

## ARTICLE OPEN



# Single trusted qubit is necessary and sufficient for quantum realization of extremal no-signaling correlations

Ravishankar Ramanathan<sup>1✉</sup>, Michał Banacki<sup>2,3</sup>, Ricard Ravell Rodríguez<sup>2</sup> and Paweł Horodecki<sup>2,4</sup>

The problem of achieving security of device-independent (or semi-device-independent) cryptography (for quantum key distribution and randomness generation) against the most general no-signaling adversaries has remained open. It has been recognized that the realization of extremal no-signaling non-local boxes (or extremal no-signaling non-local assemblages) could provide a route toward devising such highly secure protocols. We first prove a general no-go result that in the Bell non-locality scenario, quantum theory does not allow us to realize any extremal no-signaling non-local box, even if scenarios of arbitrary sequential measurements are considered. On the other hand, we secondly prove a positive result showing that a one-sided device-independent scenario where a single party trusts their qubit system is already sufficient for quantum theory to realize a self-testing extremal non-local point within the set of no-signaling assemblages.

*npj Quantum Information* (2022)8:119; <https://doi.org/10.1038/s41534-022-00633-0>

## INTRODUCTION

Correlations in entangled states cannot be realized by local hidden variables theories where results of measurements on subsystems are locally predetermined<sup>1–3</sup>. This phenomenon evidenced by the violation of Bell inequalities<sup>4,5</sup> led to the powerful idea of device-independent (DI) cryptography<sup>6–10</sup> where no assumption on the nature of the quantum systems subject to measurement needs to be made. In the DI setting, security is ultimately based on the observation of non-local correlations by honest parties and the property of monogamy of quantum non-local correlations<sup>11,12</sup>. A stronger property than monogamy is that of extremality of the measurement statistics, i.e., the observation of extremal behavior by honest parties within the set of all measurement behaviors. Such extremal behavior guarantees that their system is completely decoupled from that of any adversary. For any such extremal behavior, one can also find a Bell inequality that is maximally violated by the extremal statistics. Moreover, in certain cases, such a violation even permits the self-testing<sup>13</sup> of the quantum pure state measured, i.e., its uniqueness up to irrelevant local operations.

This analysis can be carried over into general probabilistic theories beyond quantum theory<sup>14</sup> that only obey the no-signaling condition of relativity. In this case, there are families of statistics called no-signaling boxes that obey the no-signaling constraints but may otherwise be super-quantum, and as such may violate Bell inequalities more strongly than quantum boxes, the quintessential example here being the Popescu–Rohrlich (PR) box<sup>15</sup>. The extremality of a family of statistics in any such no-signaling theory then means that it is uncorrelated from other measurement behaviors (boxes) and as such is very useful in realizing secure DI protocols.

Later, the weaker scenario of semi-DI schemes has been developed in the setting where some of the parties may be considered to have full control of the quantum systems in their laboratory (see<sup>16</sup>). Here, instead of just the measurement

statistics, one considers quantum assemblages, and instead of Bell inequalities, one considers the so-called steering inequalities (see<sup>17</sup>). Similarly, just as the no-signaling boxes, one considers here the no-signaling assemblages only constrained by the no-signaling conditions<sup>18</sup>.

The interesting question whether quantum DI cryptography can stay secure against a general no-signaling adversary has been posed<sup>10</sup>. Some partial positive results have been provided in problems of secret key<sup>10</sup> or randomness amplification<sup>19–21</sup>. These proofs uniformly utilize quantum measurement behaviors that do not represent extremal points in the set of no-signaling behaviors. It was recognized that if one could realize such extremal postquantum behaviors by measurements on quantum states, then the security proofs could be much more streamlined. Hence, the natural question was whether there is any scenario in which quantum correlations give rise to extremal no-signaling behaviors.

An important, though partial, a negative result in this direction was obtained in<sup>22</sup> where it was shown that in the usual Bell non-locality framework, there exists no scenario (number of parties, measurement settings, or outcomes) in which quantum correlations represent an extremal point in the set (convex polytope) of no-signaling boxes. The question whether the same is true in more general correlation scenarios such as that of sequential Bell non-locality<sup>23</sup> or in quantum steering scenarios<sup>18</sup> was left unanswered.

Here we provide complete answers to both these questions. First, we extend the no-go result of<sup>22</sup> to the general scenario of sequential Bell non-locality<sup>23</sup>: quantum sequential non-local correlations cannot realize extremal no-signaling behaviors, irrespective of the number of measurement settings or outcomes. Second, we also provide a positive answer in the setting of steering inequalities: if one of the parties has a fully trusted qubit system then there exist situations where quantum assemblages are extremal within general no-signaling assemblages. Crucially, the latter result holds in the setting of three-party steering where quantum assemblages have been shown to be a strict subset of

<sup>1</sup>Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong, Hong Kong. <sup>2</sup>International Centre for Theory of Quantum Technologies, University of Gdańsk, Jana Bażyńskiego 1A, 80-309 Gdańsk, Poland. <sup>3</sup>Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland. <sup>4</sup>Faculty of Applied Physics and Mathematics, National Quantum Information Centre, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland. ✉email: ravi@cs.hku.hk

the set of no-signaling assemblages. This result, in view of the unrealisability of super-quantum boxes such as the PR box in non-locality and the consequences thereof<sup>5,24</sup>, should have further implications both in quantum foundations and in the development of semi-DI cryptography secure against no-signaling adversaries.

