No-go theorem for device-independent security in relativistic causal theories

R. Salazar,[1,2,3,4,*] M. Kamoń,[2] K. Horodecki,[3,5] D. Goyeneche,[6] D. Saha,[1,7] R. Ramanathan,[8] and P. Horodecki[2,5]

[1]*Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, University of Gdansk, 80-308 Gdansk, Poland*

[2]*Faculty of Applied Physics and Mathematics, National Quantum Information Centre, Gdansk University of Technology, 80-233 Gdansk, Poland*

[3]*Institute of Informatics Faculty of Mathematics, Physics, and Informatics, University of Gdansk, 80-308 Gdansk, Poland*

[4]*Institute of Physics, Jagiellonian University, 30-059 Krakow, Poland*

[5]*International Centre for Theory of Quantum Technologies, University of Gdansk, Wita Stwosza 63, 80-308 Gdansk, Poland*

[6]*Departamento de Física, Facultad de Ciencias Básicas, Universidad de Antofagasta, Casilla 170, Antofagasta, Chile*

[7]*Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland*

[8]*Department of Computer Science, University of Hong Kong, Pokfulam Road, Hong Kong*

(Received 25 May 2021; accepted 28 June 2021; published 13 August 2021)

A fundamental question in device-independent quantum cryptography is to determine the minimal physical principle upon which the security of such a cryptographic protocol (such as for key distribution or for randomness generation) may be based. Since the seminal work on device-independent quantum key distribution by J. Barrett, L. Hardy, and A. Kent [Phys. Rev. Lett. **95**, 010503 (2005)], a conjectured candidate for certification of device-independent security has been the principle of relativistic causality, namely the disallowance of causal loops. While this principle has thus far been equated with the no-signaling constraints, it has been shown recently that in multiparty Bell scenarios, the no-signaling constraints are sufficient but not necessary for relativistic causality, and a refined set of constraints has been proposed that more precisely capture the notion of relativistic causality. In this paper, we build upon this finding to show that, in contrast to the no-signaling constraints, the constraints of relativistic causality are not sufficient for certification of device-independent security. More specifically, we show that there exist correlations allowed by the causality principle that allow an adversary to gain complete information about the measurement outcomes of honest parties in any device-independent cryptographic protocol, thereby rendering the protocol completely insecure. As a tool to develop this adversarial attack strategy, we fully characterize the set of correlations allowed by relativistic causality in the tripartite Bell scenario of three parties, each performing two binary measurements, that may be of independent interest. We also demonstrate the difference between the relativistic causal correlations and those allowed by the usual no-signaling constraints by presenting explicit communication tasks wherein the two sets exhibit striking difference in their respective winning probabilities.

DOI: 10.1103/PhysRevResearch.3.033146

I. INTRODUCTION

Quantum cryptography has played a foundational role in the development of the field of quantum information (QI), covering a plethora of security scenarios ranging from secure key distribution to randomness generation and bit commitment [1,2]. The security of quantum cryptographic protocols is based on the very laws of nature, and does not rely on any restrictions on the computational power of an adversary. Furthermore, quantum mechanics also allows for the highest form of security called device-independent (DI) security [3–10]. In the DI paradigm, the honest users do not even need to trust the devices used to execute the protocol, and can verify the security of the protocol directly by checking for a Bell inequality violation by the input-output statistics of their devices.

Security of DI cryptographic protocols (such as for key distribution or randomness generation) has been shown in two different scenarios. In one scenario, the adversary is assumed to be constrained by the entire machinery of quantum mechanics [11]. In the second scenario, the adversary is only assumed to be constrained by the no-signaling constraints [3,4,7–9]. The no-signaling constraints have been justified on the grounds of special relativity; namely they were designed to capture the notion of no-faster-than-light transfer of information, or equivalently of relativistic causality, namely the disallowance of causal loops in a physical theory. Recently it has been shown [12] that in Bell scenarios with more than two spatially separated parties, the no-signaling constraints are, in general, sufficient but not necessary for a theory to obey the principle of relativistic causality. In their stead, a (in general, smaller) subset of relativistic causality constraints

*rb.salazar.vargas@gmail.com

has been proposed, depending on the exact spacetime configuration of the measurement events, that are both necessary and sufficient for causality. Since in DI cryptographic scenarios, one naturally has to deal with at least two spatially separated honest parties (that perform a Bell test on their devices) plus an adversary, the tripartite Bell scenario is in general minimal for DI protocols. It is also noteworthy that the spacetime configuration of the measurement events of the adversary are in general unknown to the honest parties so that the subset of relativistic causality constraints is the more accurate one to choose in this paradigm. It is then natural to ask if the security of DI protocols that has thus far been established based on the no-signaling constraints can equally be established on the basis of the relativistic causality constraints alone. In other words, can device-independent security be predicated upon the principle of relativistic causality alone?

In this paper, we prove a negative answer to this fundamental question. We show an explicit attack strategy obeying relativistic causality that can be executed by two cooperating adversaries, and that can break the security of any DI protocol. In particular, we show that independently of the number of honest parties in the DI protocol, and irrespective of the specific Bell inequality tested, the two adversaries are able to perfectly determine (through measurements on their own systems) the measurement outcomes obtained by the honest parties. Therefore, any DI protocol that uses these outcomes either for randomness extraction or for key distribution cannot be proven secure on the basis of relativistic causality alone. Additional assumptions such as that the adversaries are constrained by the laws of quantum mechanics, or by some other fundamental physical principle, are therefore required to restore device-independent security.

The paper is organized as follows. We first introduce the notion of relativistic causality and explain how the causality constraints differ in general from the no-signaling constraints [12,13]. We then show that the phenomenon of monogamy of Bell inequalities that underpins security of DI protocols and that has been proven to hold under the usual no-signaling constraints does not hold when considering the causality constraints alone. Specifically, we present spatiotemporal configurations of measurement events for which monogamy is broken for any bipartite Bell inequality. We then present the main result, namely that DI security cannot solely be based upon the relativistic causality principle. We establish an attack strategy for two adversaries who exploit specific correlations allowed by relativistic causality to completely learn a copy of the correlations shared by honest parties, as a shared secret between the adversaries which they can subsequently recover. We present a detailed proof for the explicit case of two honest parties executing a DI key distribution protocol. Finally, as a technical tool that may be of independent interest, we provide a complete characterization of the set of correlations allowed by the relativistic causality constraints in the simplest tripartite Bell scenario where three parties each perform two binary measurements. We demonstrate the difference between these correlations and the usual no-signaling correlations by presenting explicit communication tasks wherein the two sets exhibit striking difference in their respective winning probabilities.

II. RELATIVISTIC CAUSALITY VERSUS NO-SIGNALING

Relativistic causality is the physical principle which states that an effect cannot occur from a cause that is not in its past light cone, and similarly a cause cannot have an effect outside its future light cone, i.e., that there must be no causal loops in a physical theory [14,15]. This principle captures the idea of no-faster-than-light propagation of information. The no-signaling constraints are a set of mathematical constraints on the observed probability distributions in a Bell experiment conducted by two or more spatially separated parties that was designed to capture the idea of relativistic causality. Specifically, the no-signaling constraints state that the conditional probability distribution of the measurement outcomes of any subset of parties is independent of the input choice of the remaining parties, and are in general sufficient to ensure that there are no causal loops in the theory. On the other hand, it was pointed out in [12,13] that in general, not all the no-signaling constraints are necessary to ensure that relativistic causality holds. In particular, in Bell experiments with three or more spatially separated parties, there exist spacetime configurations of the three parties' measurement events such that a subset of the no-signaling constraints are already sufficient to ensure relativistic causality. As such, in multiparty Bell scenarios, the set of constraints necessary to guarantee relativistic causality are in general a subset of the no-signaling conditions. As pointed out earlier, this is especially relevant in Bell experiments conducted as part of DI cryptographic protocols, where the spacetime configuration of the measurement events of one of the parties, namely the adversary, is not under the honest parties' control. We explain the difference between the two sets of constraints with a particularly relevant example here. Consider a Bell experiment with three parties—Alice (A), Bob (B), and Charlie (C). The input choices for the three parties are labeled x, y, z, respectively, with the corresponding measurement outcomes being labeled a, b, c. Now, consider the spacetime measurement configuration of the three parties' measurement events shown in Fig. 1. The noteworthy property of this configuration is that the intersection of the future light cones of measurement events detected by Alice and Charlie is contained within the future light cone of the measurement event detected by Bob. This property ensures that no breakdown of causality occurs if the joint distribution of the outcomes a, c were to depend on Bob's input y. This may be intuitively understood from the fact that the information concerning the correlations between a and c is only accessible at a point in the intersection of the future light cones of Alice and Charlie's measurement events, which is itself contained within the future light cone of Bob's measurement event. This observation, shown with a more detailed argument in [12,13], implies that only a strict subset of the no-signaling constraints, given in (1) and called the relativistic causality constraints, is necessary and sufficient to ensure causality when the measurement events follow this spacetime configuration:

$$\sum_a P(a,b,c \mid x,y,z) = \sum_a P(a,b,c \mid x',y,z),$$
$$\sum_c P(a,b,c \mid x,y,z) = \sum_c P(a,b,c \mid x,y,z'),$$

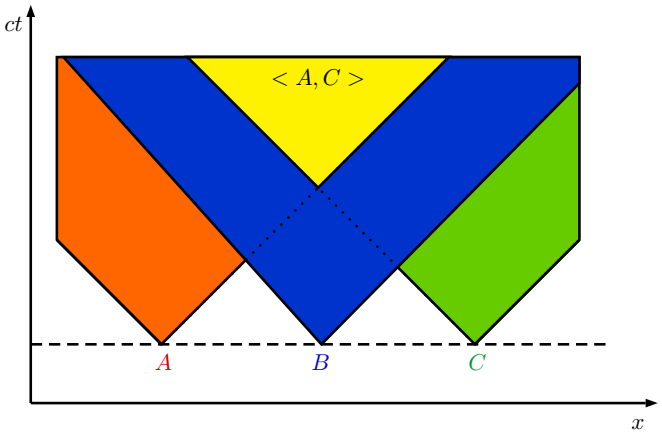

FIG. 1. Spacetime configuration of measurement events in the three-party Bell experiment, when measurements are simultaneous in a common reference frame. The information about two-point correlations $\langle A, C\rangle$ between Alice and Charlie's outputs is only accessible in the yellow region that lies within the causal future of Bob's measurement event.

$$\sum_{b,c} P(a,b,c \mid x,y,z) = \sum_{b,c} P(a,b,c \mid x,y',z'),$$
$$\sum_{a,b} P(a,b,c \mid x,y,z) = \sum_{a,b} P(a,b,c \mid x',y',z),$$

for all $x, x', y, y', z, z', a, b, c$. We refer to the above set of constraints as the relativistic causality constraints in this measurement configuration. A couple of points are worth mentioning here. First, the absence of the no-signaling condition for AC does not imply the presence of signaling, i.e., a faster-than-light transmission of information in a standard, point-to-point sense. Second, the above observation shows that in general multiparty Bell scenarios, the set of necessary and sufficient constraints to guarantee relativistic causality depends explicitly on the spacetime configuration of the measurement events of all participating parties. This also means that the polytope of behaviors (correlations) obeying relativistic causality is richer in structure and in general has a higher dimensionality than the usual no-signaling polytope for the multiparty Bell scenario. Finally, we also note that the above constraints are manifestly Lorentz covariant. If the intersection of the future light cones of A and C is contained within the future light cone of B in one inertial reference frame, then the same holds for all inertial reference frames. In Appendix B, we provide the necessary and sufficient constraints imposed by relativistic causality for an arbitrary number of parties in arbitrary globally hyperbolic spacetime.

III. MONOGAMY OF NONLOCALITY

One of the most intriguing properties of quantum nonlocal correlations is the phenomenon of monogamy of nonlocality. The monogamy relations were first derived, based on the no-signaling constraints for the well-known CHSH inequality, by Toner [16], after which more stringent relations based on the laws of quantum theory were also derived. The monogamy relations are direct trade-off relations between the amount of violation of an inequality observed by a pair of agents Alice and Bob and the correlations between Alice (or Bob) and a third party Charlie's system. The monogamy of nonlocality underpins the security of device-independent key distribution and randomness generation protocols [3,4], besides having other applications such as in deriving nontrivial bounds on cloning [17], and even helping in the detection of gravitational decoherence [18]. Since, as we have seen, the relativistic causality constraints are in general only a strict subset of the no-signaling constraints, a fundamental question arises: Can the monogamy of nonlocality be derived on the basis of relativistic causality alone? In this section, we answer this question in the negative in a very general setting. Namely, we show a general theorem stating that there exist spacetime measurement configurations such as in Fig. 1 for which no two-party Bell inequality admits a monogamy relation on the basis of the relativistic causality constraints alone. Note that detailed proofs are deferred to the appendices.

Consider a general bipartite Bell scenario with two parties Alice and Bob performing measurements labeled x, y and obtaining outcomes a, b, respectively. Let us write a general Bell inequality G in this scenario as

$$G := \sum_{a,b,x,y} V(a,b,x,y) P(a,b|x,y) \leqslant \omega_c(G), \tag{1}$$

where $V(a,b,x,y)$ is a predicate indicating which probabilities enter the Bell expression and $\omega_c(G)$ denotes the maximal value achievable for the Bell expression within a classical (local hidden variable) theory. Let $\omega_{rc}(G) \geqslant \omega_c(G)$ denote the maximal value achievable within a general physical theory obeying causality.

The following proposition shows that in a three-party Bell scenario with a third player Charlie performing measurements z and obtaining outcomes c, when the measurement events occur in the spacetime configuration given by Fig. 1, relativistic causal correlations allow both pairs of parties, i.e., A-B and B-C, to simultaneously observe the maximum relativistic causal value $\omega_{rc}(G)$ of the inequality.

Proposition 1. Consider any bipartite Bell inequality G of the form in Eq. (1). Suppose three players A, B, C perform their measurements in the spacetime configuration of Fig. 1, and that both A-B and B-C test for the violation of G. Then, there exist correlations $\{P(a,b,c|x,y,z)\}$ obeying relativistic causality that allow both pairs A-B and B-C to achieve the maximal relativistic causal value $\omega_{rc}(G)$ of the inequality.

An important insight gained from Proposition 1 goes into the very roots of the structure of correlations in theories constrained by causality alone. In all generalized probabilistic theories studied thus far, given a composite physical system, the *extremal points* of the polytope of allowed correlations in the system were always of the form that guaranteed a lack of correlations of the system with any external observer. According to Proposition 1, there is a dramatic change in theories constrained by relativistic causality alone (RC theories). In such theories, even extremal points could potentially be correlated with an environmental system giving rise to a very interesting structure of allowed behaviors and physical phenomena.

