{s.t.} \quad \begin{aligned} &\textstyle\sum_{\mathbf{e}} p_{ABE}(a, \mathbf{b}, \mathbf{e}|x, \mathbf{y}) = P_{\exp}(a, \mathbf{b}|x, \mathbf{y}), \\ &p_{ABE}(a, \mathbf{b}, \mathbf{e}|x, \mathbf{y}) \in \mathcal{Q}_{SEQ}. \end{aligned} \tag{16}$$

The first condition of Eq. (16) compels Eve to use a strategy p_{ABE} that is compatible with the experimental correlations $P_{\exp}(a, \mathbf{b}|x, \mathbf{y})$. The second means that the strategy is also quantum in the sense explained in the sequential scenario and the sequentiality requirement applies only to the Bobs.

With this definition, we can express the second main result of our work:

Result 2. For any sequential quantum correlation in our scenario such that $\langle S_c\rangle = 2\sqrt{2}$ and $\langle S_\theta\rangle = \sqrt{2}$ for a given $\theta \neq n\frac{\pi}{4}$, the min-entropy is

$$H_{\min} = 2 \text{ bits} \tag{17}$$

when evaluated with the input sequence $\mathbf{y_r} = (0, 1)$. If $\langle S_\theta\rangle = \sqrt{2}$ for some $\theta = n\frac{\pi}{4}$, it reduces to $H_{\min} = 1$ bit.

The proof, provided in Supplementary Methods C, is based on the self-testing properties of the CHSH inequality[23], which are valid because $\langle S_c\rangle = 2\sqrt{2}$, and on the additional necessary conditions that the quantum state and measurements must satisfy in order to saturate also Eq. (10). We emphasize that the demonstration is conducted in a device-independent scenario, and it remains valid regardless of the dimension and specific details of the sequential quantum realization. Examples of states and operators capable of producing 2 bits of randomness are those described in Sequential-CHSH protocol.

Two dichotomic measurements can provide, at most, two random bits. The fact that they achieve this bound, certifies the complete unpredictability of their outcomes. This descends from the features of the entire correlation $P_{exp}(a, \mathbf{b}|x, \mathbf{y})$ and not just from the pairwise ones. Indeed $\langle S_1\rangle$ and $\langle S_2\rangle$ cannot be maximized simultaneously, and the situations in which one is maximized are exactly those for which the randomness drops to one bit. By compromising on their respective nonlocality, Bob$_1$ and Bob$_2$ achieve the best results in terms of randomness. There are even regions on the boundary in which either the correlations between Alice and Bob$_1$ or those between Alice and Bob$_2$ are entirely local, as can be checked by verifying that all CHSH inequalities involving their paired results are respected. Yet, thanks to the three-party correlations, the min-entropy is still maximal at two bits.

However, due to unavoidable experimental imperfections, a real implementation cannot generate ideal correlations that sit exactly at the boundary, therefore it is important to study the amount of device-independent randomness in the interior of Q_{SEQ}. We address this problem numerically using the Navascués-Pironio-Acín (NPA) hierarchy[24,25], and its sequential generalization[17]. This tool replaces the usually difficult-to-verify second condition in (16) with an ordered series of increasingly stringent necessary conditions on linear combinations of the probabilities $p_{ABE}(a, \mathbf{b}, \mathbf{e}|x, \mathbf{y})$. The constraint $p_{ABE}(a, \mathbf{b}, \mathbf{e}|x, \mathbf{y}) \in \mathcal{Q}_{SEQ}$ is retrieved when all conditions are satisfied, but stopping to a finite order k of the series allows casting the problem to a practical semi-definite program (SDP)[26] and restricts p_{ABE} to belong to a set $\mathcal{Q}^k_{SEQ} \supseteq \mathcal{Q}_{SEQ}$[17]. This means that the optimization is performed over a larger set of correlations than what is allowed by quantum mechanics and gives Eve more power than she actually has. The solution of the program is then an upper bound of the actual guessing probability: Finding a value G through the SDP certifies in a device-independent way that the min-entropy of the two outcomes is at least $-\log_2 G$ bits.