## RESULTS

### Extremality in sequential Bell non-locality

We begin with the scenario of sequential Bell non-locality<sup>23</sup>, where each party performs measurements on their system in a sequential manner, leading to a time-ordered no-signaling (TONS) structure and the corresponding inequalities consider correlations between outcomes obtained in sequential runs. This scenario is in many ways richer than the usual Bell non-locality scenario, with the appearance of novel phenomena such as “hidden non-locality”<sup>25</sup>, wherein some quantum states only display local correlations in traditional Bell experiments while exhibiting non-local correlations when correlations are considered also between outcomes of measurements performed in sequence by each party. Here, one party Alice chooses to measure one of  $m_A^{(j_A)}$  inputs  $i_A^{(j_A)} = 1, \dots, m_A^{(j_A)}$  in the  $j_A$ th run of the Bell experiment, and obtains one of  $d_A^{(j_A)}$  outputs  $o_A^{(j_A)} \in \{1, \dots, d_A^{(j_A)}\}$ . Similarly, the other party Bob chooses to measure in the  $j_B$ th run, one of  $m_B^{(j_B)}$  inputs  $i_B^{(j_B)} = 1, \dots, m_B^{(j_B)}$ , and obtains one of  $d_B^{(j_B)}$  outputs  $o_B^{(j_B)} \in \{1, \dots, d_B^{(j_B)}\}$  outputs. Here,  $j_A = 1, \dots, N_A$  and  $j_B = 1, \dots, N_B$  where  $N_A, N_B$  denote the number of measurement runs of Alice and Bob, respectively. Such a sequential Bell scenario is denoted by  $\mathbf{B}(2; (\vec{m}_A, \vec{d}_A); (\vec{m}_B, \vec{d}_B))$ , where  $\vec{m}_A := (m_A^{(1)}, \dots, m_A^{(N_A)})$ ,  $\vec{d}_A := \left( (d_{A,1}^{(1)}, \dots, d_{A,m_A^{(1)}}^{(1)}), \dots, (d_{A,1}^{(N_A)}, \dots, d_{A,m_A^{(N_A)}}^{(N_A)}) \right)$ . We will simplify the notation by choosing  $m_A^{(j_A)} = m_B^{(j_B)} = m$ ,  $d_A^{(j_A)} = d_B^{(j_B)} = d$  for all  $j_A, j_B$ , and  $N_A = N_B = N$  where this does not affect the generality of the argument. The joint probability of obtaining the outcomes  $\mathbf{o}_A := (o_A^{(1)}, \dots, o_A^{(N)})$  for Alice, and  $\mathbf{o}_B := (o_B^{(1)}, \dots, o_B^{(N)})$  for Bob, for given measurement settings  $\mathbf{i}_A := (i_A^{(1)}, \dots, i_A^{(N)})$  and  $\mathbf{i}_B := (i_B^{(1)}, \dots, i_B^{(N)})$ , respectively, will be denoted by  $P_{\mathbf{o}_A, \mathbf{o}_B | \mathbf{i}_A, \mathbf{i}_B}(\mathbf{o}_A, \mathbf{o}_B | \mathbf{i}_A, \mathbf{i}_B)$ . As before, we may view these  $n_{\text{seq}} := (md)^{2N}$  probabilities as forming the components of a vector  $P_{\mathbf{o}_A, \mathbf{o}_B | \mathbf{i}_A, \mathbf{i}_B} = |P\rangle$  in  $\mathbb{R}^{n_{\text{seq}}}$ , and are described as forming a box  $P$ .

We consider the set of general TONS boxes in the scenario of sequential non-locality as obeying the TONS constraints (where there is no-signaling between all rounds of Alice and all rounds of Bob, while signaling is allowed between past rounds of Alice (Bob) to future rounds of Alice (Bob)) in addition to those of normalization and non-negativity, and denote this set as  $\mathbf{TONS}[\mathbf{B}(2; (\vec{m}_A, \vec{d}_A); (\vec{m}_B, \vec{d}_B))]$ . The important subset of TONS boxes is the classical time-ordered local deterministic polytope, denoted by  $\mathbf{TOLoc}[\mathbf{B}(2; (\vec{m}_A, \vec{d}_A); (\vec{m}_B, \vec{d}_B))]$ , which is the convex hull of all boxes where all entries are integral, i.e., in  $\{0, 1\}$ . The boxes obtainable by performing general sequential quantum measurements on a quantum state of arbitrary dimension form the set of sequential quantum correlations denoted by  $\mathbf{Qseq}[\mathbf{B}(2; (\vec{m}_A, \vec{d}_A); (\vec{m}_B, \vec{d}_B))]$ . These sets are defined explicitly in Supplementary Note 1. We ask the question whether quantum correlations can realize the extremal boxes of the general TONS polytope, where an extremal box or a vertex is

one that cannot be expressed as a non-trivial convex combination of boxes in the polytope. This fundamental question in quantum foundations gains additional interest in DI quantum cryptography due to the simple but powerful fact that extremal quantum correlations are automatically decoupled from any systems held by any no-signaling adversary<sup>14</sup>. By considering an extension to the scenario of sequential non-locality<sup>26,27</sup> of the well-known NPA hierarchy<sup>28</sup> of semi-definite programming relaxations to the set of quantum correlations, and developing the techniques from<sup>22</sup> to this scenario, we prove (see detailed description in Supplementary Note 1) the following.