IV. A NO-GO THEOREM FOR DEVICE-INDEPENDENT SECURITY

We build on the shareability of correlations derived in the previous section to show that for any device-independent cryptographic protocol (say for randomness or key distribution), there exists an attack strategy by two eavesdroppers with suitably chosen spacetime measurement configurations that completely breaks the security of the protocol. Moreover, the hacking strategy is valid irrespective of the number of honest parties executing the protocol and regardless of the Bell inequality that they test for in the protocol. First consider any DI protocol which begins with parallel measurements on the device by the two honest parties. These protocols consist of the operations called "measurement on device followed by local operations and public communication" (MDLOPC) [19]. Note that all known protocols secure against the nonsignaling adversary perform this MDLOPC paradigm; see, e.g., [8,9,20]. To establish the result, let us consider N spacelike separated parties performing a multiparty Bell test as part of a DI protocol with the general Bell inequality given by

$$G := \sum_{\mathbf{r},\mathbf{q}} V(\mathbf{r},\mathbf{q}) P(\mathbf{r} \mid \mathbf{q}) \leqslant \omega_c(G). \tag{2}$$

Here, the inputs $\mathbf{q} = x, y_1, \ldots, y_{N-1}$ and outputs $\mathbf{r} = a, b_1, \ldots, b_{N-1}$ correspond to the N reliable agents labeled as $A, B_1, \ldots, B_{N-1}$. We show that even in the extreme noiseless scenario where the honest parties observe the maximal (relativistic causal) value for the Bell expression (2), the protocol is rendered completely insecure against adversaries who are restricted only by the relativistic causality principle. In other words, DI security cannot be predicated upon the causality principle alone.

Theorem 1. Consider a multipartite Bell inequality (2) and assume that N reliable agents perform measurements in some fixed but arbitrary spacetime configuration, obtaining a violation $\omega^* > \omega_c$. Then, there is a spacetime configuration of two eavesdroppers, implementing N measurements each, such that the correlations of those measurements fully reproduce the statistics of the N reliable agents, which the eavesdroppers can recover by communicating their results.

A configuration in which two eavesdroppers E_1, E_2 can use their outputs c_1, c_2 to infer the output a of an honest party A for any of its inputs x is shown in Fig. 2. Now to be more concrete, let us explicitly consider the case of a DI quantum key distribution protocol between two parties Alice (A) and Bob (B), and define the notion of *distillable key* K_D^{RC}. This quantity is the maximum ratio of the number of key bits divided by the initial number of devices n, in the asymptotic limit of large n, that can be obtained via protocols based on operations from n copies of identically prepared quantum systems. For further details see Definitions 1 and 2 in Appendix E. We build upon Theorem 1 to show that K_D^{RC} is zero within the framework of relativistic causal theories.

Theorem 2. (no-go for MDLOPC secure key distribution). For any $P_{AB} \equiv P(A, B|X, Y)$ satisfying the no-signaling constraints, there exists a spacetime configuration of two eavesdroppers E_1 and E_2 and a four-partite distribution $P(A, B, E_1, E_2|X, Y)$ satisfying RC constraints, with bipartite

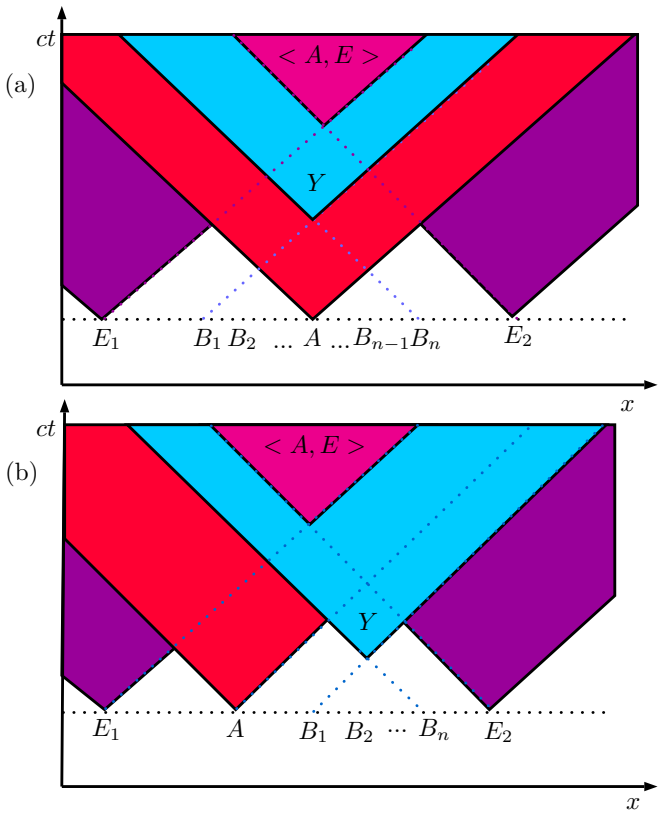

FIG. 2. One-dimensional illustration of the no-go theorem. Here E stands for the correlation between measurement outputs of the two eavesdroppers E_1 and E_2. The measurement events $A, B_1, \ldots, B_{N-1}$ of the reliable parties determine a spatial convex hull from which there are two possible situations: (a) The party A is in the interior of the convex hull of the events, or (b) the party A is at the boundary of the convex hull. In both cases the eavesdroppers can choose positions far enough such that the inputs $Y = y_1, \ldots, y_{N-1}$ can influence the correlation $\langle A, E \rangle$. This is allowed by RC theory when the eavesdroppers calibrate the region where information from $\langle A, E \rangle$ (pink) is accessible only in a region inside the causal future of all inputs Y (light blue).

marginal distribution on A-B equal to P_{AB} such that

$$K_D^{\mathrm{RC}}[P(ABE_1E_2|XY)] = 0. \tag{3}$$

Note that in RC theories, the eavesdropper could, in principle, even decorrelate the honest parties Alice and Bob. However, in such case they would abort the protocol. Hence, the challenge in Theorem 2 was to find an eavesdropping strategy, for two eavesdroppers in this case, that works without changing the correlations between Alice and Bob.

At this point, one might be tempted to believe that security can be restored by an additional assumption that the devices are sufficiently shielded from any influence beyond the no-signaling constraints. However, we remark that the attack by the adversaries is based on the relaxation from no-signaling to relativistic causal constraints. These latter constraints allow for point-to-region physical influences of correlations without having a point-to-point faster-than-light transfer of information [12]. Such effects are locally undetectable and may be controlled by an adversary, in such a way to have the

correlations within his or her light cone, outside of the region occupied by the trusted parties. Moreover, the point-to-region effect may have a physical nature that prevents shielding by the honest parties. In contemporary physics, we know already of a prominent example of a phenomenon of this kind, namely vacuum correlations in quantum electrodynamics which cannot be shielded for fundamental reasons.

V. THE TRIPARTITE RELATIVISTIC CAUSAL POLYTOPE

For bipartite systems, relativistic causal (RC) constraints coincide with the no-signaling constraints. The simplest scenario where the two differ is the (3,2,2) Bell scenario, i.e., three parties Alice, Bob, and Charlie performing two binary measurements each, in the particular measurement configuration of Fig. 1. RC correlations in this case form a finite polytope that strictly contains the no-signaling polytope. An important method to illustrate the difference between the two correlations is to consider the following question: Are there any information processing tasks for which RC correlations work better than the no-signaling ones? As a tool to answer this question, we first provide a complete characterization of the RC polytope in terms of its extremal behaviors. More specifically, by using the software *polymake* [21], we computed [22] all the extremal boxes for the RC polytope in the (3,2,2) scenario (see Appendix I). We found 153 600 extremal behaviors of the RC polytope, of which 64 belong to the local hidden variable (LHV) polytope, 2144 to the no-signaling (NS) polytope, and 151 392 being outside of the NS polytope. Considering equivalences up to local transformations and symmetry between Alice and Charlie, we have 1 Classical, 5 NS, and 190 genuinely RC equivalence classes, shown explicitly in Appendix I.

We also computed the general dimensionality of the RC polytope in the Bell scenario $(3, m, n)$, i.e., three parties with m measurements having n outcomes each, again in the measurement configuration of Fig. 1. This quantity works out to $\mathcal{D}[RC(3, m, n)] = [m(n-1)+1]^3 + m^2(m-1)(n-1)^2 - 1$ which is significantly larger than that of the usual no-signaling polytope. Further details are given in Appendix G.

The above characterization of the relativistic causal behaviors allowed us to identify *communication complexity scenarios*, cf. [23], in which relativistic causal correlations outperform all no-signaling correlations. As an example, in the Supplemental Material [24], we show a three-partite function that can be fully computed nonlocally using RC correlations, while the probability of doing so using no-signaling correlations is at most $3/4$.

VI. CONCLUDING REMARKS

Many interesting open questions arise from this work. The complete characterization of the RC correlation polytope in the (3,2,2) scenario provides a useful tool to investigate multiparty nonlocality in causal networks [25–31]. Another interesting question is to investigate the interplay between communication complexity and hardness in security proofs; for instance, does an information-theoretic principle, such as the nonreduction of communication complexity beyond the NS constraints, ensure the security of DI protocols? A crucial question is to identify natural physical principles upon which the security of DI cryptographic protocols can be based. An open question is whether these principles would allow correlations beyond the limits imposed by the no-signaling condition, in which case a new range of phenomena could be studied. Finally, it would also be interesting to study possible changes to the device-independent paradigm to restore security against adversaries only constrained by causality.

ACKNOWLEDGMENTS

R.S. acknowledges support of Comision Nacional de Investigacion Ciencia y Tecnologia (CONICYT) Programa de Formacion Capital Humano Avanzado/Beca de Postdoctorado en el extranjero (BECAS CHILE) 74160002, John Templeton Foundation and by Foundation for Polish Science under the grant TEAM-NET project (Contract No. POIR.04.04.00-00-17C1/18-00). M.K., D.G., and P.H. acknowledge support of John Templeton Foundation. K.H. acknowledges the grant Sonata Bis 5 (Grant No. 2015/18/E/ST2/00327) from the National Science Center and John Templeton Foundation. K.H. and P.H. are also supported by the Foundation for Polish Science (IRAP project, ICTQT, Contract No. 2018/MAB/5, co-financed by EU within Smart Growth Operational Programme). R.R. acknowledges the support of the Start-up Fund "Device-Independent Quantum Communication Networks" from The University of Hong Kong (166DRRAVI), 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)'. D.G. acknowledges partial support from Grant FONDECYT Iniciación number 11180474, Chile, and D.S. acknowledges support of NCN Grants No. 2016/23/N/ST2/02817 and No. 2014/14/E/ST2/00020.

APPENDIX A: INTRODUCTION TO THE APPENDICES

The most fundamental cryptography task is to achieve secure communication between two separated parties; this is the task of secure key distribution. We focus on this task in the parallel measurement scenario, as in this case an adversary cannot pursue drastic attacks. As one of the main results, we show that contrary to the case of no-signaling theory, there is no protocol in the parallel measurement scenario that allows for distributing keys secure against RC adversaries.

The way to check whether security is possible in NS theory is to test the level of violation of a Bell inequality. Special cases of Bell inequalities with only either 0 or 1 coefficients are called games [32]. In NS theory if some two parties share a device, the statistics of which violate a Bell inequality by a sufficiently high amount (or, in the case of games, win the game with high enough probability), then the so-called *monogamy* holds: none of them can achieve the same with respect to some other party, i.e., win the game with someone with large probability. This fact is fundamental for secure communication in quantum and NS theories. On our way to answer the main question we therefore first study whether

monogamy takes place in RC. Interestingly, we show a drastic violation of this phenomenon in the RC scenario. The above fact leads to our main contribution: that key rate in any Bell violation based security protocol is zero against RC adversaries.

APPENDIX B: GENERAL CONSTRAINTS OF RELATIVISTIC CAUSAL CORRELATIONS

In this Appendix we introduce a general formalism for the study of RC constraints in multipartite scenarios and a general spacetime. Consider a set of $[n] = \{1, \ldots, n\}$ parties with a string of inputs $\boldsymbol{x} = \{x_1, \ldots, x_n\}$ and string of outputs $\boldsymbol{a} = \{a_1, \ldots, a_n\}$, $\boldsymbol{S} \subseteq [n]$, with complement $\boldsymbol{S}^c$, such that $\boldsymbol{a_S} = \{a_i\}_{i\in\boldsymbol{S}}$ and an analogous definition for $\boldsymbol{x_S}$. In this scenario, the usual no-signaling constraints can be written as

$$P(\boldsymbol{a_S} \mid \boldsymbol{x_S}) = \sum_{\boldsymbol{a'_{S^c}}} P(\boldsymbol{a'_{S^c}}, \boldsymbol{a_S} \mid \boldsymbol{x'_{S^c}}, \boldsymbol{x_S}) = \sum_{\boldsymbol{a''_{S^c}}} P(\boldsymbol{a''_{S^c}}, \boldsymbol{a_S} \mid \boldsymbol{x''_{S^c}}, \boldsymbol{x_S}) \tag{B1}$$

for all $\boldsymbol{x'_{S^c}}$, $\boldsymbol{x''_{S^c}}$ In words, these constraints state that the probability distribution of the outputs of any subset of parties is independent from the inputs of the complementary set of parties. In the multipartite relativistic causal set of constraints we also consider the spacetime measurement events $\{M_{a_1}^{x_1}, \ldots, M_{a_n}^{x_n}\}$ in the spacetime $(\mathcal{M}, g_{\mu\nu})$ for some coordinate system (in special relativity this could be a particular reference frame). For a party p to influence the correlations of a set of parties $\boldsymbol{S} \not\ni \{p\}$ the event $M_{a_p}^{x_p}$ must satisfy

$$\bigcap_{q\in\boldsymbol{S}} J^+\left(M_{a_q}^{x_q}\right) \subset J^+\left(M_{a_p}^{x_p}\right). \tag{B2}$$

In words, this condition states that the causal future $J^+(M_{a_p}^{x_p})$ of party p's measurement event contains the intersection of the causal futures of the measurement events of all the parties $q \in \boldsymbol{S}$. Thus, a set $\boldsymbol{K}$ of parties might signal to another set $\boldsymbol{S}$ iff for each $\{p\} \in \boldsymbol{K}$ the condition (B2) is satisfied. If $\boldsymbol{K}$ cannot signal to $\boldsymbol{S}$ we say $\boldsymbol{K} \nrightarrow \boldsymbol{S}$; thus the RC conditions are all those of the form

$$P(\boldsymbol{a_S} \mid \boldsymbol{x_S}) = \sum_{\boldsymbol{a'_{S^c}}} P(\boldsymbol{a'} \mid \boldsymbol{x'}) = \sum_{\boldsymbol{a''_{S^c}}} P(\boldsymbol{a''} \mid \boldsymbol{x''}) \text{ iff } \forall\, \boldsymbol{K} \subseteq \boldsymbol{S}^c,\ \boldsymbol{K} \nrightarrow \boldsymbol{S}. \tag{B3}$$

Of course, in general this definition has redundant constraints and in general a subset of these constraints can determine the full set. By definition the RC constraints are a subset of no-signaling constraints; therefore no-signaling boxes satisfy the RC constrains while the opposite is not always true. An important remark to be made here is that for any spacetime and spacelike separated parties we have

$$P(a_p \mid x_p) = \sum_{\boldsymbol{a'}_{\{p\}^c}} P(\boldsymbol{a'} \mid \boldsymbol{x'}) = \sum_{\boldsymbol{a''}_{\{p\}^c}} P(\boldsymbol{a''} \mid \boldsymbol{x''}) \tag{B4}$$

for any single party p. This is the minimum number of RC constraints, which corresponds to the largest correlation polytope. Since always the single-party outcome probabilities are well defined, the signaling in RC can only target sets of parties with two or more elements, i.e., to a *region*. In this article we only consider cases where signaling from a region is the union of the several individual signals from parties inside that region; accordingly we designate the signaling allowed by RC as *point-to-region* (PTR) signaling without any loss of generality.