Numerical issues could in principle overestimate the min-entropy, but this can be prevented by giving tolerances to the constraints of Eq. (16). These tolerances always benefit Eve and, if chosen much larger than the machine precision, overwhelm its the potentially dangerous effect[27].

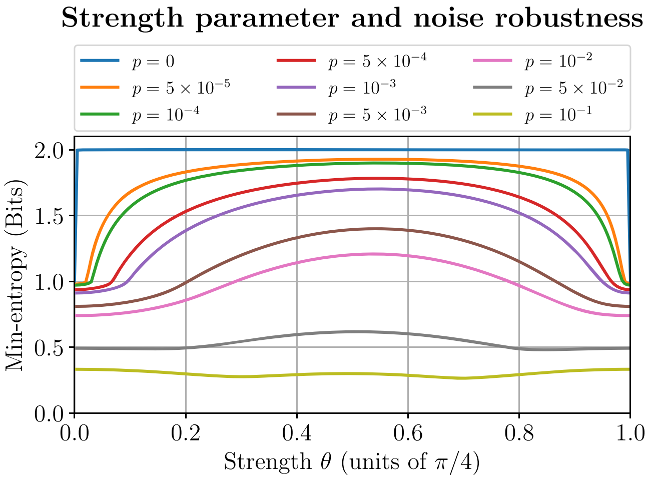

Fig. 3 | Min-entropy from the sequential protocol proposed in Sequential-CHSH protocol as a function of the strength θ for several values of the noise p. Simulations achieved with the NPA order 1 + AB. For $p = 0$ we retrieve the results obtained analytically.

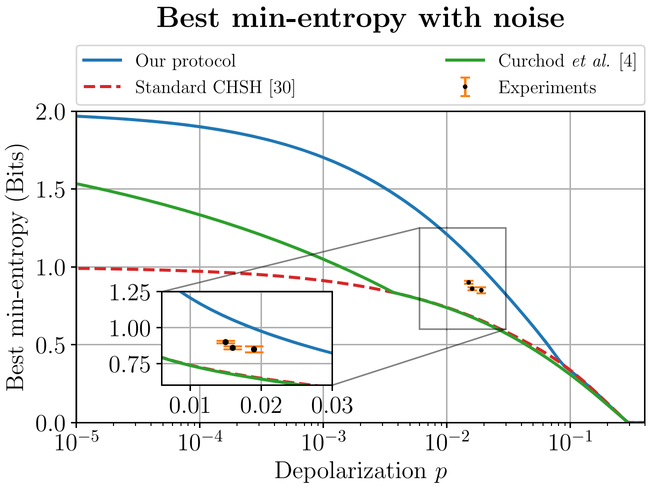

Fig. 4 | Best min-entropy achievable with three different protocols as a function of the depolarization parameter. Our proposal, explained in Sequential-CHSH protocol, the standard CHSH protocol based on numerical optimization (NPA at order 4)[35], and the sequential protocol proposed by ref. 4. The experimental data are subjected to additional type of noise not considered by the curves simulations, such as the c parameter discussed in Experiment.

Rather than computing the min-entropy for all possible values of $\langle S_c\rangle$ and $\langle S_\theta\rangle$, we do it in the context of the protocol explained in Sequential-CHSH protocol, so as to study also its noise robustness. We numerically generate the experimental correlations using the maximally entangled state $|\phi^+\rangle$ mixed with random noise, namely $\rho_{AB} = (1-p)|\phi^+\rangle\langle\phi^+| + p\mathbb{1}/4$, and the measurements required by the protocol. We then set these correlations as constraint in the optimization problem (15). We perform such computation for different values of the strength parameter θ, since, for noisy states, different values of θ could influence the performance of the protocol by imposing different limitations on Eve's strategies. Because of the symmetry of the protocol, it is sufficient to restrict the analysis to $\theta \in [0, \frac{\pi}{4}]$. For such numerical computations we adopt Ncpol2sdpa[28] and the solver SDPA-DD[29], setting a minimal solver precision of 10^{-12} for all the theoretical simulations. The NPA order is 1 + AB[17], which is enough for retrieving the analytical result in the ideal case scenario.