**Theorem 1** For any  $(\vec{m}_A, \vec{d}_A), (\vec{m}_B, \vec{d}_B)$  let  $P$  be an extremal box of the TONS polytope  $\mathbf{TONS}[\mathbf{B}(2; (\vec{m}_A, \vec{d}_A); (\vec{m}_B, \vec{d}_B))]$  such that  $P \notin \mathbf{TOLoc}[\mathbf{B}(2; (\vec{m}_A, \vec{d}_A); (\vec{m}_B, \vec{d}_B))]$ . Then,  $P \notin \mathbf{Qseq}[\mathbf{B}(2; (\vec{m}_A, \vec{d}_A); (\vec{m}_B, \vec{d}_B))]$ . The latter stays true even when the no-signaling constraints are relaxed to allow signaling from the  $j$ th run of Alice (Bob) to the  $j+k$ th run of Bob (Alice) for all  $j = 1, \dots, n, k \geq 1$ .

Together with the results from<sup>22</sup> the above theorem rules out the quantum realization of extremal postquantum statistics, at least in the ubiquitous two-party non-locality setting. Nevertheless, subsequently, we show below that the situation can be remedied in the steering scenario with the addition of a third party holding a trusted qubit system.

### Extremality of quantum assemblages

Consider a bipartite steering scenario<sup>17,29</sup> in which two distant subsystems  $A$  (Alice) and  $B$  (Bob) share a quantum state  $\rho^{(AB)}$ . We assume that  $A$  is uncharacterized (i.e., dimension of its Hilbert space, reduced quantum state, and local measurements which are performed on it are unknown), while the quantum system of  $B$  is fully characterized. Let  $M_{a|x}^{(A)}$  represent an element of a positive operator valued-measure (POVM) on  $A$ , corresponding to the outcome  $a \in \mathcal{A}$  of the measurement setting  $x \in \mathcal{X}$  with fixed and finite alphabet sizes  $|\mathcal{A}|$  and  $|\mathcal{X}|$ . According to measurements performed on  $A$ , the subsystem  $B$  is then described by the set of subnormalized states

$$\sigma_{a|x}^{(B)} = \text{Tr}_A(M_{a|x}^{(A)} \otimes \mathbb{1} \rho^{(AB)}). \quad (1)$$

The probability of obtaining outcome  $a$  while performing measurement  $x$  on subsystem  $A$  is given by  $\text{Tr}_B(\sigma_{a|x}^{(B)})$ , and subsystem  $B$  after this measurement is described by the state  $\frac{\sigma_{a|x}^{(B)}}{\text{Tr}_B(\sigma_{a|x}^{(B)})}$ . The collection of subnormalized states  $\Sigma^{(B)} = \{\sigma_{a|x}^{(B)}\}_{a,x}$  acting on a Hilbert space (of subsystem  $B$ ) of dimension  $d_B$  is known as a quantum assemblage.

One can also consider a general abstract notion of a no-signaling assemblage (also acting on a  $d_B$  dimensional Hilbert space) defined by the following no-signaling conditions  $\forall_{a,x} \sigma_{a|x}^{(B)} \geq 0$ ,  $\forall_{x,x'} \sum_a \sigma_{a|x}^{(B)} = \sigma^{(B)} = \sum_a \sigma_{a|x'}^{(B)}$  and  $\text{Tr}(\sigma^{(B)}) = 1$ . One can think of such a no-signaling assemblage as the effect of the steering of a quantum state describing subsystem  $B$  (with dimension  $d_B$ ) by local measurements performed on an uncharacterized separated subsystem  $A$ , when the joint state of both subsystems is no longer described by quantum mechanics, but rather as the state in some no-signaling generalized probabilistic theory. However, it has been proven in<sup>30,31</sup>, that any two-party no-signaling assemblage also admits a quantum realization, i.e., there exist a subsystem  $A$ , POVM elements  $M_{a|x}^{(A)}$  and a joint quantum state  $\rho^{(AB)}$ , such that all the elements  $\sigma_{a|x}^{(B)}$  can be reconstructed as in formula (1). Therefore there is no postquantum steering in this bipartite setting.

The situation dramatically changes if we consider assemblages with three separated subsystems  $A, B, C$ , in which a characterized subsystem  $C$  (Charlie) associated with a Hilbert space of dimension  $d_C$  shares with uncharacterized parties  $A, B$  a joint state in some no-signaling generalized probabilistic theory<sup>32</sup>. Analogously to the bipartite case, one may perform uncharacterized (local, independent) measurements on  $A$  and  $B$  (with settings and outcomes labeled by pairs  $x, a$  and  $y, b$ , respectively). Subsystem  $C$  is then described by a set of subnormalized states  $\sigma_{ab|xy}^{(C)}$  satisfying the no-signaling conditions. In this case, the abstract no-signaling assemblage (acting on the  $d_C$  dimensional space)  $\Sigma^{(C)} =$

$$\left\{ \sigma_{ab|xy}^{(C)} \right\}_{a,b,x,y} \text{ is therefore defined by the conditions}$$

$$\forall_{b,x,x',y} \sum_a \sigma_{ab|xy}^{(C)} = \sum_a \sigma_{ab|x'y}^{(C)}, \quad (2)$$

$$\forall_{a,x,y,y'} \sum_b \sigma_{ab|xy}^{(C)} = \sum_b \sigma_{ab|xy'}^{(C)}, \quad (3)$$

$$\forall_{x,y} \text{Tr} \left( \sum_{a,b} \sigma_{ab|xy}^{(C)} \right) = 1, \quad \forall_{a,b,x,y} \sigma_{ab|xy}^{(C)} \geq 0. \quad (4)$$