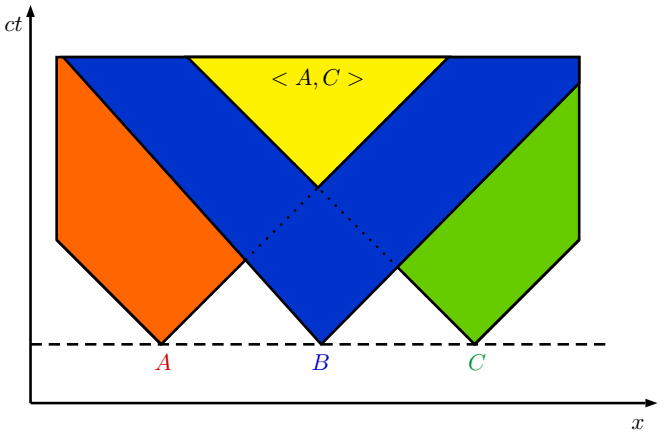

FIG. 3. A particular spacetime configuration of measurement events in the three-party Bell experiment. The spacetime locations of Alice, Bob, and Charlie's measurement events are A, B, C, respectively. The yellow area shows $J^+(A) \cap J^+(C)$, the only region where the information from the correlations between the outputs of Alice and Charlie, denoted $\langle A, C\rangle$, is accessible. The crucial property of this measurement configuration is that $J^+(A) \cap J^+(C) \subset J^+(B)$.

APPENDIX C: COMMUNICATION COMPLEXITY ADVANTAGE IN RELATIVISTIC CAUSAL THEORIES

The relativistic causal correlations in the measurement configuration of Fig. 3 are separated from the usual no-signaling correlations by constraints of the form

$$\sum_b P(a, b, c|x, y, z) - \sum_b P(a, b, c|x, y', z) = 0 \quad \forall\, a, c, x, z, y \neq y'. \tag{C1}$$

The usual no-signaling constraints impose equality above while this equality is not necessary for relativistic causality to hold as shown in [12]. The relaxation of these constraints is also reflected in a difference between the optimal success probability $\omega(G)$ of multiplayer games in NS theories versus that in RC theories. We first note that as in the no-signaling case, the calculation of the optimal success probability of multiplayer games in RC theories can be achieved in polynomial time by means of a linear program, and second we explain how advantages in some of these games imply communication complexity advantages.

As a first example of the difference in $\omega(G)$ between NS and RC theories, consider the "guess your neighbor's input" game (GYNI) in the (3,2,2) Bell scenario. The inputs x, y, z to the three parties in the game obey the promise $x \oplus y \oplus z = 0$ and the task is for each party to output their neighbor's input,

so that the expression for the success probability in the game is given by

$$\omega(\mathrm{GYNI}) = \tfrac{1}{4}[P(000|000) + P(110|011) + P(011|101) + P(101|110)]. \quad \text{(C2)}$$

It was shown in [33] that $\omega_c(\mathrm{GYNI}) = \omega_q(\mathrm{GYNI}) = \frac{1}{4}$ while correlations obeying the no-signaling constraints allow $\omega_{ns}(\mathrm{GYNI}) = \frac{1}{3}$. Here, ω_c, ω_q, and ω_{ns} denote the optimal success probability in classical, quantum, and no-signaling theories, respectively, while similarly ω_{rc} will denote the optimal success probability in theories that only impose relativistic causality. A simple maximization over the constraints in Eq. (B3) gives that $\omega_{rc}(\mathrm{GYNI}) = \frac{1}{2}$ and this optimal value is achieved by the RC box (extremal box class No. 77 in Appendix I):

$$B^{\mathrm{RC}}_{\mathrm{GYNI}} : P(abc \mid xyz) = \begin{cases} \frac{1}{2}, & \text{if } (1 \oplus b \oplus c \oplus y)(1 \oplus a \oplus b \oplus x) = 1, \\ 0, & \text{otherwise.} \end{cases} \quad \text{(C3)}$$

As a second example, we present games where RC correlations allow the players to win with certainty (success probability 1) while the best no-signaling strategy gives a success probability less than 1. In these games, we consider three parties, of whom only the outputs of two parties appear in the winning constraint, while the third player helps the others achieve their task, so that one might term these games as "games with allies" (GWA). Specifically, we propose a GWA game for Alice and Charlie with Bob as the ally, with a winning constraint given by

$$xy \oplus yz = a \oplus c, \quad \text{(C4)}$$

where as usual x, y, z denote the inputs of the three players and a, b, c denote their respective outputs. For this game, a simple maximization over the usual no-signaling constraints by a linear program shows that $\omega_{ns}(\mathrm{GWA}) = \frac{3}{4}$. In fact, a classical strategy exists that achieves this value, and is simply given when Alice and Charlie output $a = c = 0$ for any input x, y, z. When $y = 0$, this strategy satisfies the winning constraint $a \oplus c = (x \oplus z)y = 0$, and when $y = 1$, this strategy satisfies $a \oplus c = (x \oplus z)$ in exactly half of the cases, so that the optimal success probability $\omega_c(\mathrm{GWA}) = \frac{3}{4}$ is achieved. On the other hand using a RC box is it possible to win the GWA with certainty. Specifically, consider the RC box (extremal box class No. 76 in Appendix I):

$$B^{\mathrm{RC}}_{\mathrm{GWA}} : P(abc \mid xyz) = \begin{cases} \frac{1}{2}, & \text{if } (1 \oplus a \oplus b \oplus xy)(1 \oplus b \oplus c \oplus zy) = 1, \\ 0, & \text{otherwise.} \end{cases} \quad \text{(C5)}$$

This box satisfies $a \oplus b = xy$ and $b \oplus c = zy$ (two Popescu-Rohrlich type boxes between A-B and B-C) so that it directly satisfies $a \oplus c = xy \oplus zy$, which gives $\omega_{rc}(\mathrm{GWA}) = 1$. In the literature the condition (C4) appears in [34] as a communication complexity task for Alice and Charlie: They must compute functions $f(x, y, z) = h(x, y) \oplus g(y, z)$, sharing 1 bit of information and without communication with Bob. This shows that RC boxes can be used to trivialize some communication complexity tasks [34]. This remarkable result suggests that a communication principle demanding the nontrivialization of GWA games has direct consequences on RC correlations. Could it be that a communication principle implies enough restrictions to certify a security protocol in RC theories? We leave for future research the investigation of this question.

APPENDIX D: LACK OF MONOGAMY FOR TWO-PLAYER GAMES IN RC THEORIES

An important consequence of the relaxation of the no-signaling constraints to those that are sufficient to ensure relativistic causality is the resulting lack of monogamy for general two-player games in RC theories. In particular, when the players' measurements are arranged in the spacetime configuration of Fig. 3, for any two-player game G it holds that $\omega_{rc}(G^{AB}) = \omega_{rc}(G^{BC}) = \omega_{ns}(G)$. In other words, both players are able to achieve the maximum no-signaling (equal to the relativistic causal) value of the two-player game G in this configuration. We give the proof of this statement for a general bipartite Bell inequality in this section.

Consider a general bipartite Bell inequality G of the form

$$G := \sum_{a,b,x,y} \alpha_{a,b,x,y} P(a, b|x, y) \leqslant \omega_c(G), \quad \text{(D1)}$$

where we take without loss of generality $\alpha_{a,b,x,y} \geqslant 0$ and normalize the inequality so that $\omega_c(G) \leqslant 1$.

Proposition 2. Consider any bipartite Bell inequality G of the form in Eq. (D1). Suppose three players perform their measurements in the spacetime configuration of Fig. 3, and that both Alice-Bob and Bob-Charlie test for the violation of G. Then, there exist correlations $\{P(a, b, c|x, y, z)\}$ in RC theories that allow both A-B and B-C to achieve $\omega_{ns}(G)$.

Proof. We construct the required RC box $\{P(a, b, c|x, y, z)\}$ depending on the bipartite Bell inequality G as follows. Let $\{Q(a, b|x, y)\}$ be a two-party no-signaling box that achieves the maximum no-signaling (equal to relativistic causal, in this bipartite case) value $\omega_{ns}(G)$.

Fix $y = 1$. The box $\{Q(a, b|x, y = 1)\}$ is local realistic by virtue of the fact that party B only chooses the single input $y = 1$. We construct a symmetric extension of $\{Q(a, b|x, y = 1)\}$ to the three-party box $\{\tilde{Q}_1(a, b, c|x, y = 1, z)\}$ such that the two-party marginals A-B and C-B are equal to $Q(a, b|x, y = 1)$; i.e., we impose

$$Q(a, b|x, y = 1) = \sum_c \tilde{Q}_1(a, b, c|x, y = 1, z) = \sum_{a'} \tilde{Q}_1(a', b, c'|x', y = 1, z') \quad \forall \; b, a = c', x = z'. \quad \text{(D2)}$$

Such a symmetric extension can always be constructed for the local realistic box $\{Q(a, b|x, y = 1)\}$. To make this more explicit, suppose that the box has the following decomposition into classical deterministic boxes:

$$Q(a, b|x, y = 1) = \sum_\lambda p_\lambda Q_A(a|x, \lambda) Q_B(b|y = 1, \lambda). \quad \text{(D3)}$$

One can then construct the symmetric extension $\{\tilde{Q}_1(a, b, c|x, y = 1, z)\}$ as

$$\tilde{Q}_1(a, b, c|x, y = 1, z) = \sum_{\lambda} p_\lambda Q_A(a|x, \lambda) Q_B(b|y = 1, \lambda) Q_A(c|z, \lambda), \quad \text{(D4)}$$

where the marginal distribution for party C is the same as that for A, and Q_A, Q_B are deterministic boxes. Note that the symmetric extension obeys all the usual no-signaling constraints; i.e., every bipartite marginal $\tilde{Q}_1(a, b|x, y = 1)$ and $\tilde{Q}_1(b, c|y = 1, z)$ as well as the single-party marginals $\tilde{Q}_1(a|x)$, $\tilde{Q}_1(b|y = 1)$, and $\tilde{Q}_1(c|z)$ are well defined independently of the inputs of the remaining parties.

Similarly, fix $y = 2, 3, \ldots, |Y|$ and construct the corresponding symmetric extensions $\tilde{Q}_k(a, b, c|x, y = k, z)$ for each of the local realistic boxes $Q(a, b|x, y = k)$. In all these boxes again, the bipartite and single-party marginals are well defined independently of the inputs of the other parties, and moreover we have that

$$\begin{aligned} \tilde{Q}_k(a|x) = \tilde{Q}_{k'}(a|x) = \sum_b Q(a, b|x, y = 1) \quad \forall] a, x, k, k', \\ \tilde{Q}_k(c|z) = \tilde{Q}_{k'}(c|z) = \sum_b Q(c, b|z, y = 1) \quad \forall\, c, z, k, k', \end{aligned} \quad \text{(D5)}$$

by the property of the symmetric extension; i.e., A and C's marginals are the same in each extension.

Now, putting together all the symmetric extensions, we obtain the combined box $P(a, b, c|x, y, z)$ that is the required box shared by the three parties A, B, and C, with $P(a, b, c|x, y = k, z) = \tilde{Q}_k(a, b, c|x, y = k, z)$ for every k, a, b, c, x, z. This box satisfies all the RC constraints in Eq. (B3) by the argument above. Note that in general,

$$\sum_b P(a, b, c|x, y = k, z) \neq \sum_b P(a, b, c|x, y = k', z) \quad k \neq k', \quad \text{(D6)}$$

but we have seen that this is precisely the missing constraints from the usual no-signaling conditions, that is not necessary to ensure by causality in this measurement configuration. Since the two-party marginals $P(a, b|x, y)$ and $P(c, b|z, y)$ are both equal to $Q(a, b|x, y)$, we have that both A-B and B-C achieve the maximum no-signaling value $\omega_{ns}(G)$. This completes the proof. ■

As an example of the general proposition above, we find that the following RC box,

$$B^{\mathrm{RC}}_{G_u} : P(abc \mid xyz) = \begin{cases} \frac{1}{d}, & \text{if } a = \pi_{xy}(b),\ c = \pi_{zy}(b), \\ 0, & \text{otherwise,} \end{cases} \quad \text{(D7)}$$

allows both A-B and B-C to achieve the maximum no-signaling value of 1, for any unique game G_u defined by a set of permutations $\{\pi_{xy}\}$.

APPENDIX E: THE NO-GO THEOREM FOR DEVICE-INDEPENDENT SECURITY IN RELATIVISTIC CAUSAL THEORIES

In this Appendix we complete the proof of the no-go theorem presented in our article. The main theorem is as follows:

Theorem 3. Assume that N reliable agents perform their measurements with inputs $\mathbf{q} = y_1, \ldots, y_N$ and outputs $\mathbf{r} = b_1, \ldots, b_N$ in arbitrary spacelike separated positions, to compute any multipartite Bell inequality G of the form

$$G := \sum_{\mathbf{r},\mathbf{q}} V(\mathbf{r}, \mathbf{q}) P(\mathbf{r} \mid \mathbf{q}) \leqslant \omega_c(G), \quad \text{(E1)}$$

in which a violation of G, $\omega^* > \omega_c$ is observed. Then, there is a spacetime configuration for two eavesdroppers' measurements, so that N correlations of those measurements will reproduce the statistics of the N reliable agents after the eavesdroppers meet or communicate their results.