In Fig. 3 we plot the simulation result, which confirms that, in the ideal case ($p = 0$), the min-entropy of the measurements of the protocol is two bits for each value of $\theta \in (0, \frac{\pi}{4})$. When the strength parameter θ is at one of the two extremes, the min-entropy drops to one bit, in agreement with our theoretical result. With the help of the sequential protocol, it is straightforward to understand the drop by observing the state after the measurement of Bob$_1$. For $\theta = 0$, Bob$_1$ measures projectively, hence the state sent to Bob$_2$ is separable and Eve can easily guess the second bit. For $\theta = \frac{\pi}{4}$, the measurements of Bob$_1$ produce no useful correlations and their outcomes are also easily predictable by Eve. Yet, because the measurement is non-interactive, Bob$_2$ still receives a portion of a maximally entangled pair and generates with Alice the perfect correlations that allow him to certify that his outcomes are unpredictable. In both cases, one outcome (and hence one bit) is securely random, and the other is known to Eve.

Figure 3 also shows the impact that the noise quantified by p has on the performance. Intermediate values of θ are optimal, as they are farthest from the extremal points that reduce the randomness even in the ideal case. The approximate flatness of the curve also means that inaccuracies in the setting of θ reduce performance only slightly, simplifying the requirements for the experimental implementation. This descends from the fact that the performance of the noiseless protocol is independent of θ (except for the extremal points). This is in contrast with all other protocols present in the literature, whose optimal performance is obtained for specific values of θ which are close to pathological points[4,9,17].

In Fig. 4, we show the best min-entropy achievable with the sequential protocol as a function of the parameter p. It indicates that it is possible to generate more than one random bit per state even if $p \approx 1.8 \times 10^{-2}$. This value is fairly typical for sources of polarization-entangled photon pairs based on spontaneous parametric down-conversion, and can be reduced with state-of-the-art equipment[30–34]. For comparison, we also plot the min-entropy achievable with a non-sequential protocol that works in the CHSH scenario and uses the NPA hierarchy[35]. We find that the threshold value of p at which the two curves begin to split is approximately 8.5×10^{-2}, meaning that for any smaller value, the sequential protocol performs better than its non-sequential counterpart. The equivalent threshold for the protocol of ref. 4 is a much smaller 3.7×10^{-3} [9].

We point out that this value is in general affected by the finite orders of the NPA hierarchy set in the maximization (15) of the two protocols, which are 1 + AB and 4 respectively.

In a realistic implementation of the sequential scheme (which still neglects finite-size effects), Alice and the Bobs would generate random inputs to select the measurements to be performed on each state. Their choices should be unbalanced, favoring $\mathbf{y} = \mathbf{y_r} = (0, 1)$ for the Bobs, and arbitrarily one of the two observables for Alice. This is to reduce the randomness cost to select the inputs, which, in the asymptotic limit, can be made arbitrarily close to zero bits per state. Alice and the Bobs' devices should receive the inputs and produce the outputs while outside of one another's light cones, to avoid the locality loophole. From the complete list of inputs and outputs gathered in a time interval, Alice and the Bobs should calculate the experimental correlations $P_{\text{exp}}(a, \mathbf{b}|x, \mathbf{y})$ to use in the SDP (15) with the help of the NPA hierarchy. The string of outputs of the Bobs corresponding to $\mathbf{y} = \mathbf{y_r}$ should be considered as consisting of pairs of bits (one from Bob$_1$ and one from Bob$_2$). The average min-entropy corresponding to each pair would be calculated from the guessing probability G resulting from the problem. Finally, the Bobs should reduce the string using a randomness extractor and the knowledge of the min-entropy, producing a shorter but uniform and secure sequence of random bits[36]. The post-processing, consisting of the SDP and the extraction, could be executed during the acquisition of further outputs for a subsequent experimental run, thus reducing its impact on performance. However, the SDP for this protocol can typically be solved in seconds on average personal computers if tackled at level 1 + AB of the NPA hierarchy. This holds independently of the number of samples, as only probabilities are used. The extraction scales at worst quadratically with the length of the raw key, but can be efficiently parallelized[37].