Crucially, as opposed to the bipartite setting, not all no-signaling assemblages  $\Sigma^{(C)}$  in the tripartite setting, admit a quantum realization<sup>18</sup> as  $\sigma_{ab|xy}^{(C)} = \text{Tr}_{AB} \left( M_{a|x}^{(A)} \otimes N_{b|y}^{(B)} \otimes \mathbb{1} \rho^{(ABC)} \right)$ , with POVM elements  $M_{a|x}^{(A)}, N_{b|y}^{(B)}$  and tripartite state  $\rho^{(ABC)}$  of the quantum system  $ABC$ .

Indeed, one may consider a no-signaling assemblage defined as  $\sigma_{ab|xy}^{(C)} = p^{(AB)}(ab|xy) \rho^{(C)}$  with  $p^{(AB)}(ab|xy)$  denoting the so-called PR box distributions<sup>18</sup>. This assemblage is postquantum and this is a direct consequence of the postquantum non-locality of the PR box (see detailed discussion in Supplementary Note 2). Interestingly, it has been found that there are also no-signaling assemblages  $\Sigma^{(C)} = \left\{ \sigma_{ab|xy}^{(C)} \right\}_{a,b,x,y}$ , for which any POVM elements  $R_{c|z}^{(C)}$  provide no-signaling boxes  $p^{(ABC)}(abc|xyz) = \text{Tr} \left( R_{c|z}^{(C)} \sigma_{ab|xy}^{(C)} \right)$  with quantum realization, and yet the whole assemblage does not admit quantum realization<sup>18</sup>. These show that postquantum non-locality and postquantum steering are genuinely different phenomena in the tripartite setting and beyond. It is noteworthy that the (i) set of no-signaling assemblages and (ii) the subset of assemblages that admit quantum realization are both convex—see discussion in Supplementary Note 2.

Inside the discussed set of quantum assemblages one can single out the convex subset of local hidden state (LHS) assemblages that represent steering with a classically correlated system<sup>33</sup>. A no-signaling assemblage admits LHS model if it can be represented by  $\sigma_{ab|xy}^{(C)} = \sum_i q_i p_i^{(A)}(a|x) p_i^{(B)}(b|y) \sigma_i^{(C)}$  where  $q_i \geq 0, \sum q_i = 1$ , and  $\sigma_i^{(C)}$  are some states of characterized subsystem  $C$  and  $p_i^{(A)}(a|x), p_i^{(B)}(b|y)$  denote conditional probability distributions for uncharacterized subsystems  $A$  and  $B$  respectively. Equivalently, for LHS  $\sigma_{ab|xy}^{(C)} = \sum_i q_i p_i^{(AB)}(ab|xy) \sigma_i^{(C)}$  where  $L_i = \left\{ p_i^{(AB)}(ab|xy) \right\}_{a,b,x,y}$  is a deterministic box of conditional probabilities (compare with Supplementary Note 2).

As in a tripartite case, one can discuss different types of separability (entanglement), we introduce another convex set of biseparable assemblages (BIS) as a collection of all assemblages with quantum realization  $\sigma_{ab|xy}^{(C)} = \text{Tr}_{AB} \left( M_{a|x}^{(A)} \otimes N_{b|y}^{(B)} \otimes \mathbb{1} \rho^{(ABC)} \right)$  where  $\rho^{(ABC)}$  is biseparable<sup>32</sup> (see further discussion in Supplementary Note 2). It is easy to see that biseparable

assemblages form an intermediate set between LHS and quantum assemblages.

One can show that a no-signaling assemblage can be excluded from the set of LHS assemblages by the violation of a steering inequality, i.e., for any no-signaling assemblage  $\Sigma^{(C)}$  that does not admit an LHS model, there exists a linear real-valued functional  $F$  on no-signaling assemblages such that  $F(\Sigma^{(C)}) > C_{\text{LHS}}$  and  $F(\Sigma_{\text{LHS}}^{(C)}) \leq C_{\text{LHS}}$  for all LHS assemblages  $\Sigma_{\text{LHS}}^{(C)}$ . Similarly certain subclass of such inequalities may be used for certification that a given assemblage is not biseparable. In particular, in case of quantum assemblages, steering inequalities may indicate that the initial state is not fully separable or biseparable.

One can easily generalize the notion of no-signaling assemblages to the scenario with  $n > 2$  uncharacterized parties<sup>33</sup>. For simplicity, we will restrict our attention to the case when  $n = 2$  and  $a, b, x, y \in \{0, 1\}$ . Note that a no-signaling assemblage can be then seen as a box of positive operators (i.e., subnormalized states) where  $(a|x)$  label rows and  $(b|y)$  label columns, i.e.,

$$\Sigma^{(C)} = \begin{pmatrix} \sigma_{00|00}^{(C)} & \sigma_{01|00}^{(C)} & \sigma_{00|01}^{(C)} & \sigma_{01|01}^{(C)} \\ \sigma_{10|00}^{(C)} & \sigma_{11|00}^{(C)} & \sigma_{10|01}^{(C)} & \sigma_{11|01}^{(C)} \\ \sigma_{00|10}^{(C)} & \sigma_{01|10}^{(C)} & \sigma_{00|11}^{(C)} & \sigma_{01|11}^{(C)} \\ \sigma_{10|10}^{(C)} & \sigma_{11|10}^{(C)} & \sigma_{10|11}^{(C)} & \sigma_{11|11}^{(C)} \end{pmatrix}. \quad (5)$$

In particular, LHS assemblages are convex combinations of extremal boxes (of operators) that have only four nonzero positions occupied by the same pure state forming a rectangle with exactly one element for each pair  $(x, y)$  (see an example of such extreme point in Supplementary Note 2).