Proof. We begin with a brief description of the idea of the proof. We consider two eavesdroppers E_1 and E_2. We show that satisfying RC constraints one can construct a device such that the inputs and outputs of the honest parties' devices are encoded into correlations between E_1 and E_2. In order to avoid signaling, the local marginals of the eavesdroppers are uniform, as one of the Eves in a sense one-time-pads the information of the other. We borrow this idea from the simplest secret sharing scheme. To give a concrete example, the outputs of the honest parties $\mathbf{r} = b_1, \ldots, b_N$ will be encoded into variables of Eves $\mathbf{d}$ and $\mathbf{c}$, respectively, as follows. For each of $j \in \{1, \ldots, N\}$ there is $d_j = c_j \oplus_{H_j} b_j$ where addition is modulo H_j—the dimension of b_j—and the distribution of c_j is $\frac{1}{H_j}$. It is easy to see that none of the eavesdroppers can gain any knowledge about each of b_j; however upon meeting they can learn each of b_j perfectly.

We are ready to proceed with details of the proof. Consider two eavesdroppers E_1, E_2 with devices that have only outputs $\mathbf{s}_1 = c_1, \ldots, c_N, z_1, \ldots, z_N$, $\mathbf{s}_2 = d_1, \ldots, d_N, w_1, \ldots, w_N$, respectively. Let us say the eavesdroppers want to attack all trusted parties $B_1, \ldots, B_N$. Given a particular reference system $S(\vec{r}, t)$ there always exists an event p_B in a causal spacetime, such that the spacetime convex hull $\mathcal{B}$ of the spacelike separated measurement events $p_{B_1}, \ldots, p_{B_N}$ performed by the $B_1, \ldots, B_N$ parties is completely inside its causal past $J^-(p_B) \supseteq \mathcal{B}$. When the two eavesdroppers E_1, E_2 can choose any spacelike separated positions for their measurement events p_{E_1}, p_{E_2}, in particular they can satisfy $J^+(p_{E_1}) \cap J^+(p_{E_2}) \subseteq J^+(p_B)$ for any spacetime which is causal and simply connected. In this case every $B_1, \ldots, B_N$ can signal to any correlation between the outputs of E_1, E_2.

Then, the eavesdroppers could distribute a behavior that satisfies

$$\sum_{\mathbf{r}} \tilde{Q}_{\mathbf{k}}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k}) \neq \sum_{\mathbf{r}} \tilde{Q}_{\mathbf{k}'}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k}') \quad \forall\, \mathbf{k} \neq \mathbf{k}'. \tag{E2}$$

The correlation between the outputs of E_1, E_2 can be chosen such that $d_j = c_j \bigoplus_{H_j} b_j$ and $w_j = z_j \bigoplus_{L_j} y_j$, with H_j the dimension of outputs b_j (also outputs c_j, d_j are chosen to have dimension H_j), L_j the dimension of inputs y_j (also outputs z_j, w_j are chosen to have dimension L_j), and $\bigoplus_{H_j}, \bigoplus_{L_j}$ are sums mod H_j and mod L_j, respectively.

Now, we should check that no-signaling conditions are satisfied according to the scenario. First, because the E_1, E_2 have no input, they cannot signal to the $B_1, \ldots, B_N$. Second, the $\tilde{Q}_{\mathbf{k}}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k})$ is a classical distribution because it has a single input $\mathbf{k}$ and in consequence we can choose

$$\tilde{Q}_{\mathbf{k}}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k}) = \sum_{\lambda} p_\lambda Q_B(\mathbf{r} \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) Q_E(\mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) \quad \forall\, \mathbf{k}, \tag{E3}$$

where $Q_B(\mathbf{r} \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k}))$ reproduce the marginals of $Q(\mathbf{r} \mid \mathbf{q} = \mathbf{k})$ for each particular $\mathbf{k}$ when $Q(\mathbf{r} \mid \mathbf{q})$ is the no-signaling box that achieves the value $\omega'(G) > \omega_c(G)$ expected by the parties $B_1, \ldots, B_N$ for the Bell inequality G. Because $Q(\mathbf{r} \mid \mathbf{q})$ is no-signaling, then no B_i signals to any B_j. Now, what is left is to check that $B_1, \ldots, B_N$ do not signal either to E_2 or to E_1. That is,

$$\begin{aligned} \sum_{\mathbf{r},\mathbf{s}_2} \tilde{Q}_{\mathbf{k}}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k}) &= \sum_{\mathbf{r},\mathbf{s}_2} \tilde{Q}_{\mathbf{k}'}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k}') \quad \forall\, \mathbf{k} \neq \mathbf{k}', \\ \sum_{\mathbf{r},\mathbf{s}_1} \tilde{Q}_{\mathbf{k}}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k}) &= \sum_{\mathbf{r},\mathbf{s}_1} \tilde{Q}_{\mathbf{k}'}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k}') \quad \forall\, \mathbf{k} \neq \mathbf{k}'. \end{aligned} \tag{E4}$$

At this point we remark that λ carries on the information from $\mathbf{r} = b_1, \ldots, b_N$ which determine the correlation of outputs c_j, d_j. Now, since $d_j = c_j \bigoplus_{H_j} b_j$ and $w_j = z_j \bigoplus_{L_j} y_j$ the outputs c_j, d_j, z_j, w_j depend only on the inputs and outputs y_j, b_j of agent B_j. Because of the functional dependencies above we can rewrite $Q_E(\mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k}))$ as

$$Q_E(\mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) = \prod_j Q_E^{(j)}(c_j, d_j, z_j, w_j \mid \lambda(b_j, y_j), y_j). \tag{E5}$$

Here a valid choice for each $Q_E^{(j)}$ is

$$Q_E^{(j)}(c_j, d_j, z_j, w_j \mid \lambda(b_j, y_j), y_j) = \begin{cases} \frac{1}{H_j L_j}, & d_j = c_j \bigoplus_{H_j} b_j \text{ and } w_j = z_j \bigoplus_{L_j} y_j, \\ 0, & \text{otherwise.} \end{cases} \tag{E6}$$

If we consider the behavior of the form (E3) to obtain the marginal of E_2,

$$\begin{aligned} \sum_{\mathbf{r},\mathbf{s}_1} \tilde{Q}_{\mathbf{k}}(\mathbf{r}, \mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{q} = \mathbf{k}) &= \sum_{\mathbf{r},\mathbf{s}_1} \sum_{\lambda} p_\lambda Q_B(\mathbf{r} \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) Q_E(\mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) \\ &= \sum_{\mathbf{r}} \sum_{\lambda} p_\lambda Q_B(\mathbf{r} \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) \sum_{\mathbf{s}_1} Q_E(\mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) \\ &= \sum_{\mathbf{r}} \sum_{\lambda} p_\lambda Q_B(\mathbf{r} \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) \sum_{c_N, z_N} \cdots \sum_{c_1, z_1} Q_E(\mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})). \end{aligned}$$

But, if we sum the distributions $Q_E(\mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k}))$ over the components (c_i, z_i) of $\mathbf{s}_1$ we obtain

$$\begin{aligned} \sum_{c_i, z_i} Q_E(\mathbf{s}_1, \mathbf{s}_2 \mid \mathbf{k}, \lambda(\mathbf{r}, \mathbf{k})) &= \sum_{c_i, z_i} \prod_j Q_E^{(j)}(c_j, d_j, z_j, w_j \mid \lambda(b_j, y_j), y_j) \\ &= \prod_{j \neq i} Q_E^{(j)}(c_j, d_j, z_j, w_j \mid \lambda(b_j, y_j), y_j) \sum_{c_i, z_i} Q_E^{(i)}(c_i, d_i, z_i, w_i \mid \lambda(b_j, y_j), y_j) \\ &= \prod_{j \neq i} Q_E^{(j)}(c_j, d_j, z_j, w_j \mid \lambda(b_j, y_j), y_j) \sum_{c_i, z_i} Q_E^{(i)}\left(d_i = c_i \bigoplus_{H_i} b_i, w_i = z_i \bigoplus_{L_i} y_i \mid \lambda(b_j, y_j), y_j\right) \\ &= \prod_{j \neq i} Q_E^{(j)}(c_j, d_j, z_j, w_j \mid \lambda(b_j, y_j), y_j) \left(\frac{1}{H_i L_i}\right), \end{aligned}$$

where in the last step we use the fact that the permutations $\pi_{b_j}(\cdot) = (\cdot) \bigoplus_{H_j} b_j$ and $\pi_{y_j}(\cdot) = (\cdot) \bigoplus_{L_j} y_j$ have a unique value. Since the above calculation is equally valid when summing up over every pair (c_i, z_i) of $\mathbf{s}_1$ we have

$$\begin{aligned}\sum_{\mathbf{r},\mathbf{s}_1}\tilde{Q}_{\mathbf{k}}(\mathbf{r},\mathbf{s}_1,\mathbf{s}_2\mid\mathbf{q}=\mathbf{k}) &= \sum_{\mathbf{r}}\sum_{\lambda} p_\lambda Q_B(\mathbf{r}\mid\mathbf{k},\lambda(\mathbf{r},\mathbf{k}))\sum_{c_N,z_N}\cdots\sum_{c_1,z_1} Q_E(\mathbf{s}_1,\mathbf{s}_2\mid\mathbf{k},\lambda(\mathbf{r},\mathbf{k}))\\ &= \sum_{\mathbf{r}}\sum_{\lambda} p_\lambda Q_B(\mathbf{r}\mid\mathbf{k},\lambda(\mathbf{r},\mathbf{k}))\left(\frac{1}{H_1L_1}\right)\sum_{c_N,z_N}\cdots\sum_{c_2,z_2}\prod_{j\neq 1} Q_E^{(j)}(c_j,d_j,z_j,w_j\mid\lambda(b_j,y_j),y_j)\\ &\vdots\\ &= \sum_{\mathbf{r}}\sum_{\lambda} p_\lambda Q_B(\mathbf{r}\mid\mathbf{k},\lambda(\mathbf{r},\mathbf{k}))\left(\prod_{j=1}^{N}\frac{1}{H_jL_j}\right)\\ &= \left(\prod_{j=1}^{N}\frac{1}{H_jL_j}\right)\sum_{\mathbf{r}}\sum_{\lambda} p_\lambda Q_B(\mathbf{r}\mid\mathbf{k},\lambda(\mathbf{r},\mathbf{k})) = \prod_{j=1}^{N}\frac{1}{H_jL_j}.\end{aligned}$$

Hence, the marginal of E_2 is

$$\sum_{\mathbf{r},\mathbf{s}_1}\tilde{Q}_{\mathbf{k}}(\mathbf{r},\mathbf{s}_1,\mathbf{s}_2\mid\mathbf{q}=\mathbf{k}) = \prod_{j=1}^{N}\frac{1}{H_jL_j}\quad\forall\,\mathbf{k}. \tag{E7}$$

Now, since the permutations $\pi_{b_j}(\cdot)$, $\pi_{y_j}(\cdot)$ have unique inverses $\pi_{b_j}^{-1}(\cdot)$, $\pi_{y_j}^{-1}(\cdot)$, respectively, we can apply the same arguments when summing up with every pair (d_i, w_i) of $\mathbf{s}_2$. Then, a direct calculation shows that the marginal of E_1 is

$$\sum_{\mathbf{r},\mathbf{s}_2}\tilde{Q}_{\mathbf{k}}(\mathbf{r},\mathbf{s}_1,\mathbf{s}_2\mid\mathbf{q}=\mathbf{k}) = \prod_{j=1}^{N}\frac{1}{H_jL_j}\quad\forall\,\mathbf{k}. \tag{E8}$$

This demonstrates that the marginals of E_1 and E_2 are independent from the inputs of B_j for each $j\in\{1,\ldots,N\}$.

To complete the attack, we specify how the eavesdroppers can extract the information of $Q(\mathbf{r}\mid\mathbf{q})$ from $\mathbf{s}_1,\mathbf{s}_2$. As we have seen the value of $Q_E(\mathbf{s}_1,\mathbf{s}_2\mid\mathbf{q}=\mathbf{k},\lambda(\mathbf{r},\mathbf{k}))$ is nonzero only when $d_j = c_j\bigoplus_{H_j} b_j$ and $w_j = z_j\bigoplus_{L_j} y_j$ for every $j\in\{1,\ldots,N\}$. Then, from the table of values $\mathbf{s}_1,\mathbf{s}_2$ is possible to compute a table $\mathbf{r},\mathbf{q}$ and determine a distribution $Q_E(\mathbf{r},\mathbf{q})$. From here we compute

$$Q(\mathbf{r}\mid\mathbf{q}) = \frac{Q_E(\mathbf{r},\mathbf{q})}{\sum_{\mathbf{r}}Q_E(\mathbf{r},\mathbf{q})}. \tag{E9}$$

Finally, the eavesdroppers are able to compute $Q(\mathbf{r}\mid\mathbf{q})$ without affecting the violation $\omega'(G)>\omega_c(G)$ observed by parties B_j.■

We remark that such attack is possible because behaviors $\tilde{Q}_{\mathbf{k}}(\mathbf{r},\mathbf{s}_1,\mathbf{s}_2\mid\mathbf{q}=\mathbf{k})$ are allowed by the relativistic causal constraints.

APPENDIX F: NO SECURE KEY DISTILLATION VIA DIRECT MEASUREMENT AND LOPC OPERATIONS, AGAINST RC ADVERSARIES

In the previous Appendix, we have shown that two collaborating eavesdroppers can learn a copy of correlations shared by two honest parties. Intuitive as it is, in such a case, no cryptographic protocol based on these correlations could be accomplished. However, cryptography is a domain which studies a plethora of security scenarios. Proving a no-go result for each of them is a difficult task, as the proof is highly dependent on the mathematical description of a particular scenario (such as two-party cryptographic protocols, secret sharing, anonymous voting, public-key cryptographic protocols, or private randomness generation). The most fundamental among those scenarios is, no doubt, the secure key distribution between two honest parties against an adversary. To exemplify that it may not be possible in RC, we prove in detail that a broad class of protocols yield zero key rate in the latter scenario. These are protocols that obtain key via the same measurement in each run of the protocol. They are called "measured device followed by local operations and public communications" (MDLOPC). Notably, all modern protocols in device-independent cryptography and quantum device-independent cryptography are MDLOPC operations (see [32] and [19] and references therein). Moreover, in the scenario of secure key distribution against the nonsignaling adversary, it is believed that a more general class cannot yield positive key [35]. This fact justifies our focus on MDLOPC operations that lead to positive key in the case of a nonsignaling adversary [8,9,36]. As we will see, no such protocol can achieve a positive key rate against the relativistic causal ones. Since we will base the discussion on the results of Theorem 3, we will consider two collaborating adversaries (eavesdroppers) rather than a single one.