Table 1 | Experimental results of the sequential CHSH experiment

ID	p	c	θ (rad)	$H_{\min}$ (Model) (bits)	$H_{\min}$ (Experiment) (bits)
1	0.019	0.017	0.412	0.82	0.85 ± 0.02
2	0.016	0.012	0.436	0.89	0.86 ± 0.01
3	0.015	0.012	0.357	0.90	0.90 ± 0.01

ID	$\langle S_1\rangle$ (Model)	$\langle S_1\rangle$ (Experiment)	$\langle S_2\rangle$ (Model)	$\langle S_2\rangle$ (Experiment)	$\langle S_c\rangle$ (Model)	$\langle S_c\rangle$ (Experiment)
1	2.305	2.292 ± 0.002	2.388	2.421 ± 0.003	2.751	2.738 ± 0.003
2	2.270	2.268 ± 0.002	2.444	2.433 ± 0.003	2.766	2.760 ± 0.002
3	2.272	2.432 ± 0.002	2.446	2.250 ± 0.003	2.770	2.778 ± 0.002

Level 1+AB of the NPA hierarchy is used. Data retrieved with an exposure time of 100 s (~3 × 10^5 coincidences).

Experiment

We evaluated the protocol presented above with a proof-of-concept experiment, with the goal of verifying the feasibility of meeting the required quality for the entangled state and measurements. For this purpose, we did not create an actual random number generator, but only a setup that reproduces all the quantum operations needed by the protocol, to observe the correlations. Furthermore, we did not include the random inputs but only scanned all the measurement settings one by one. Hence, our setup did not require any randomness source, which would be needed by a true generator. As mentioned before, we can only infer probabilities from our experiment by assuming that the results for each quantum state are independent and identically distributed and neglecting the effects of a finite dataset. We did not close either the detection or the locality loophole, relying instead on fair sampling and on the assumption that Alice and the Bobs do not communicate while producing outcomes (although Bob$_1$ is allowed to send information to Bob$_2$). All of this can only be valid at the proof-of-concept level of our experiment and should be improved for a true implementation of the scheme. Yet, our observations are critical to show the feasibility and experimental robustness of the proposed protocol.

The experimental setup is the same as our previous works and uses polarization-entangled photon pairs and Mach-Zehnder interferometers to implement the Kraus operators (12)[8,9] (see also Supplementary Methods E for a detailed description). Most of the imperfections in this setup can be modeled by a bipartite state of the form

$$\rho_{AB} = (1-p-c)|\phi^+\rangle\langle\phi^+| + p\frac{\mathbb{1}}{4} + c\frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2}\,, \qquad (18)$$

where $p \in [0, 1]$, as above, accounts for the depolarization caused by mixing with random noise, whereas $c \in [0, 1]$ induces decoherence by reducing the extreme antidiagonal terms of the density matrix with respect to the diagonal ones. In optical experiments, this is caused by alignment inaccuracies that increase the distinguishability between the two photons in each pair. The two parameters p and c can be easily estimated experimentally by measuring the visibilities in the $\mathcal{Z}$ and $\mathcal{X}$ bases, indeed $p = 1 - V_{\mathcal{Z}}$ and $c = V_{\mathcal{Z}} - V_{\mathcal{X}}$[9].

We performed three experiments, labeled by an ID $\in \{1, 2, 3\}$. Each of them attempts to reproduce the correlations required by the sequential-CHSH protocol described in Sequential-CHSH protocol and by the standard CHSH protocol. For each experiment, we measured the correlations between Alice and the Bobs and we used them as constraints in an NPA hierarchy but instead of setting the whole statistic $P_{\exp}(a, \mathbf{b}|x, \mathbf{y})$, we constrained only the single-observable mean values $\langle A_x\rangle$, $\langle B_{y_1}\rangle$ and $\langle B_{y_1,y_2}\rangle$, and the two-observable mean values $\langle A_x B_{y_1}\rangle$ and $\langle A_x B_{y_1,y_2}\rangle$, which are all obtainable from the experiment. Doing so allowed us to get around the fact that our simplified experiment can produce results that do not strictly meet the requirements of the protocol. Indeed, during the experiment, the state produced by the source changes slightly. This is mainly due to temperature variations that lead to the movement of the optical components. This affects the interferometers and fiber couplings and, eventually, the experimental probability distribution. Since we are scanning the measurements one by one, we are effectively using different states for each measurement, in contrast with Eq. (3). Constraining all correlations would have prevented the SDP from finding a proper solution, whereas our relaxed constraints allowed us to find one with a small solver tolerance of 10^{-12}[29]. In general, this approach does not introduce security issues, since having a smaller number of constraints only gives more power to Eve and finds a min-entropy that is lower than what could be achieved by considering all the correlations. The execution of the SDP was carried out on a personal computer and took less than 10 s.