In analogy to the fundamental question in non-locality, it is interesting to ask whether a quantum assemblage can realize an extremal non-classical point in the set of no-signaling assemblages. In the case of bipartite steering, all no-signaling assemblages admit quantum realization, therefore such a question is uninteresting. The first relevant scenario is a tripartite setup with at least two measurement settings on uncharacterized parties (see discussion in Supplementary Note 10). We show below that in contrast to non-locality the question admits the affirmative answer in this setting.

Any extremal quantum assemblage can be obtained by measurements performed on a pure state, therefore we may restrict only to such states (see discussion in Supplementary Note 5). Recall that a pure state  $|\psi^{(ABC)}\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_C}$  is genuine three-party entangled if it is entangled with respect to any bipartite splitting of the tripartite system.

**Proposition 2** For any pure genuine three-party entangled state  $|\psi^{(ABC)}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^d$  there exists a pair of PVMs with two outcomes on subsystems  $A$  and  $B$  respectively such that a no-signaling assemblage  $\Sigma^{(C)}$  obtained by these measurements is extremal. In particular,  $\Sigma^{(C)}$  is not LHS and not biseparable. Moreover,  $\Sigma^{(C)}$  is the unique no-signaling assemblage that maximally violates some steering inequality  $F_{\Sigma^{(C)}}$ .

The reasoning behind the above proposition is based on a notion of inflexibility that we shall introduce in Definition 6 of Methods. This notion enables us to provide an explicit construction of  $F_{\Sigma^{(C)}}$  given by (7) and in particular shows that the maximal value of  $F_{\Sigma^{(C)}}$  over no-signaling assemblages is equal to 4. The following provides an example of an assemblage from Proposition 2.

**Example 3** Consider a GHZ three qubit state  $|\psi^{(ABC)}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ . Let  $\Sigma_{\text{GHZ}}^{(C)}$  be given by  $\sigma_{ab|xy}^{(C)} = \text{Tr}_{AB} \left( P_{a|x}^{(A)} \otimes Q_{b|y}^{(B)} \otimes \mathbb{1} |\psi^{(ABC)}\rangle \langle \psi^{(ABC)}| \right)$  with  $P_{0|0}^{(A)} = Q_{0|0}^{(B)} = |+\rangle \langle +|$

and  $P_{01}^{(A)} = Q_{01}^{(B)} = |0\rangle\langle 0|$ , i.e.,

$$\Sigma_{\text{GHZ}}^{(C)} = \frac{1}{4} \begin{pmatrix} |+\rangle\langle +| & |-\rangle\langle -| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ |-\rangle\langle -| & |+\rangle\langle +| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ |0\rangle\langle 0| & |0\rangle\langle 0| & 2|0\rangle\langle 0| & 0 \\ |1\rangle\langle 1| & |1\rangle\langle 1| & 0 & 2|1\rangle\langle 1| \end{pmatrix}.$$

Assemblage  $\Sigma_{\text{GHZ}}^{(C)}$  is extremal and maximal values obtained by related functional  $F_{\Sigma_{\text{GHZ}}^{(C)}}$  on LHS assemblages and biseparable assemblages are given respectively by  $C_{\text{LHS}} = \sup_{|\phi\rangle} \text{Tr}[(3|0\rangle\langle 0| + |+\rangle\langle +|)|\phi\rangle\langle\phi|] = \frac{4+\sqrt{10}}{2}$  and  $C_{\text{BIS}} = \frac{5+\sqrt{5}}{2}$  (see detailed calculation in Supplementary Note 7).

To investigate the result further, let us fix  $|\psi^{(ABC)}\rangle$  together with its related  $\Sigma^{(C)}$  obtained using PVMs  $P_{a|x}^{(A)}, Q_{b|y}^{(B)}$  as in Proposition 2. Consider an arbitrary pure state  $|\tilde{\psi}^{(ABC)}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^d$  and corresponding assemblage  $\tilde{\Sigma}^{(C)}$  given by two pairs of PVMs  $\tilde{P}^{(A)}, \tilde{Q}^{(B)}$  with two outcomes as  $\tilde{\sigma}_{ab|xy}^{(C)} = \text{Tr}_{AB}(\tilde{P}_{a|x}^{(A)} \otimes \tilde{Q}_{b|y}^{(B)} \otimes \mathbb{1})|\tilde{\psi}^{(ABC)}\rangle\langle\tilde{\psi}^{(ABC)}|$ . One can see that  $F_{\tilde{\Sigma}^{(C)}} = 4$  iff  $|\tilde{\psi}^{(ABC)}\rangle = U_A \otimes U_B \otimes \mathbb{1} |\psi^{(ABC)}\rangle$ ,  $\tilde{P}_{a|x}^{(A)} = U_A P_{a|x}^{(A)} U_A^\dagger$  and  $\tilde{Q}_{b|y}^{(B)} = U_B Q_{b|y}^{(B)} U_B^\dagger$  for some local unitaries  $U_A, U_B$ . Indeed, it is the case, as we will show in the discussion in Methods that the first two rows and one column of  $\Sigma^{(C)}$  from Proposition 2 consist of different rank one operators. This observation together with a well-known Jordan's lemma leads to the following self-testing result (see Supplementary Note 8 for an explicit statement of Jordan's lemma and complete reasoning behind self-testing).