1. Scenario for secure key distribution against the relativistic causal adversary

In the scenario of secure key distribution against relativistic causal (RC) adversaries, the M honest parties share N copies of a (single-use) device. The M parties first measure each of N devices $P(ABE_1E_2|Y_1,\ldots,Y_M,Z_1,Z_2)$ with the same direct $\mathbf{q} := (y_1^1,\ldots,y_M^1)$. They further apply an LOPC (local operations and public communications) operation on outputs $\mathbf{r} := (b_1,\ldots,b_M)$ of the measurement. This class of operations (introduced in [19]) is called MDLOPC (measurement on device followed by LOPC operations).

In practical protocols, there are two phases: testing and key generation. The measurements in the protocol are taken randomly for both tests and key generation. There is a finite set of test measurements, while there is a single measurement for key generation [here $(y_i^1)_{i=1}^M$]. The testing rounds are necessary for checking the value of the Bell inequality. If this value is high enough, the data from key generation rounds are processed to produce key. The whole protocol is aborted otherwise. In what follows, we assume that the device has passed the test, which means that the tested Bell violation is high enough (or even maximal possible). This fact ensures that in the no-signaling case, Alice and Bob would be able in principle to produce key by postprocessing (information reconciliation and privacy amplification). For the sake of clarity, we will present the proof for $M = 2$ honest parties and later show how to generalize the result for an arbitrary number of them based on Ref. [37]. Consequently, instead of inputs Y_1, Y_2 and outputs B_1, B_2 we will write X, Y and A, B, respectively, and use lowercase for the values of random variables (e.g., $X = x, Y = y$). In what follows, the attack by the Eves will be chosen such that Z_1, Z_2 will both be unary, and hence omitted in notation in most cases.

We are ready to define the protocol of key distillation for the case of the two honest parties A and B.

Definition 1. A protocol of key distillation is a sequence of MDLOPC operations $\Lambda = \{\Lambda_N\}$, performed by the honest parties, each element of which consisting of a measurement stage $\{\mathcal{M} = (y_i^1)_{i=1}^M\}$ with $y_i^1 = y^1$, followed by a postprocessing $\{\mathcal{P}_N\}$. Moreover, for each consecutive N copies of shared devices $P \equiv P(A, B, E|XYZ)^{\otimes N}$, it outputs a conditional probability distribution such that

$$\left\| \Lambda_N(P^{\otimes N}) - \hat{P}_{\text{ideal}}^{(d_N)} \right\|_{RC} \leqslant \varepsilon_N \overset{N\to\infty}{\longrightarrow} 0, \tag{F1}$$

where an *ideal distribution* $\hat{P}_{\text{ideal}}^{(d_N)}$ is perfectly correlated between the honest parties, and product with the device of the eavesdroppers:

$$\hat{P}_{\text{ideal}}^{(d_N)}(A = a, B = b, E_1, E_2|Z_1, Z_2) = \left(\frac{\delta_{A=a,B=b}}{d_N}\right) \sum_{a,b} P(A = a, B = b, E_1, E_2|Z_1, Z_2), \tag{F2}$$

with $P(A = a, B = b, E_1, E_2|Z_1, Z_2) \equiv \Lambda_N(P^{\otimes N})$. Moreover by $||P - Q||_{RC} := \sup_{\theta \in RC} ||\theta(P) - \theta(Q)||_1$, we mean the supremum of distinguishability between the distributions achievable by the linear operations satisfying relativistic causality, and $d_N = \text{dimA}^N$.

Knowing what the protocols of key distillation in the considered scenario are, we can pass to define the quantity of the key secure against RC adversaries. We limit ourselves here to the case of the key distilled by MDLOPC protocols.

Definition 2 (key secure against RC adversary). Given a tripartite device $P \equiv P(ABE|XYZ)$ the secret key rate of the protocol of key distillation $\{\Lambda_N\}$, on N iid copies of the device, denoted by $\mathcal{R}(\Lambda|_P)$ is a number $\limsup_{N\to\infty} \frac{\log_2 d_N}{N}$, where $\log_2 d_N$ is the length of a secret key shared between Alice and Bob, with $d_N = \dim_A(\Lambda_N(P^{\otimes N}))$. The rate of device-independent key secure against RC adversary in the iid scenario is given by

$$K_{DI}^{\text{RC}}(P) = \sup_{\Lambda_N \in \text{MDLOPC}} \mathcal{R}(\Lambda|_P), \tag{F3}$$

where the supremum is taken with respect to MDLOPC protocols.

2. No-go for MDLOPC protocols

To show that the key rate obtained by MDLOPC operations secure against RC adversaries is zero, we demonstrate an upper bound on the key rate and show that it is zero. We achieve this task by relating the introduced scenario of security against relativistic causal adversaries with the so-called *secure key agreement* (SKA) [38].

Since we are going to refer to SKA, we recall it briefly here. There, the honest parties and an eavesdropper share (asymptotically growing number) N copies of a joined probability distribution $P(A, BE)$. The parties can perform LOPC operations. The eavesdropper collects the public communication during the protocol. The original security condition that is demanded for an output of a key distillation protocol is rather involved [38]. It has been however shown in [19] that a simple lower bound holds:

Theorem 4. [19]. The secret key rate $S(A : B||E)$ of the SKA cryptographic model [38,39] is lower bounded by the following asymptotic expression:

$$\text{S}(A : B||E)_{P(ABE)} \geqslant \sup_{\mathcal{P}} \limsup_{N\to\infty} \frac{\log_2 \dim_A}{[\mathcal{P}_N(P^{\otimes N}(ABE))]} N, \tag{F4}$$

with security condition

$$\left\| \mathcal{P}_N(P^{\otimes N}(ABE)) - P_{\text{ideal}}^{(d_N)} \right\|_1 \leqslant \delta_N \overset{N\to\infty}{\longrightarrow} 0, \tag{F5}$$

where $\mathcal{P} = \cup_{N=1}^{\infty}\{\mathcal{P}_N\}$ is a cryptographic protocol consisting of LOPC operations, acting on N iid copies of the classical probability distribution $P(ABE)$. Moreover $P_{\text{ideal}}^{(d_N)} = \frac{\delta_{A=a,B=b}}{d_N} P(E)$, and $P(E) = \sum_{a,b} P(A = a, B = b, E)$.

Let us describe the idea of the proof of the no-go briefly. We consider a family of tripartite devices with unary input on the eavesdropper's part (hence omitted in notation) that realize the attack described in Theorem 3. For a fixed number of copies N, it reads $P(ABE_1E_2|XY)^{\otimes N}$. Since the honest parties first measure their device, the figure of merit is, in fact, a

joined probability distribution $P(ABE_1E_2|X=x,Y=y)^{\otimes N}$. In this case, the norm $||.||_{RC}$ of the difference of two conditional distributions in Eq. (F1) is equal to the variational distance between two distributions. Hence, the key secret against the Eves under this particular strategy turns out to be upper bounded by the key obtained from $P(AB\bar{E})^{\otimes N}$ by LOPC operations, where $\bar{E}=(AB)$. Indeed from Theorem 3, the two Eves can upon meeting learn the realization of the marginal $P(AB|X=x,Y=y)$. In this way, the Eves switch from the RC scenario to the secrete key agreement scenario. In the latter scenario, there is a well known bound on the secure key $S(A:B||\bar{E})$, called *intrinsic information*. The intrinsic information of a distribution $P(ABE)$ is $I(A:B\downarrow E)_{P(ABE)}:=\inf_{\Lambda_E:E\to E'} I(A:B|E')_{P(ABE')}$. Here $I(A:B|E')_{P(ABE')}$ is the *conditional mutual information* equal to $H(AE')+H(BE')-H(E')-H(ABE')$ with $H(X)$ denoting a Shannon entropy of the random variable X, and the infimum is taken over stochastic maps transforming E into E'. We have then the following:

Theorem 5. [40]. For any tripartite distribution $P(ABE)$, there is

$$S(A:B||E)_{P(ABE)}\leqslant I(A:B\downarrow E)_{P(ABE)}. \tag{F6}$$

We are ready now to state the main result of this section: a no-go for distillation via MDLOPC operations.

Theorem 6. (no-go for MDLOPC secure key distribution). For any $P_{AB}\equiv P(A,B|X,Y)$ satisfying no-signaling constraints, there exists a spacetime configuration of two eavesdroppers E_1 and E_2 and a tripartite distribution $P(A,B,E_1,E_2|X,Y)$ satisfying RC constraints, with marginal distribution on AB equal to P_{AB} such that

$$K_D^{\mathrm{RC}}(P(ABE_1E_2|XY))=0. \tag{F7}$$

Proof. Let us fix $\eta>0$. For this η there exist natural N, $\epsilon_N>0$ and the operation of the MDLOPC protocol, which is η-optimal. We denote this operation as $\Lambda_N:=\mathcal{P}_N\circ\mathcal{M}_N$. The first part $\mathcal{M}_N$ is equivalent to an N-fold measurement x^1,y^1 [the same on each of the copies of $P(ABE_1E_2|X,Y)$]. By η-optimality we mean that the rate of protocol $\{\Lambda_N\}$ is close by η to the optimal $K_D^{\mathrm{RC}}(P(ABE_1E_2|XY))$:

$$(1/N)\log_2\dim_A[\Lambda_N(P^{\otimes N}(ABE_1E_2|X,Y))]\geqslant K_D^{\mathrm{RC}}(P(ABE_1E_2|X,Y))-\eta \tag{F8}$$

and

$$\left\|\Lambda_N(P^{\otimes N}(ABE_1E_2|XY))-\hat{P}_{\mathrm{ideal}}^{(d_N)}\right\|_{RC}\leqslant\epsilon_N. \tag{F9}$$

Now, thanks to Theorem 3 the device $P(ABE_1E_2|XY)$ can be chosen such that the two Eves, upon meeting, are able to learn a copy of a realization of each copy of the distribution $P(A,B|X=x^1,Y=y^1)$. Let us note here that the Eves can learn not only the outputs AB but also the inputs X,Y. However in the class of MDLOPC protocols the measurement (x^1,y^1) that attains the supremum in the definition of K_D^{RC} is known to Eve(s). This is because the protocol, as it is usually assumed, is publicly known in particular to adversaries. We focus then on the fact that the Eves learn the outputs, so that $\Omega_E((E_1E_2)^{\otimes N})=(AB)^{\otimes N}$. Since Ω_E is (in principle unnecessary) action of Eves, the key can only be higher after performing Ω_E:

$$\frac{\log_2\dim_A[\Lambda_N(P^{(N)}(ABE_1E_2|XY))]}{N}=\frac{\log_2\dim_A[\mathcal{P}_N(P^{(N)}(ABE_1E_2|X=x^1,Y=y^1))]}{N}\leqslant\frac{\log_2\dim_A[\mathcal{P}_N(P(AB(AB))^{\otimes N})]}{N}, \tag{F10}$$

where $(\frac{1}{N})\log_2\dim_A[\mathcal{P}_N(P(AB(AB))^{\otimes N})]$ is the key rate of the LOPC protocol $\mathcal{P}_N$ when acting on $P(AB(AB))^{\otimes N}$. We have also

$$\left\|\Lambda_N(P(ABE_1E_2|XY)^{\otimes N})-\hat{P}_{\mathrm{ideal}}^{(d_N)}\right\|_{RC}\leqslant\epsilon_N\Rightarrow\left\|\mathcal{P}_N(P(AB(AB))^{\otimes N})-P_{\mathrm{ideal}}^{(d_N)}\right\|_1\leqslant\epsilon_N. \tag{F11}$$

Indeed, the measurement $(X,Y)=(x^1,y^1)$ operation composed with an LOPC protocol $\mathcal{P}_N$ is one of the linear operations satisfying RC; hence we have

$$\sup_{\theta\in RC}\left\|\theta\left[\Lambda_N(P(AB(AB)|XY)^{\otimes N})-\hat{P}_{\mathrm{ideal}}^{(d_N)}\right]\right\|_1\leqslant\epsilon_N\Rightarrow\left\|\mathcal{P}_N(P(ABE_1E_2|X=x^1,Y=y^1)^{\otimes N})-\tilde{P}_{\mathrm{ideal}}^{(d_N)}\right\|_1\leqslant\epsilon_N, \tag{F12}$$

where $\tilde{P}_{\mathrm{ideal}}^{(d_N)}=\frac{\delta A=a,B=b}{d_N}\sum_{a,b}P(A=a,B=b,E_1E_2|X=x^1,Y=y^1)$. We use now contractivity of the $||.||_1$ norm under stochastic maps, including Ω_E which maps E_1E_2 to AB, to obtain finally (F11) with $P_{\mathrm{ideal}}^{(d_N)}=\frac{\delta(A=a,B=b)}{d_N}P(AB)$. Now $P(AB(AB)|X=x^1,Y=y^1)^{\otimes N}$ is a tripartite probability distribution which we denote as $P(AB(AB))^{\otimes N}$. It is an instance of the SKA scenario. We can therefore apply Theorem 4 (with $\delta_N=\epsilon_N$). Indeed, in $\mathcal{P}_N$ we recognize an LOPC operation such that (since ϵ_N can be arbitrarily small) we have

$$S(A:B||(AB))\geqslant\frac{\log_2\dim_A[\mathcal{P}_N(P(AB(AB))^{\otimes N})]}{N}. \tag{F13}$$

Now by Eqs. (F10) and (F8) there is

$$S(AB||(AB))\geqslant\frac{\log_2\dim_A[\mathcal{P}_N(P(AB(AB))^{\otimes N})]}{N}\geqslant\frac{\log_2\dim_A[\Lambda_N(P^{(N)}(ABE_1E_2|XY))]}{N}\geqslant K_D^{\mathrm{RC}}(P(ABE_1E_2|XY))-\eta. \tag{F14}$$

Since η was arbitrary, we can set it to 0, keeping the above inequality true. It is enough to observe now that

$$S(A:B||(AB))_{P(AB(AB))} \leqslant I(A:B\downarrow(AB))_{P(AB(AB))} = 0. \tag{F15}$$