Table 2 | Experimental results of the CHSH experiment

ID	$\langle S\rangle$ (Experiment)	$H_{\min}$ (Model) (bits)	$H_{\min}$ (Experiment) (bits)
1	2.761 ± 0.003	0.60	0.61 ± 0.01
2	2.772 ± 0.003	0.63	0.64 ± 0.01
3	2.797 ± 0.002	0.64	0.73 ± 0.01

$\langle S\rangle$ is the CHSH value and for the min-entropy the analytical bound is used[39]. Data retrieved with an exposure time of 100 s (~3 × 10^5 coincidences).

We also compared the results with those predicted by our model using the same constraints, with the values of p, c, and θ that best fit the experimental data. We calculated the statistical errors on the experimental results as standard deviations of a sample of 300 simulated experiments. In each of these, the photon counts descend from a Poisson distribution whose mean value is the experimental datum.

Tables 1 and 2 summarize the results of all three experiments, reporting the min-entropies and the mean values of the CHSH quantities $\langle S_1\rangle$, $\langle S_2\rangle$, $\langle S_c\rangle$, and $\langle S\rangle$ (which is measured in the non-sequential scenario). They show that our protocol not only is feasible but can overcome the rate of the standard CHSH scheme in real world implementations. Indeed, we found min-entropies between 0.82 and 0.90 bits, or between 23% and 39% higher than those obtained in the non-sequential scenario with the same states, even with visibilities $V_{\mathcal{Z}}\approx 98\%$ and $V_{\mathcal{X}}\approx 97\%$, which are readily accessible to entangled-photon sources built with commercial components.

In addition, the comparison between our results and the predictions of the model show that the latter can be used to evaluate the performance of this type of schemes. The discrepancies can be attributed to other static imperfections in the setup which are not considered by the model and to the aforementioned changes of the state from one measurement to the next.

Discussion

In this work, we studied the set of sequential quantum correlations through a geometric perspective. Initially, we presented a general mathematical framework applicable to describing any sequential quantum scenario. Using this framework in the context of one party on one side and two sequential parties on the other, we identified a Tsirelson-like quantum boundary. This boundary can be interpreted as a monogamy trade-off between the amounts of nonlocality of the sequential users shared with the remote one. Despite this trade-off, we proved analytically that the correlations on the boundary certify the maximal amount of randomness in our device-independent scenario, specifically, two bits (excluding exceptional cases). This result introduces a fundamental perspective: a trade-off for nonlocality does not necessarily translate into one for randomness. In simpler terms, even if the correlations of one sequential user with the spatially separated one are explicable through local hidden variable theories, they can contribute to the generation of secure randomness when considered *jointly* with the correlations of the other users.

We also proposed an explicit simple qubit-based protocol to generate the correlations on the boundary in the ideal case, and we numerically studied its noise robustness, finding that it can beat the non-sequential CHSH protocol for depolarization $p \lesssim 8.5 \times 10^{-2}$ and produce more than one random bit for $p \lesssim 1.8 \times 10^{-2}$, values that are feasible to achieve with current technologies.

Finally, we implemented a proof-of-concept experiment, demonstrating not only the feasibility of our protocol, but also that it can perform better than the non-sequential CHSH-based scheme with real-world systems. Indeed, we overcame the min-entropy of the latter by 23% to 39%, and produced 0.90 ± 0.01 bits in our best run. To the best of our knowledge, this is the first experimental observation of the advantage of a sequential protocol with respect to its one-step counterpart in terms of randomness generation.