**Proposition 4** For any pure state  $|\tilde{\psi}^{(A'B'C)}\rangle \in \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_{B'}} \otimes \mathbb{C}^{d_C}$  and assemblage  $\tilde{\Sigma}^{(C)}$  with elements  $\tilde{\sigma}_{ab|xy}^{(C)} = \text{Tr}_{A'B'}(\tilde{P}_{a|x}^{(A')} \otimes \tilde{Q}_{b|y}^{(B')} \otimes \mathbb{1})|\tilde{\psi}^{(A'B'C)}\rangle\langle\tilde{\psi}^{(A'B'C)}|$ ,  $F_{\tilde{\Sigma}^{(C)}} = 4$  iff  $V_{A'} \otimes V_{B'} \otimes \mathbb{1} |\tilde{\psi}^{(A'B'C)}\rangle = |\phi_{A'B'}^{\text{junk}}\rangle |\psi^{(ABC)}\rangle$ , and  $(V_{A'} \otimes V_{B'} \otimes \mathbb{1})(\tilde{P}_{a|x}^{(A')} \otimes \tilde{Q}_{b|y}^{(B')} \otimes \mathbb{1})|\tilde{\psi}^{(A'B'C)}\rangle = |\phi_{A'B'}^{\text{junk}}\rangle (P_{a|x}^{(A)} \otimes Q_{b|y}^{(B)} \otimes \mathbb{1})|\psi^{(ABC)}\rangle$  where  $V_{A'}, V_{B'}$  are some local isometries and  $|\psi^{(ABC)}\rangle$  together with  $P_{a|x}^{(A)}, Q_{b|y}^{(B)}$  are as in Proposition 2, while  $|\phi_{A'B'}^{\text{junk}}\rangle$  is some irrelevant junk state.

Note that besides the general results stated above, one can also construct particular examples of (non-local) extreme assemblages with quantum realization also in a tripartite setting with two measurements and  $d$  outcomes per uncharacterized party (see construction provided in Supplementary Note 9).

## DISCUSSION

We have proved that in the most general scenario of sequential measurements it is impossible to quantumly realize non-local extremal points of the TONS polytope. This answers the open question posed in<sup>22</sup>. On the contrary, if one of the parties has access to at least one fully trusted qubit system, we have shown that one can obtain quantum assemblages which are extremal within the set of no-signaling assemblages. While this opens the path toward security proofs for semi-DI cryptographic protocols against general adversaries, numerous interesting open questions arise for future research. In particular, in the setting of sequential Bell non-locality, the immediate question is to extend the result to the multi-partite setting, as well as to the scenario of single-party contextuality. Quantitative bounds on the distance of quantum boxes from extremal TONS ones should be obtained utilizing the methods involved in the proof of Theorem 1, i.e., by lower bounding the minimum eigenvalue of the matrix  $\tilde{A}_p^\top \tilde{A}_p$  associated with the extremal box  $P$  (see Supplementary Note 1

for explicit definition of the aforementioned matrix). Is it possible to generalize the main result of Proposition 2 by showing that for any genuinely entangled third-party  $d_A \otimes d_B \otimes d_C$  state, there are some  $k_A$  PVMs (or POVMs) with  $s_A$  outcomes on system  $A$  and  $k_B$  PVMs (or POVMs) with  $s_B$  outcomes on system  $B$  such that the corresponding assemblage is again extremal in the set of all no-signaling assemblages? If yes, what are the minimal number of settings and outcomes? Clear extensions to many-party scenarios should naturally be explored. Finally, as obviously not all extremal no-signaling assemblages admit quantum realization (e.g.,  $\sigma_{ab|xy}^{(C)} := p^{(AB)}(ab|xy)|\phi^{(C)}\rangle\langle\phi^{(C)}|$  with  $p^{(AB)}(ab|xy)$  coming from a PR box), it would be natural to ask for a characterization of such extremal points and information-theoretic consequences thereof.

## METHODS

### Similarity and inflexibility

Below we shall introduce the concepts of similarity and inflexibility of no-signaling assemblages with at most rank one elements  $\sigma_{ab|xy}^{(C)}$  which are crucial for reasoning staying behind already described results.

**Definition 5** Consider a general no-signaling assemblage  $\Sigma^{(C)}$  as in Eq. (5) with all positions occupied by at most rank one operators and denote it by  $\Sigma^{(C)} = \{p_i |\psi_i^{(C)}\rangle\langle\psi_i^{(C)}|\}_i$ , where  $i = (ab|xy)$  and  $p_i = \text{Tr}(\sigma_i^{(C)})$ . In this case, we say that  $\Sigma^{(C)}$  is an assemblage of pure states. Consider any other assemblage of pure states  $\tilde{\Sigma}^{(C)} = \{q_i |\psi_i^{(C)}\rangle\langle\psi_i^{(C)}|\}_i$  with the same states  $|\psi_i^{(C)}\rangle\langle\psi_i^{(C)}|$  at the same positions as in  $\Sigma^{(C)}$ . If additionally  $p_i = 0$  implies  $q_i = 0$  for any  $i$ , we say that  $\tilde{\Sigma}^{(C)}$  is similar to  $\Sigma^{(C)}$ .