The inequality is thanks to Theorem 5. Equality holds due to the fact that the intrinsic information $I(A:B\downarrow(AB))$ equals 0. Indeed, there is

$$\begin{aligned} I(A:B|(AB)) &= H(A(AB)) + H(B(AB)) - H(AB) - H(AB(AB)) \\ &= H(AAB) + H(BAB) - H(AB) - H(ABAB) = H(AB) + H(BA) - H(AB) - H(AB) = 0, \end{aligned} \tag{F16}$$

and so $I(A:B\downarrow AB) = \inf_{\kappa:AB\to E'} I(A:B|E') = 0$, as the infimum is achieved for κ being an identity operation. From Eq. (F14), and Eq. (F15), we conclude that

$$K_D^{\mathrm{RC}}(P(ABE_1E_2|XY)) \leqslant S(A:B||(AB)) \leqslant 0. \tag{F17}$$

By definition $K_D^{\mathrm{RC}} \geqslant 0$ as the rate 0 is achieved for a protocol which traces out the input yielding output with $d_N = 1$. Hence the assertion follows from the above inequality. ■

In the above proof we have considered $M = 2$ of the honest parties. We argue now that analogous result holds for the conference key obtained by the $M > 2$ parties, secure against RC adversaries. First, the analog of a technical Theorem 4 of [19] is straightforward. Then, the proof of an analog of Theorem 6 goes along similar lines to those for $M = 2$, with a modification in Eq. (F15). There we base the discussion on the following analog of Theorem 5 shown in [37] (see Theorem 4, and Example 2 there):

$$S(B_1:B_2:\ldots:B_M||E)_{P(B_1,\ldots,B_ME)} \leqslant \frac{1}{(M-1)} I(B_1:B_2:\ldots:B_M\downarrow E)_{P(B_1,\ldots,B_ME)}, \tag{F18}$$

for any $M+1$-partite device $P(B_1,\ldots,B_ME)$, where $S(B_1:B_2:\ldots:B_M||E)$ denotes the so called *conference key*, while $I(B_1:B_2:\ldots:B_M\downarrow E) = \sum_{i=1}^{M} H(B_i,E) - H(B_1,\ldots,B_M,E) - (M-1)H(E)$. The fact that $I(B_1,\ldots,B_M\downarrow E)$ equals zero for $E = (AB)$ can be checked by direct inspection.

APPENDIX G: DIMENSIONALITY OF THE RC POLYTOPE

In this Appendix we compute the dimensionality $\mathcal{D}[\ldots]$ of the polytope of RC correlations in the three-party m inputs, n outputs $(3, m, n)$ scenario. We proceed with our calculation in three steps: (1) begin with the general set of constraints and divide them into appropriate subsets, (2) compute in detail the dimensionality of the (3,2,2) scenario (i.e., $\mathcal{D}[RC(3,2,2)]$), and (3) reproduce computation in step 2 for the general scenario of $(3, m, n)$ with the corresponding alterations.

Step 1: General setting

The general setting corresponds to the 3-party, m inputs, n outputs $(3, m, n)$ scenario with correlations satisfying the following constraints:

$$P(a,b,c|x,y,z) \in [0,1] \quad \forall_{x,y,z,a,b,c}, \tag{G1}$$

$$\sum_{a,b,c} P(a,b,c|x,y,z) = 1 \qquad \forall_{x,y,z}, \tag{G2}$$

$$P(b,c|y,z) = \sum_a P(a,b,c|x,y,z) = \sum_a P(a,b,c|x',y,z) \quad \forall_{x,x',y,z,b,c}, \tag{G3}$$

$$P(a,b|x,y) = \sum_c P(a,b,c|x,y,z) = \sum_c P(a,b,c|x,y,z') \quad \forall_{z,z',x,y,a,b}, \tag{G4}$$

$$P(a|x) = \sum_{b,c} P(a,b,c|x,y,z) = \sum_{b,c} P(a,b,c|x,y',z')\ \forall_{y,y',z,z',x,a}, \tag{G5}$$

$$P(c|z) = \sum_{a,b} P(a,b,c|x,y,z) = \sum_{a,b} P(a,b,c|x',y',z)\ \forall_{x,x',y,y',z,c}. \tag{G6}$$

We divide the equalities (G2)–(G6) into three sets of constraints $\mathcal{N} = \{(G2)\}$, $\mathcal{P} = \{(G3), (G4)\}$, and $\mathcal{RC} = \{(G5), (G6)\}$. The cardinalities of these sets, for any m, n, are given by

$$|\mathcal{N}| = m^3, \tag{G7}$$

$$|\mathcal{P}| = 2m^2n^2(m-1), \tag{G8}$$

$$|\mathcal{RC}| = 2mn(mn-1), \tag{G9}$$

and together fully describe the $(3, m, n)$ RC polytope.

Since the set of normalization constraints $\mathcal{N}$ involves mutually independent equalities we consider them—without loss of generality—as independent and describe the dependencies of equations in other sets with respect to them.

Step 2: Computing $\mathcal{D}[RC(3, 2, 2)]$

Here we discuss in detail mutual dependencies between equalities in and between the sets $\mathcal{N}$, $\mathcal{P}$, and $\mathcal{RC}$ for the (3,2,2) scenario. We begin by writing explicitly all equations of $\mathcal{P}$ and $\mathcal{RC}$ in the form of tables:

$\mathcal{P}$	$c1$		$c2$	$c3$		$c4$
	Q1			**Q5**		
$r1$	$\sum_a P(a00\|000)$	$=$	$\sum_a P(a00\|100)$	$\sum_c P(00c\|000)$	$=$	$\sum_c P(00c\|001)$
$r2$	$\sum_a P(a01\|000)$	$=$	$\sum_a P(a01\|100)$	$\sum_c P(01c\|000)$	$=$	$\sum_c P(01c\|001)$
$r3$	$\sum_a P(a10\|000)$	$=$	$\sum_a P(a10\|100)$	$\sum_c P(10c\|000)$	$=$	$\sum_c P(10c\|001)$
$r4$	$\sum_a P(a11\|000)$	$=$	$\sum_a P(a11\|100)$	$\sum_c P(11c\|000)$	$=$	$\sum_c P(11c\|001)$
	Q2			**Q6**		
$r5$	$\sum_a P(a00\|001)$	$=$	$\sum_a P(a00\|101)$	$\sum_c P(00c\|010)$	$=$	$\sum_c P(00c\|011)$
$r6$	$\sum_a P(a01\|001)$	$=$	$\sum_a P(a01\|101)$	$\sum_c P(01c\|010)$	$=$	$\sum_c P(01c\|011)$
$r7$	$\sum_a P(a10\|001)$	$=$	$\sum_a P(a10\|101)$	$\sum_c P(10c\|010)$	$=$	$\sum_c P(10c\|011)$
$r8$	$\sum_a P(a11\|001)$	$=$	$\sum_a P(a11\|101)$	$\sum_c P(11c\|010)$	$=$	$\sum_c P(11c\|011)$
	Q3			**Q7**		
$r9$	$\sum_a P(a00\|010)$	$=$	$\sum_a P(a00\|110)$	$\sum_c P(00c\|100)$	$=$	$\sum_c P(00c\|101)$
$r10$	$\sum_a P(a01\|010)$	$=$	$\sum_a P(a01\|110)$	$\sum_c P(01c\|100)$	$=$	$\sum_c P(01c\|101)$
$r11$	$\sum_a P(a10\|010)$	$=$	$\sum_a P(a10\|110)$	$\sum_c P(10c\|100)$	$=$	$\sum_c P(10c\|101)$
$r12$	$\sum_a P(a11\|010)$	$=$	$\sum_a P(a11\|110)$	$\sum_c P(11c\|100)$	$=$	$\sum_c P(11c\|101)$
	Q4			**Q8**		
$r13$	$\sum_a P(a00\|011)$	$=$	$\sum_a P(a00\|111)$	$\sum_c P(00c\|110)$	$=$	$\sum_c P(00c\|111)$
$r14$	$\sum_a P(a01\|011)$	$=$	$\sum_a P(a01\|111)$	$\sum_c P(01c\|110)$	$=$	$\sum_c P(01c\|111)$
$r15$	$\sum_a P(a10\|011)$	$=$	$\sum_a P(a10\|111)$	$\sum_c P(10c\|110)$	$=$	$\sum_c P(10c\|111)$
$r16$	$\sum_a P(a11\|011)$	$=$	$\sum_a P(a11\|111)$	$\sum_c P(11c\|110)$	$=$	$\sum_c P(11c\|111)$

$\mathcal{RC}$	$c1$		$c2$	$c3$		$c4$
	Q1			**Q5**		
$r1$	$\sum_{a,b} P(ab0\|000)$	$=$	$\sum_{a,b} P(ab0\|010)$	$\sum_{b,c} P(0bc\|000)$	$=$	$\sum_{b,c} P(0bc\|001)$
$r2$		$=$	$\sum_{a,b} P(ab0\|100)$		$=$	$\sum_{b,c} P(0bc\|010)$
$r3$		$=$	$\sum_{a,b} P(ab0\|110)$		$=$	$\sum_{b,c} P(0bc\|011)$
	Q2			**Q6**		
$r4$	$\sum_{a,b} P(ab1\|000)$	$=$	$\sum_{a,b} P(ab1\|010)$	$\sum_{b,c} P(1bc\|000)$	$=$	$\sum_{b,c} P(1bc\|001)$
$r5$		$=$	$\sum_{a,b} P(ab1\|100)$		$=$	$\sum_{b,c} P(1bc\|010)$
$r6$		$=$	$\sum_{a,b} P(ab1\|110)$		$=$	$\sum_{b,c} P(1bc\|011)$
	Q3			**Q7**		
$r7$	$\sum_{a,b} P(ab0\|001)$	$=$	$\sum_{a,b} P(ab0\|011)$	$\sum_{b,c} P(0bc\|100)$	$=$	$\sum_{b,c} P(0bc\|101)$
$r8$		$=$	$\sum_{a,b} P(ab0\|101)$		$=$	$\sum_{b,c} P(0bc\|110)$
$r9$		$=$	$\sum_{a,b} P(ab0\|111)$		$=$	$\sum_{b,c} P(0bc\|111)$
	Q4			**Q8**		
$r10$	$\sum_{a,b} P(ab1\|001)$	$=$	$\sum_{a,b} P(ab1\|011)$	$\sum_{b,c} P(1bc\|100)$	$=$	$\sum_{b,c} P(1bc\|101)$
$r11$		$=$	$\sum_{a,b} P(ab1\|101)$		$=$	$\sum_{b,c} P(1bc\|110)$
$r12$		$=$	$\sum_{a,b} P(ab1\|111)$		$=$	$\sum_{b,c} P(1bc\|111)$

We use this table as a means to refer to its elements (terms of sums of probabilities) using rows and columns [e.g., $\sum_{a,b} P(ab0|010) \equiv \mathcal{RC}(1, 2)$] and to define sub-tables referred to as sectors [e.g., $\mathcal{P}(\mathbf{Q1})$ or $\mathcal{RC}(\mathbf{Q2})$].

Consider $\mathcal{P}$. In each sector $\mathcal{P}(\mathbf{Qi})$, $i \in \{1, \ldots, 8\}$, the last equality is implied by the previous ones and one of 8 normalization conditions in $\mathcal{N}$, which gives 8 dependent equalities. There are two more redundant conditions that can be found by writing two sequences of equalities that begin and end with the same sum of probabilities, but with different rows or columns in the tables above. In sectors $\{\mathcal{P}(\mathbf{Q1}), \mathcal{P}(\mathbf{Q2}), \mathcal{P}(\mathbf{Q5}), \mathcal{P}(\mathbf{Q7})\}$ and $\{\mathcal{P}(\mathbf{Q3}), \mathcal{P}(\mathbf{Q4}), \mathcal{P}(\mathbf{Q6}), \mathcal{P}(\mathbf{Q8})\}$ we identify the corresponding two sequences (G10) and (G11), respectively. We designate these kind of sequences as *closed paths*:

$$\begin{aligned} \mathcal{P}(1,2)+\mathcal{P}(2,2) &= \mathcal{P}(1,1)+\mathcal{P}(2,1) = \mathcal{P}(1,3)+\mathcal{P}(3,3) = \mathcal{P}(1,4)+\mathcal{P}(3,4) \\ &= \mathcal{P}(5,1)+\mathcal{P}(6,1) = \mathcal{P}(5,2)+\mathcal{P}(6,2) = \mathcal{P}(9,4)+\mathcal{P}(11,4) \\ &= \mathcal{P}(9,3)+\mathcal{P}(11,3), \end{aligned} \tag{G10}$$

$$\begin{aligned}\mathcal{P}(9,2)+\mathcal{P}(10,2) &= \mathcal{P}(9,1)+\mathcal{P}(10,1) = \mathcal{P}(5,3)+\mathcal{P}(7,3) = \mathcal{P}(5,4)+\mathcal{P}(7,4)\\ &= \mathcal{P}(13,1)+\mathcal{P}(14,1) = \mathcal{P}(13,2)+\mathcal{P}(14,2) = \mathcal{P}(13,4)+\mathcal{P}(15,4)\\ &= \mathcal{P}(13,3)+\mathcal{P}(15,3),\end{aligned} \tag{G11}$$

$$\begin{aligned}\textstyle\sum_{ac} P(a0c|100) &= \textstyle\sum_a P(a00|100)+\sum_a P(a01|100) = \mathcal{P}(1,2)+\mathcal{P}(2,2)\\ &= \cdots = \mathcal{P}(9,3)+\mathcal{P}(11,3)\\ &= \textstyle\sum_c P(00c|100)+\sum_c P(10c|100) = \sum_{ac} P(a0c|100),\end{aligned} \tag{G12}$$

$$\begin{aligned}\textstyle\sum_{ac} P(a0c|110) &= \textstyle\sum_a P(a00|110)+\sum_a P(a01|110) = \mathcal{P}(9,2)+\mathcal{P}(10,2)\\ &= \cdots = \mathcal{P}(13,3)+\mathcal{P}(15,3)\\ &= \textstyle\sum_c P(00c|110)+\sum_c P(10c|110) = \sum_{ac} P(a0c|110).\end{aligned} \tag{G13}$$

Notice that the first and last terms in each pair ((G10), (G11)) and ((G12), (G13)) describe the same values.