On the basis of this work, we envisage further steps as follows. When correlations lie on a quantum boundary, it may happen that they identify, or self-test, a unique (up to local isometries) quantum representation that realizes them[23,38]. It would be interesting to understand if this can happen also in the sequential case and whether the correlations of our protocol can self-test the state and measurements that produce them.

In addition, other portions of the boundary in this scenario might prove useful. A possible avenue is to relax the condition $\langle S_c \rangle = 2\sqrt{2}$ and study the bounds for $\langle S_\theta \rangle$. Our formalization of quantum sequential correlations in terms of commuting projective measurements might be helpful, but if boundary features cannot be analytically probed, the sequential extension of the NPA hierarchy can be used[17]. It could also be meaningful to consider other parameterizations of the boundary. For example, the upper bound of Eq. (10) can equivalently be written in terms of

$$S'_\alpha \equiv \cos\alpha\, S_+ + \sin\alpha\, S_- \tag{19}$$

as

$$\langle S'_\alpha \rangle \leq 2\,, \tag{20}$$

with $S_\pm = (A_0 + A_1)B_0 \pm (A_0 - A_1)B_{0,1}$. This expression, detailed in Supplementary Methods B, gives the boundary represented in Fig. 5. Without constraining $\langle S_c \rangle = 2\sqrt{2}$ and without the commutation relations of Eq. (4) (derived from sequentiality), the Tsirelson-like bound of $\langle S' \rangle$ is relaxed to $2\sqrt{2}$, leading to a relation similar to the one in[14]. Due to this greater similarity with the existing literature, S'_α might be easier to investigate than S_θ.

Our protocol could also be more thoroughly investigated in its robustness to losses. The standard way to treat losses in device-independent schemes is to assign the no-output events to one of the legitimate outputs. In our case, this would cause the correlations to fall from the boundary and into the interior of Q_{SEQ}. Could this be partially compensated for with a different set of states and measurements?

It would also be interesting to study whether the protocol can be extended to more Bobs. This stems from the intuition that the independence of the min-entropy from the strength parameter is due to the sequence of two mutually unbiased measurements, σ_z and σ_x. This opens up the possibility of adding a third sequential party measuring σ_y: In this case, the bits would be extracted from a sequence of three mutually unbiased observables.

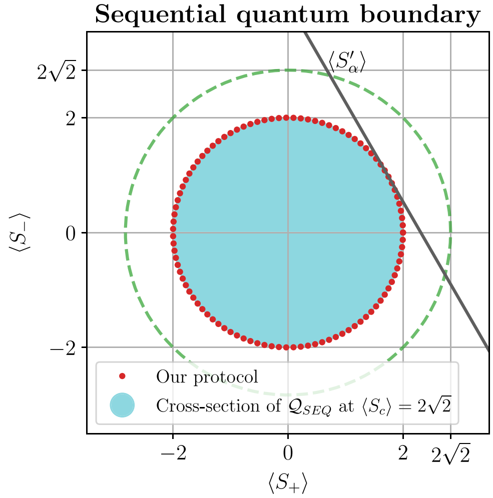

Fig. 5 | Cross-section of the sequential quantum set at $\langle S_c \rangle = 2\sqrt{2}$ in the parametrization $\langle S_\pm \rangle$. The dashed circumference denotes the maximum values achievable in non-sequential quantum scenarios, without restrictions on $\langle S_c \rangle$. The red dots mark the geometric location of the correlations achievable with the protocol explained in Sequential-CHSH protocol.

Is it then possible to achieve three bits regardless of the strength parameters under ideal conditions? Could the noise robustness of such a protocol be enough for real-world implementations? A limitation might be the complexity of the SDP, which grows considerably with the number of Bobs.

In conclusion, this work offers tools and results that can improve our understanding of sequential quantum correlations and the performance of randomness generation protocols. The formulation in terms of products of commuting measurements might provide a more intuitive description and suggest interesting points of view from which to analyze a given scenario. For example, it can be used for the investigation of the sharing of nonlocality[10–12]. The boundary correlations we studied highlight that the greatest quantum advantage is reached using the entire set of experimental probabilities, and not just the pairwise ones. This paves the way for further studies on the complex relationship between nonlocality and randomness and can improve the performance of device-independent random number generators with present-day technologies.