Note that the above relation is not symmetric, i.e., it may happen that  $\tilde{\Sigma}^{(C)}$  is similar to  $\Sigma^{(C)}$ , but  $\Sigma^{(C)}$  is not similar to  $\tilde{\Sigma}^{(C)}$ .

**Definition 6** An assemblage of pure states  $\Sigma^{(C)}$  is called inflexible if for any  $\tilde{\Sigma}^{(C)}$  similar to  $\Sigma^{(C)}$  we get  $\Sigma^{(C)} = \tilde{\Sigma}^{(C)}$ .

Note that as we considered assemblages of pure states, in particular, inflexibility implies extremality in the set of all no-signaling assemblages (see complete derivation of this fact in Supplementary Note 3). If so, then checking for inflexibility becomes a method of certifying extremality.

Indeed, to prove the statement of Proposition 2 observe that as  $|\psi^{(ABC)}\rangle$  is genuine three-party entangled there exists a PVM with elements  $P_{a|0}^{(A)} = |\phi_{a|0}\rangle\langle\phi_{a|0}|$  on the subsystem  $A$  such that  $\langle\phi_{a|0}|\psi^{(ABC)}\rangle$  are entangled and linearly independent (see discussion in Supplementary Note 6 for justification of this claim). Therefore, one can choose a pair of PVMs with respective elements  $Q_{b|0}^{(B)}, Q_{b|1}^{(B)}$  on the subsystem  $B$ , such that each of the first two rows of  $\Sigma^{(C)}$  consists of elements proportional to normalized pure states which are all different. Moreover, there is an index  $(b|y)$  for which  $\sigma_{0b|0y}^{(C)}$  and  $\sigma_{1b|0y}^{(C)}$  are not proportional to the same pure state (see discussion in Supplementary Note 6 for justification of this claim). Choosing the second PVM on subsystem  $A$  such that its elements  $P_{a|1}^{(A)}$  do not commute with the first, we obtain a column  $(b|y)$  with the same property as the first and the second row, i.e., having all the normalized elements pure and different. A detailed analysis of assemblages with such properties proves that  $\Sigma^{(C)}$  is inflexible and hence extremal (compare description of sufficient conditions for inflexibility given in Supplementary Note 4).

Define now

$$\rho_{ab|xy} = \begin{cases} 0 & \text{for } \sigma_{ab|xy}^{(C)} = 0, \\ \frac{\sigma_{ab|xy}^{(C)}}{\text{Tr}(\sigma_{ab|xy}^{(C)})} & \text{for } \sigma_{ab|xy}^{(C)} \neq 0. \end{cases} \quad (6)$$

For any no-signaling assemblage  $\tilde{\Sigma}^{(C)}$  consider

$$F_{\tilde{\Sigma}^{(C)}}(\tilde{\Sigma}^{(C)}) = \sum_{a,b,x,y=0,1} \text{Tr}(\rho_{ab|xy} \tilde{\sigma}_{ab|xy}^{(C)}). \quad (7)$$

Observe that  $F_{\tilde{\Sigma}^{(C)}}(\tilde{\Sigma}^{(C)}) \leq 4$  and equality holds if and only if the no-signaling assemblage  $\tilde{\Sigma}^{(C)}$  is similar to  $\Sigma^{(C)}$ , so by inflexibility the maximal value of  $F_{\tilde{\Sigma}^{(C)}}$  is uniquely obtained for  $\tilde{\Sigma}^{(C)}$ . Since any LHS assemblage is a convex combination of assemblages consisting of the same pure state occupying four positions forming a rectangle, and the first and second row of  $\Sigma^{(C)}$  consist of different rank one operators,  $\Sigma^{(C)}$  is not an LHS assemblage and  $C_{\text{LHS}} = \sup_{\text{LHS}} F_{\Sigma^{(C)}}(\Sigma_{\text{LHS}}^{(C)}) < 4$ . Analyzing the structure of the set of biseparable assemblages presented in Supplementary Note 2 one can additionally show that  $C_{\text{BIS}} = \sup_{\text{BIS}} F_{\Sigma^{(C)}}(\Sigma_{\text{BIS}}^{(C)}) < 4$  as form of  $\Sigma^{(C)}$  does not agree with the possible form of extremal no-signaling assemblage that is biseparable.

Note that to find  $C_{\text{LHS}}$ , the value  $\sum_{a,b,x,y \in I(L)} \text{Tr}(\rho_{ab|xy} |\phi\rangle\langle\phi|)$  is maximized over pure states  $|\phi\rangle$  and deterministic boxes  $L$ , where  $I(L)$  denotes the set of  $(ab|xy)$  (forming a rectangle) for which  $p(ab|xy) = 1$  in  $L$ —by convexity, optimization need be performed only over the extremal points. Optimization over biseparable assemblages boils down to optimization over three classes of assemblages covering all possible extreme points in the set of biseparable assemblages. To see this compare a detailed discussion on biseparable assemblages in Supplementary Note 2. These observations were crucial for explicit calculation for Example 3 covered in Supplementary Note 7.