From this observation, it follows that one equality is dependent in $\{\mathcal{P}(\mathbf{Q1}), \mathcal{P}(\mathbf{Q2}), \mathcal{P}(\mathbf{Q5}), \mathcal{P}(\mathbf{Q7})\}$ and similarly one in $\{\mathcal{P}(\mathbf{Q3}), \mathcal{P}(\mathbf{Q4}), \mathcal{P}(\mathbf{Q6}), \mathcal{P}(\mathbf{Q8})\}$. This, for the first case, can be schematically represented as

$$\left(\left\{\begin{array}{c}\mathcal{P}(1,1)=\mathcal{P}(1,2)\\ \mathcal{P}(2,1)=\mathcal{P}(2,2)\\ \mathcal{P}(9,3)=\mathcal{P}(9,4)\\ \mathcal{P}(11,3)=\mathcal{P}(11,4)\end{array}\right\}+\{\mathcal{P}(1,2)+\mathcal{P}(2,2)=\mathcal{P}(9,3)+\mathcal{P}(11,3)\}\right)$$

$$\Downarrow$$

$$\left(\left\{\begin{array}{c}\mathcal{P}(1,2)+\mathcal{P}(2,2)=\mathcal{P}(9,3)+\mathcal{P}(11,3)\\ \mathcal{P}(2,1)=\mathcal{P}(2,2)\\ \mathcal{P}(9,3)=\mathcal{P}(9,4)\\ \mathcal{P}(11,3)=\mathcal{P}(11,4)\end{array}\right\}\Rightarrow\{\mathcal{P}(1,1)=\mathcal{P}(1,2)\}\right).$$

For the second case an analogous reasoning shows the redundancy of one equation. Closed paths (G10) and (G11) are the shortest possible paths in $\mathcal{P}$ so there are no more dependent equalities leaving in total $8+22$ independent conditions for the set of constraints $\mathcal{N}\cup\mathcal{P}$.

Now, consider the full set of RC constraints $\mathcal{N}\cup\mathcal{P}\cup\mathcal{RC}$. Due to the normalization conditions, it follows that each sector $\mathcal{RC}(\mathbf{Qi}+1)$, $i\in 1,3,5,7$, is implied by $\mathcal{RC}(\mathbf{Qi})$ giving 12 dependent conditions. Furthermore in each of the remaining sectors of $\mathcal{RC}$ two out of three equalities are implied by $\mathcal{P}$. As an example consider sector $\mathcal{RC}(\mathbf{Q1})$, then write

$$\mathcal{RC}(1,1)=\mathcal{RC}(2,2)\Leftrightarrow\mathcal{P}(1,1)+\mathcal{P}(3,1)=\mathcal{P}(1,2)+\mathcal{P}(3,2), \tag{G14}$$

$$\mathcal{RC}(1,2)=\mathcal{RC}(3,2)\Leftrightarrow\mathcal{P}(9,1)+\mathcal{P}(11,1)=\mathcal{P}(9,2)+\mathcal{P}(11,2). \tag{G15}$$

In other words two out of three equalities is sector $\mathcal{RC}(\mathbf{Q1})$ are implied by sectors $\mathcal{P}(\mathbf{Q1})$ and $\mathcal{P}(\mathbf{Q3})$. Analogously sectors $\{\mathcal{P}(\mathbf{Q2}), \mathcal{P}(\mathbf{Q4})\}$, $\{\mathcal{P}(\mathbf{Q5}), \mathcal{P}(\mathbf{Q6})\}$, and $\{\mathcal{P}(\mathbf{Q7}), \mathcal{P}(\mathbf{Q8})\}$ leave only one independent equation in sectors $\mathcal{RC}(\mathbf{Q3})$, $\mathcal{RC}(\mathbf{Q5})$, and $\mathcal{RC}(\mathbf{Q7})$, respectively. In summary, the RC (3,2,2) polytope is fully described by 34 independent conditions so its dimensionality is $\mathcal{D}[RC(3,2,2)]=64-34=30$.

Step 3: Computing $\mathcal{D}[RC(3,m,n)]$

We now proceed to compute the dimensionality of the RC polytope in the general $(3,m,n)$ scenario. Like in step 2, we first consider the set $\mathcal{P}$. Notice that using normalization conditions we can delete $2(m-1)$ equations in each of the $2m^2$ sectors $\mathcal{P}(\mathbf{Q})$. To construct closed paths between sectors one needs probabilities that for a given input and output of Bob, sum over all outputs of Alice and Charlie. This, due to normalization that removes, e.g., the last row in each sector, can be done uniquely for $n-1$ outputs and m inputs of Bob for any choice of $(m-1)^2$ combinations of columns for Alice and Charlie. This, in total, gives $2m^2(m-1)+(n-1)m(m-1)^2$ dependent equalities and by Eq. (G8), $2m^2n^2(m-1)+m^2n(2-m)+m(1-n)$ independent equalities.

For the set $\mathcal{N}\cup\mathcal{P}\cup\mathcal{RC}$ normalization conditions together with sectors $\{\mathcal{RC}(\mathbf{Qi}),\ldots,\mathcal{RC}(\mathbf{Qi}+\mathbf{m}-\mathbf{1})\}$ imply sector $\mathcal{RC}(\mathbf{Qi}+\mathbf{m})$ for $i\in\{l\cdot m\}$ with $l=\{0,1,\ldots,2*(m-1)\}$ leaving $2(n-1)m$ sectors. By a similar argument to that in the (3,2,2) scenario, in each remaining sector $\mathcal{RC}(\mathbf{Q})$ constraints in $\mathcal{P}$ imply all sums of probabilities with the same input of Bob leaving only $m-1$ equations. This gives $2(n-1)m(m-1)$ independent equalities. Subtracting the total number of independent conditions from $(m\cdot n)^3$ gives the dimensionality of RC polytope in the $(3,m,n)$ scenario as

$$\mathcal{D}[RC(3,m,n)]=[m(n-1)+1]^3+m^2(m-1)(n-1)^2-1. \tag{G16}$$

APPENDIX H: NONTRIVIAL BOUNDS FOR RELATIVISTIC CAUSAL CORRELATIONS

The main contribution of our article is the proof that two eavesdroppers can collaborate to break any device-independent security protocol if they can prepare devices with the strongest correlations allowed by RC theories. The natural assumption that the eavesdroppers can choose freely spacetime positions is shown here to be relevant for the proof of the no-go theorem. The reason is because eavesdroppers must choose necessarily appropriate positions for the measuring devices to reach the strongest correlations allowed by RC. In this Appendix we show how a restriction in the spacetime positions of the eavesdroppers could limit the device correlations even below the strength of quantum correlations, demonstrating that the selection of the spacetime positions is crucial for the attack of the eavesdroppers.

We first study trade-off relations between three-party Svetlichny expressions $\langle\mathcal{I}\rangle_{ACD}$, $\langle\mathcal{I}\rangle_{BCD}$ of the form

$$\langle\mathcal{I}\rangle_{ACD} + \langle\mathcal{I}\rangle_{BCD} \leqslant 2\mathcal{B}, \tag{H1}$$

where $\mathcal{B}$ is the so-called "broadcast" bound. We remark that the distinguishing feature of RC correlations is the point-to-region (PTR) signaling, described in detail in Appendix B, namely that in certain measurement configurations, a single party can signal to a region thus influencing the correlations between two or more other parties.

Consider a three-party situation with measurement inputs x, y, z and outputs a, b, c for Alice, Bob, and Charlie, respectively. Broadcasting correlations represent the situation when one party sends all the information about its measurement setting and outcome to the other two parties. In [41,42], it was pointed out that quantum correlations violate broadcasting correlations and this can be regarded as an alternative notion of genuine multipartite nonlocality. Tripartite broadcasting correlations $P(a, b, c|x, y, z)$ are defined as follows:

$$\begin{aligned} P(a, b, c|x, y, z) = &\sum_{\lambda_1} q(\lambda_1)P(a|x, \lambda_1)P(b|y, x, a, \lambda_1)P(c|z, x, a, \lambda_1) \\ &+ \sum_{\lambda_2} q(\lambda_2)P(b|y, \lambda_2)P(a|x, y, b, \lambda_2)P(c|z, y, b, \lambda_2) \\ &+ \sum_{\lambda_3} q(\lambda_3)P(c|z, \lambda_3)P(b|y, z, c, \lambda_3)P(a|x, z, c, \lambda_3). \end{aligned} \tag{H2}$$

Observe that in the first term, Bob's output b and Charlie's output c depend upon Alice's input and output x, a, in the case where Alice has broadcast these, and similarly for the other two terms. The following lemma makes a connection between broadcast correlations and relativistic causal (RC) correlations, under the constraint that some of the observables are jointly measurable.

Lemma 1. Any RC tripartite probability distribution can be realized by a broadcast model with the additional condition that all the observables, measured by one party who does not signal PTR, are co-measurable

Proof. Like in Sec. II of the main text, we consider the tripartite spacetime measurement configuration in Fig. 3 where Bob signals PTR (i.e., to the correlations between A and C) so that the RC constraints are given by the set of equations

$$\sum_a P(a, b, c \mid x, y, z) = \sum_a P(a, b, c \mid x', y, z) \quad \forall\, x, x', y, z, b, c, \tag{H3}$$

$$\sum_c P(a, b, c \mid x, y, z) = \sum_c P(a, b, c \mid x, y, z') \quad \forall\, z, z', x, y, a, b, \tag{H4}$$

$$\sum_{b,c} P(a, b, c \mid x, y, z) = \sum_{b,c} P(a, b, c \mid x, y', z') \quad \forall\, y, y', z, z', x, a, \tag{H5}$$

$$\sum_{a,b} P(a, b, c \mid x, y, z) = \sum_{a,b} P(a, b, c \mid x', y', z) \quad \forall\, x, x', y, y', z, c. \tag{H6}$$

From the first two conditions, we also clearly have,

$$\sum_{a,c} P(a, b, c|x, y, z) = \sum_{a,c} P(a, b, c|x', y, z'). \tag{H7}$$

This implies that $P(b|x, y, z) = P(b|y)$ is independent of x, z. Now, any RC tripartite probability distribution can be written as

$$P(a, b, c|x, y, z) = P(a, c|x, y, z, b)P(b|x, y, z) = P(a, c|x, y, z, b)P(b|y). \tag{H8}$$

Without loss of generality let us say that all the observables x measured by Alice are co-measurable. Also, let us remember some useful concepts: a *commutation graph* is a graph with vertices representing observables, edges connecting observables that are jointly measurable, and a *chordal graph* is a graph in which all cycles of four or more vertices have a chord going through them.

In our case we can define a commutation graph of all the observables measured by Alice and Charlie conditioned on a particular pair of Bob's observable and outcome y, b. In the commutation graph, all pairs x, x' and x, z are connected, so that this commutation graph is chordal. For chordal graphs of measurements there corresponds an expression for which a joint probability distribution exists and which is hence classical [43]. Therefore there exists an overall joint probability distribution of

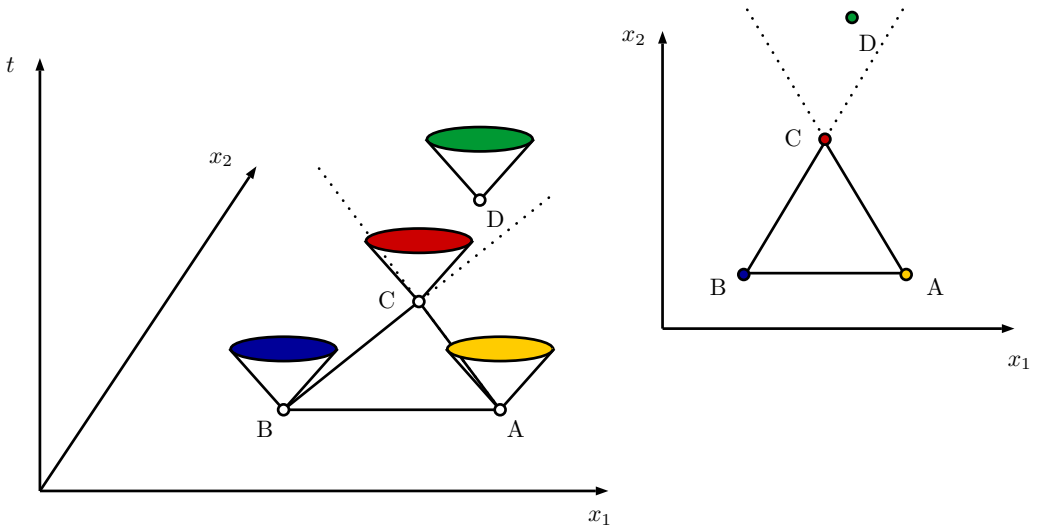

FIG. 4. Two perspectives of four parties A, B, C, D in a (2+1)-dimensional spacetime. The four parties make a simultaneous measurement in the particular reference frame of the picture. The measurement events of parties A, B, C form a triangle and party D is in some location inside the region defined by line BC and line AC (Dave's region). The correlations then satisfy a tight monogamy relation for any broadcast inequality, for instance Svetlichny's inequality [41]: $\langle \mathcal{I}_{Sve} \rangle_{ACD} + \langle \mathcal{I}_{Sve} \rangle_{BCD} \overset{RC}{\leqslant} 8$.

all x, z conditioned on y, b. By Fine's theorem [44] we conclude that $P(a, c|x, y, z, b) = P(a|x, y, b)P(c|y, z, b)$. Thus,

$$P(a, b, c|x, y, z) = P(a|x, y, b)P(c|y, z, b)P(b|y), \tag{H9}$$

which is a particular form of the broadcast correlations given in (H2) in which $q(\lambda_1) = q(\lambda_3) = 0$ and λ_2 is unique. ■

Second, we consider the Bell scenario involving four spatially separated parties Alice (A), Bob (B), Charlie (C), and Dave (D). Consider any broadcasting inequality $\langle \mathcal{I} \rangle_{ACD}$ between Alice, Charlie, and Dave in which Alice has two measurement settings $x = 0, 1$. Assume now that $x = 0, 1$ are co-measurable; then by Lemma 2,

$$\langle \mathcal{I} \rangle_{ACD} = \langle \mathcal{I} \rangle^{a_0}_{ACD} + \langle \mathcal{I} \rangle^{a_1}_{ACD} \leqslant \mathcal{B}, \tag{H10}$$

where $\mathcal{B}$ is the upper bound on broadcasting correlations (H2), and $\langle \mathcal{I} \rangle^{a_0}_{ACD}$, $\langle \mathcal{I} \rangle^{a_1}_{ACD}$ are the expressions corresponding to $x = 0, 1$ respectively.