Data availability

Data is available from the corresponding author upon reasonable request.

Code availability

The codes used for the simulations for this paper are available from the corresponding author upon reasonable request.

Received: 23 February 2024; Accepted: 16 August 2024;
Published online: 30 September 2024

References

1. Silva, R., Gisin, N., Guryanova, Y. & Popescu, S. Multiple observers can share the nonlocality of half of an entangled pair by using optimal weak measurements. *Phys. Rev. Lett.* **114**, 250401 (2015).
2. Mal, S., Majumdar, A. S. & Home, D. Sharing of nonlocality of a single member of an entangled pair of qubits is not possible by more than two unbiased observers on the other wing. *Mathematics* **4** https://www.mdpi.com/2227-7390/4/3/48 (2016).
3. Schiavon, M., Calderaro, L., Pittaluga, M., Vallone, G. & Villoresi, P. Three-observer bell inequality violation on a two-qubit entangled state. *Quantum Sci. Technol.* **2**, 015010 (2017).
4. Curchod, F. J. et al. Unbounded randomness certification using sequences of measurements. *Phys. Rev. A* **95**, 020102 (2017).

5. Hu, M.-J. et al. Observation of non-locality sharing among three observers with one entangled pair via optimal weak measurement. *npj Quant. Inf.* **4**, 63 (2018).
6. Tavakoli, A. & Cabello, A. Quantum predictions for an unmeasured system cannot be simulated with a finite-memory classical system. *Phys. Rev. A* **97**, 032131 (2018).
7. Brown, P. J. & Colbeck, R. Arbitrarily many independent observers can share the nonlocality of a single maximally entangled qubit pair. *Phys. Rev. Lett.* **125**, 090401 (2020).
8. Foletto, G. et al. Experimental certification of sustained entanglement and nonlocality after sequential measurements. *Phys. Rev. Appl.* **13**, 044008 (2020).
9. Foletto, G. et al. Experimental test of sequential weak measurements for certified quantum randomness extraction. *Phys. Rev. A* **103**, 062206 (2021).
10. Cheng, S., Liu, L., Baker, T. J. & Hall, M. J. W. Limitations on sharing bell nonlocality between sequential pairs of observers. *Phys. Rev. A* **104**, L060201 (2021).
11. Cheng, S., Liu, L., Baker, T. J. & Hall, M. J. W. Recycling qubits for the generation of bell nonlocality between independent sequential observers. *Phys. Rev. A* **105**, 022411 (2022).
12. Steffinlongo, A. & Tavakoli, A. Projective measurements are sufficient for recycling nonlocality. *Phys. Rev. Lett.* **129**, 230402 (2022).
13. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
14. Christensen, B. G., Liang, Y.-C., Brunner, N., Gisin, N. & Kwiat, P. G. Exploring the limits of quantum nonlocality with entangled photons. *Phys. Rev. X* **5**, 041052 (2015).
15. Goh, K. T. et al. Geometry of the set of quantum correlations. *Phys. Rev. A* **97**, 022104 (2018).
16. Gallego, R., Würflinger, L. E., Chaves, R., Acín, A. & Navascués, M. Nonlocality in sequential correlation scenarios. *N. J. Phys.* **16**, 033037 (2014).
17. Bowles, J., Baccari, F. & Salavrakos, A. Bounding sets of sequential quantum correlations and device-independent randomness certification. *Quantum* **4**, 344 (2020).
18. Acín, A., Pironio, S., Vértesi, T. & Wittek, P. Optimal randomness certification from one entangled bit. *Phys. Rev. A* **93**, 040102 (2016).
19. Navascués, M., Cooney, T., Pérez-García, D. & Villanueva, N. A physical approach to tsirelson's problem. *Found. Phys.* **42**, 985–995 (2012).
20. Stinespring, W. F. Positive functions on c*-algebras. *Proc. Am. Math. Soc.* **6**, 211–216 (1955).
21. Neumark, M. On a representation of additive operator set functions. *C.R. Acad. Sci. URSS* **41**, 359 (1943).
22. Brown, P. J., Ragy, S. & Colbeck, R. A framework for quantum-secure device-independent randomness expansion. *IEEE Trans. Inf. Theory* **66**, 2964–2987 (2020).
23. Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. *Quantum* **4**, 337 (2020).
24. Navascués, M., Pironio, S. & Acín, A. Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98**, 010401 (2007).
25. Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *N. J. Phys.* **10**, 073013 (2008).
26. Boyd, S. & Vandenberghe, L.Convex Optimization (Cambridge University Press, 2004).
27. Winick, A., Lütkenhaus, N. & Coles, P. J. Reliable numerical key rates for quantum key distribution. *Quantum* **2**, 77 (2018).
28. Wittek, P. Algorithm 950: Ncpol2sdpa-sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables. *ACM Trans. Math. Softw.* **41**, 1–12 (2015).
29. Nakata, M. A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: Sdpa-gmp, -qd and -dd. In *2010 IEEE International Symposium on Computer-Aided Control System Design* (IEEE, https://doi.org/10.1109/CACSD.2010.5612693 2010).
30. Poh, H. S., Joshi, S. K., Cerè, A., Cabello, A. & Kurtsiefer, C. Approaching Tsirelson's bound in a photon pair experiment. *Phys. Rev. Lett.* **115**, 180408 (2015).
31. Liu, Y. et al. Device-independent quantum random-number generation. *Nature* **562**, 548–551 (2018).
32. Liu, W.-Z. et al. Device-independent randomness expansion against quantum side information. *Nat. Phys.* **17**, 448–451 (2021).
33. Li, M.-H. et al. Experimental realization of device-independent quantum randomness expansion. *Phys. Rev. Lett.* **126**, 050503 (2021).
34. Liu, W.-Z. et al. Toward a photonic demonstration of device-independent quantum key distribution. *Phys. Rev. Lett.* **129**, 050502 (2022).
35. Nieto-Silleras, O., Pironio, S. & Silman, J. Using complete measurement statistics for optimal device-independent randomness evaluation. *N. J. Phys.* **16**, 013035 (2014).
36. Trevisan, L. & Vadhan, S. Extracting randomness from samplable distributions (2000).
37. Tang, B.-Y., Liu, B., Zhai, Y.-P., Wu, C.-Q. & Yu, W.-R. High-speed and large-scale privacy amplification scheme for quantum key distribution. *Sci. Rep.* **9**, 15733 (2019).
38. Franz, T., Furrer, F. & Werner, R. F. Extremal quantum correlations and cryptographic security. *Phys. Rev. Lett.* **106**, 250502 (2011).
39. Pironio, S. et al. Random numbers certified by bell's theorem. *Nature* **464**, 1021–1024 (2010).