## DATA AVAILABILITY

Data are available within the article and supplementary information. Any additional calculations can be obtained upon reasonable request.

Received: 7 April 2022; Accepted: 20 September 2022;

Published online: 04 October 2022

## REFERENCES

- Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777–780 (1935).
- Schrödinger, E. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften* **23**, 807–812 (1935).
- Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81**, 865–942 (2009).
- Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195–200 (1964).
- Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
- Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
- Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
- Kessler, M. & Arnon-Friedman, R. Device-independent randomness amplification and privatization. *IEEE J. Sel. Areas Inf. Theory* **1**, 568–584 (2020).
- Chung, K.-M., Shi, Y. & Wu, X. Physical randomness extractors: generating random numbers with minimal assumptions. Preprint at <https://arxiv.org/abs/1402.4797> (2014).
- Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2005).
- Pawlowski, M. & Brukner, C. Monogamy of Bell's inequality violations in non-signaling theories. *Phys. Rev. Lett.* **102**, 030403 (2009).

- Ramanathan, R. & Horodecki, P. Strong monogamies of no-signaling violations for bipartite correlation bell inequalities. *Phys. Rev. Lett.* **113**, 210403 (2014).
- Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Info. Comput.* **4**, 273–286 (2004).
- Barrett, J. & Pironio, S. Popescu-Rohrlich correlations as a unit of nonlocality. *Phys. Rev. Lett.* **95**, 140401 (2005).
- Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **24**, 379–385 (1994).
- Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
- Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.* **98**, 140402 (2007).
- Sainz, A. B., Brunner, N., Cavalcanti, D., Skrzypczyk, P. & Vértesi, T. Postquantum steering. *Phys. Rev. Lett.* **115**, 190403 (2015).
- Colbeck, R. & Renner, R. Free randomness can be amplified. *Nat. Phys.* **8**, 450–453 (2012).
- Gallego, R. et al. Full randomness from arbitrarily deterministic events. *Nat. Commun.* **4**, 2654 (2013).
- Brandão, F. G. S. L. et al. Realistic noise-tolerant randomness amplification using finite number of devices. *Nat. Commun.* **7**, 11345 (2016).
- Ramanathan, R., Tuziemiński, J., Horodecki, M. & Horodecki, P. No quantum realization of extremal no-signaling boxes. *Phys. Rev. Lett.* **117**, 050401 (2016).
- Gallego, R., Würflinger, L. E., Chaves, R., Acín, A. & Navascués, M. Nonlocality in sequential correlation scenarios. *New J. Phys.* **16**, 033037 (2014).
- Buhrman, H., Cleve, R., Massar, S. & De Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys.* **82**, 665–698 (2010).
- Popescu, S. Bell's inequalities and density matrices: revealing “hidden” nonlocality. *Phys. Rev. Lett.* **74**, 2619–2622 (1995).
- Pironio, S., Navascués, M. & Acín, A. Convergent relaxations of polynomial optimization problems with non-commuting variables. *SIAM J. Optim.* **20**, 2157–2180 (2010).
- Bowles, J., Baccari, F. & Salavrakos, A. Bounding sets of sequential quantum correlations and device-independent randomness certification. *Quantum* **4**, 344 (2020).
- Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **10**, 073013 (2008).
- Schrödinger, E. Probability relations between separated system. *Math. Proc. Cambridge Philos. Soc.* **32**, 446–452 (1936).
- Gisin, N. Stochastic quantum dynamics and relativity. *Helv. Phys. Acta* **62**, 363–371 (1989).
- Hughston, L. P., Jozsa, R. & Wootters, K. A. complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A* **183**, 14–18 (1993).
- Cavalcanti, D. et al. Detection of entanglement in asymmetric quantum networks and multipartite quantum steering. *Nat. Commun.* **6**, 7941 (2015).
- Sainz, A. B., Aolita, L., Piani, M., Hoban, M. J. & Skrzypczyk, P. A formalism for steering with local quantum measurements. *New J. Phys.* **20**, 083040 (2018).

## ACKNOWLEDGEMENTS

R.R. acknowledges support from the Start-up Fund “Device-Independent Quantum Communication Networks” from The University of Hong Kong, the Seed Fund “Security of Relativistic Quantum Cryptography” (Grant No. 201909185030), and the Early Career Scheme (ECS) grant “Device-Independent Random Number Generation and Quantum Key Distribution with Weak Random Seeds” (Grant No. 27210620). This work was supported by the National Natural Science Foundation of China through grant 11675136, the Hong Kong Research Grant Council through grant 17300918, and the John Templeton Foundation through grants 60609, Quantum Causal Structures, and 61466, The Quantum Information Structure of Spacetime (qiss.fr). The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation. M.B., R.R.R., and P.H. acknowledge support by the Foundation for Polish Science (IRAP project, ICTQT, contract no. MAB/2018/5, co-financed by EU within the Smart Growth Operational Programme).

## AUTHOR CONTRIBUTIONS

The authors contributed equally to this work. R.R. was leading the investigation concerning sequential non-locality while M.B., R.R.R. and P.H. were leading research on no-signaling assemblages and notion of inflexibility. All authors were involved in the formulation of the problems as well as the discussion and interpretation of the presented results.

## 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/s41534-022-00633-0>.

**Correspondence** and requests for materials should be addressed to Ravishankar Ramanathan.

**Reprints and permission information** is available at <http://www.nature.com/reprints>

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2022