Acknowledgements

We would like to thank Dr. Flavio Baccari (Max Planck Institute of Quantum Optics), Prof. Stefano Pironio (Université Libre de Bruxelles), and Dr. Peter Brown (Télécom Paris) for the useful discussions and clarifications. The computational resources offered by the CAPRI initiative (University of Padova Strategic Research Infrastructure Grant 2017: "CAPRI: Calcolo ad Alte Prestazioni per la Ricerca e l'Innovazione") and BLADE cluster are acknowledged. Part of this work was supported by Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) (Italian Ministry of Education, University and Research) under the initiative "Departments of Excellence" (Law No. 232/2016), by Fondazione Cassa di Risparmio di Padova e Rovigo within the call "Ricerca Scientifica di Eccellenza 2018", project QUASAR, by the European Union's Horizon 2020 research and innovation programme, project QUANGO (grant agreement No. 101004341), and by the project "Quantum Security Networks Partnership" (QSNP, grant agreement No. 101114043).

Author contributions

M.P., G.F., L.C., and G.V. provided analytical proofs. M.P. conducted numerical simulations. M.P. carried out the experiment and analyzed the results, with assistance from G.F. and L.C. during setup preparation. M.A., P.V., and G.V. supervised the work. All authors participated in result discussions and contributed to the final manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-024-00879-w.

Correspondence and requests for materials should be addressed to Giuseppe Vallone.

Reprints and permissions information is available at http://www.nature.com/reprints