Proposition 3. In the four-party scenario if the following two conditions hold,

(1) A and B do not signal PTR, and

(2) any observable measured by A and any observables measured by B are nondisturbing (or alternatively no party signals PTR such that it affects the correlations between A and B),

then the monogamy relation,

$$\langle \mathcal{I} \rangle_{ACD} + \langle \mathcal{I} \rangle_{BCD} \leqslant 2\mathcal{B}, \tag{H11}$$

is satisfied in all theories obeying relativistic causality.

Proof. The expression of interest can be written as

$$\langle \mathcal{I} \rangle_{ACD} + \langle \mathcal{I} \rangle_{BCD} = \left(\langle \mathcal{I} \rangle^{a_0}_{ACD} + \langle \mathcal{I} \rangle^{b_1}_{BCD} \right) + \left(\langle \mathcal{I} \rangle^{b_0}_{BCD} + \langle \mathcal{I} \rangle^{a_1}_{ACD} \right). \tag{H12}$$

The terms within each bracket can be interpreted as the same inequality $\mathcal{I}$ in which the first party measures $x = 0, y = 1$ and the second measures $x = 1, y = 0$. Now, any two observables measured by Alice and Bob are nondisturbing and jointly measurable since no other party signals PTR to influence the correlations between them. Moreover, both the parties do not signal PTR to affect the correlation of others. Thus, from the above Lemma 2, one concludes that each of the two terms is bounded by its broadcasting value within theories obeying relativistic causality, that is, $\mathcal{B}$. Hence, the whole expression is bounded by $2\mathcal{B}$. ■

An example of a measurement configuration given by the spacetime location of four parties' measurement events is shown in Fig. 4 where the two conditions given in Proposition 3 hold. This example shows that if eavesdroppers are constrained to spacetime positions like those allowed to Dave, their correlations are bounded by broadcast correlations, which are known to be weaker than quantum correlations [42]. This limitation introduced by the restriction on spacetime positions—to Dave's region, for instance—sets aside the attack of eavesdroppers since the reliable parties (Alice, Bob, and Charlie in the example) could perform an experiment with quantum correlations they could not reproduce.

Class	Probability	Condition for RC extremal boxes beyond no-signaling polytope
1	1	$abc(1 \oplus x)(1 \oplus z) == 1$
	$\frac{1}{2}$	$b(cx \oplus (a \oplus xy)z) == 1$
2	1	$abc(1 \oplus x)y(1 \oplus z) == 1$
	$\frac{1}{2}$	$a(c \oplus cy \oplus bz) \oplus bx(c \oplus z \oplus yz) == 1$
3	$\frac{1}{4}$	$(1 \oplus c)xy \oplus b(c \oplus y \oplus yz \oplus xyz) \oplus a(c \oplus y \oplus z \oplus bz \oplus yz \oplus bcxyz) == 1$
	$\frac{3}{4}$	$abcxyz == 1$
	$\frac{1}{2}$	$ab(1 \oplus c \oplus y \oplus z \oplus yz \oplus cxyz) == 1$
4	$\frac{1}{3}$	$ay(c \oplus z) \oplus b(1 \oplus a \oplus ac \oplus cx \oplus xy \oplus yz \oplus xyz) == 1$
	$\frac{2}{3}$	$bc((1 \oplus x)yz \oplus a(yz \oplus x(1 \oplus y \oplus yz))) == 1$
5	$\frac{1}{5}$	$x \oplus cx \oplus y \oplus cy \oplus yz \oplus xyz \oplus b(c \oplus x \oplus cx \oplus y \oplus z \oplus xyz) \oplus a(1 \oplus c \oplus yz \oplus b(1 \oplus cy \oplus z)) == 1$
	$\frac{4}{5}$	$abc(1 \oplus x)y(1 \oplus z) == 1$
	$\frac{2}{5}$	$by(cx \oplus az) == 1$
	$\frac{3}{5}$	$abc(1 \oplus y) == 1$
6	$\frac{1}{3}$	$(1 \oplus c)xy \oplus a(1 \oplus c \oplus bc \oplus bz) \oplus b(c \oplus y \oplus yz \oplus xyz) == 1$
	$\frac{2}{3}$	$abcxyz == 1$
7	$\frac{1}{4}$	$x(c \oplus y) \oplus b(c \oplus y \oplus z \oplus xz) \oplus a(c \oplus y \oplus bz \oplus bcxyz) == 1$
	$\frac{3}{4}$	$abcxyz == 1$
	$\frac{1}{2}$	$ab(1 \oplus c \oplus y \oplus z \oplus yz \oplus cxyz) == 1$
8	$\frac{1}{4}$	$cx \oplus y \oplus cy \oplus xy \oplus xz \oplus xyz \oplus b(c \oplus y \oplus xz) \oplus a(y \oplus z \oplus bz \oplus yz \oplus c(1 \oplus b(x \oplus y)z)) == 1$
	$\frac{3}{4}$	$abc(x \oplus y)z == 1$
	$\frac{1}{2}$	$ab(1 \oplus c \oplus y \oplus z \oplus cxz \oplus yz \oplus cyz) == 1$
9	$\frac{1}{3}$	$xy(c \oplus z) \oplus b(c \oplus x \oplus xy \oplus z \oplus yz \oplus xyz) \oplus a(b(1 \oplus c) \oplus y(c \oplus z)) == 1$
	$\frac{2}{3}$	$abc(x \oplus xy \oplus z \oplus yz \oplus xyz) == 1$
10	$\frac{1}{3}$	$x(c \oplus y \oplus z) \oplus a(b \oplus c \oplus bc \oplus y \oplus z) \oplus b(c \oplus yz \oplus x(y \oplus z \oplus yz)) == 1$
	$\frac{2}{3}$	$abcx(y \oplus z) == 1$
11	$\frac{1}{3}$	$cxy \oplus a(y \oplus z) \oplus b(1 \oplus a \oplus c \oplus ac \oplus y \oplus z \oplus xyz) == 1$
	$\frac{2}{3}$	$a(1 \oplus b)c(1 \oplus y \oplus z \oplus xyz) == 1$
12	$\frac{1}{4}$	$(a \oplus x)y(c \oplus z) \oplus b(1 \oplus a \oplus cx \oplus y \oplus xz \oplus acxyz) == 1$
	$\frac{3}{4}$	$abcxyz == 1$
	$\frac{1}{2}$	$bc(1 \oplus x)y \oplus ac(1 \oplus b \oplus y \oplus bxyz) == 1$
13	$\frac{1}{3}$	$cx(1 \oplus y) \oplus a(c \oplus yz) \oplus b(1 \oplus a(1 \oplus c) \oplus yz \oplus x(1 \oplus y)(1 \oplus z)) == 1$
	$\frac{2}{3}$	$(1 \oplus a)bcyz == 1$
14	$\frac{1}{3}$	$xy(c \oplus z) \oplus a(b \oplus c \oplus bc \oplus yz) \oplus b(c \oplus x \oplus xy \oplus z \oplus yz \oplus xyz) == 1$
	$\frac{2}{3}$	$abcxyz == 1$
15	$\frac{1}{3}$	$y \oplus cy \oplus b(c \oplus y \oplus xz \oplus xyz) \oplus a(1 \oplus c \oplus b(1 \oplus c \oplus z)) == 1$
	$\frac{2}{3}$	$abcy(1 \oplus z) == 1$
16	$\frac{1}{4}$	$(a \oplus x)y(c \oplus z) \oplus b(1 \oplus a \oplus y \oplus acxyz \oplus x(1 \oplus c \oplus y \oplus yz)) == 1$
	$\frac{3}{4}$	$abcxyz == 1$
	$\frac{1}{2}$	$bc(1 \oplus x)y \oplus ac(1 \oplus b \oplus y \oplus bxyz) == 1$
17	$\frac{1}{5}$	$b(c \oplus x \oplus cx \oplus y \oplus z \oplus xyz \oplus a(1 \oplus cy \oplus z)) == 1$
	$\frac{4}{5}$	$a(1 \oplus b)c(1 \oplus x)y(1 \oplus z) == 1$
	$\frac{2}{5}$	$ayz \oplus b(ay \oplus (1 \oplus a)x(1 \oplus y))z \oplus cx((1 \oplus a)bz \oplus y(1 \oplus b \oplus bz \oplus abz)) == 1$
	$\frac{3}{5}$	$a(1 \oplus b)c(1 \oplus y) == 1$
18	$\frac{1}{3}$	$(1 \oplus c)xy \oplus a(1 \oplus c \oplus bc \oplus z \oplus bz \oplus yz) \oplus b(c \oplus y \oplus yz \oplus xyz) == 1$
	$\frac{2}{3}$	$abcxyz == 1$
19	$\frac{3}{5}$	$(1 \oplus a)bc(1 \oplus y) == 1$
	$\frac{2}{5}$	$(1 \oplus b)y(1 \oplus c \oplus z) \oplus a(1 \oplus c \oplus yz \oplus b(1 \oplus c \oplus cxy \oplus yz \oplus cxyz)) == 1$
	$\frac{1}{5}$	$y((b \oplus x)(c \oplus z) \oplus a(c \oplus bc \oplus z)) == 1$

(*Continued*.)

Class	Probability	Condition for RC extremal boxes beyond no-signaling polytope
20	$\frac{1}{2}$	$(bc \oplus a(1 \oplus b \oplus c))(1 \oplus y) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus x(c \oplus z)) == 1$
21	$\frac{1}{2}$	$(ac \oplus b(1 \oplus a \oplus c))(1 \oplus y) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus cx \oplus bxz) == 1$
22	$\frac{1}{2}$	$b(c \oplus cy \oplus xyz \oplus cxyz) \oplus a(1 \oplus c \oplus y \oplus cy \oplus cxyz \oplus b(1 \oplus y \oplus xyz)) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus c \oplus cx \oplus az \oplus bxz) == 1$
23	$\frac{1}{2}$	$b(1 \oplus c)xy \oplus a(cxy(1 \oplus z) \oplus b(1 \oplus c \oplus cxy \oplus cxyz)) == 1$
	$\frac{1}{4}$	$c(x \oplus y) \oplus b(c \oplus cx \oplus z \oplus yz) \oplus a(c(1 \oplus y) \oplus (b \oplus y)z) == 1$
24	$\frac{1}{2}$	$(1 \oplus b)(1 \oplus c)xy \oplus a(1 \oplus c \oplus b(1 \oplus c \oplus cxy \oplus cxyz)) == 1$
	$\frac{1}{4}$	$cx(1 \oplus y) \oplus a(c \oplus cy \oplus bz) \oplus b(c \oplus cx \oplus z \oplus yz) == 1$
25	$\frac{1}{2}$	$xy \oplus cxy \oplus bx(c \oplus y \oplus cz \oplus cyz) \oplus a(1 \oplus c \oplus b(1 \oplus c \oplus cx \oplus cxz)) == 1$
	$\frac{1}{4}$	$b(c(1 \oplus x) \oplus (a \oplus x \oplus y)z) == 1$
26	$\frac{1}{4}$	$cxy \oplus b(1 \oplus c \oplus y \oplus a(1 \oplus c \oplus cy)) \oplus ay(1 \oplus z) == 1$
	$\frac{3}{4}$	$a(1 \oplus b)c(1 \oplus y) == 1$
	$\frac{1}{2}$	$acy((1 \oplus x)z \oplus b(x \oplus z)) == 1$
27	$\frac{1}{3}$	$xy(c \oplus z) \oplus a(b \oplus c \oplus bc \oplus z) \oplus b(c \oplus y(1 \oplus x \oplus z)) == 1$
	$\frac{2}{3}$	$abcxyz == 1$
28	$\frac{1}{4}$	$y \oplus cy \oplus a(1 \oplus c \oplus bz \oplus bcxyz) \oplus b(yz \oplus x(1 \oplus c \oplus z)) == 1$
	$\frac{3}{4}$	$abcxyz == 1$
	$\frac{1}{2}$	$bc(1 \oplus a \oplus x \oplus y \oplus xy \oplus axyz) == 1$
29	$\frac{1}{3}$	$a(1 \oplus b \oplus c \oplus bc \oplus y) \oplus y(b \oplus cx \oplus bxz) == 1$
	$\frac{2}{3}$	$(1 \oplus a)bc(1 \oplus y) == 1$
30	$\frac{1}{3}$	$xy(c \oplus z) \oplus a(b \oplus c \oplus bc \oplus z) \oplus b(c \oplus x \oplus y \oplus xz \oplus yz \oplus xyz) == 1$
	$\frac{2}{3}$	$abcxyz == 1$
31	$\frac{1}{4}$	$c \oplus bx \oplus bcx \oplus y \oplus bxy \oplus z \oplus bz \oplus a(1 \oplus c \oplus y \oplus z \oplus bz \oplus bcxyz) == 0$
	$\frac{3}{4}$	$abcxyz == 1$
	$\frac{1}{2}$	$a(by(1 \oplus z) \oplus c(1 \oplus b \oplus y \oplus bxyz)) == 1$
32	$\frac{1}{3}$	$cx(1 \oplus y) \oplus b(c \oplus y) \oplus a(b \oplus c \oplus bc \oplus cy) == 1$
	$\frac{2}{3}$	$a(1 \oplus b)cy == 1$
33	$\frac{1}{3}$	$cx(1 \oplus y) \oplus a(c \oplus yz) \oplus b(1 \oplus a \oplus ac \oplus yz) == 1$
	$\frac{2}{3}$	$(1 \oplus a)bcyz == 1$
34	$\frac{3}{5}$	$a(1 \oplus b)y(c \oplus z) == 1$
	$\frac{2}{5}$	$bx(c \oplus cy \oplus z \oplus yz \oplus cyz) \oplus a(b(1 \oplus y)z \oplus c(1 \oplus y \oplus bxyz)) == 1$
	$\frac{1}{5}$	$b(1 \oplus c \oplus x \oplus cx \oplus y \oplus xyz \oplus a(1 \oplus c \oplus cy \oplus yz)) == 1$
35	$\frac{1}{2}$	$b(1 \oplus x)(c \oplus y \oplus yz \oplus cyz) \oplus a(cy \oplus b(1 \oplus z \oplus cz \oplus x(1 \oplus c \oplus z \oplus cyz))) == 1$
	$\frac{1}{4}$	$b((a \oplus y)z \oplus x(1 \oplus c \oplus acz \oplus acyz)) == 1$
	$\frac{3}{4}$	$abcx(1 \oplus y)z == 1$
36	$\frac{1}{2}$	$(1 \oplus a)cy \oplus b((1 \oplus a \oplus y \oplus axy)z \oplus c(1 \oplus a \oplus ayz \oplus axyz)) == 1$
	$\frac{1}{4}$	$bxy \oplus cx(1 \oplus b \oplus y) \oplus a(b \oplus c \oplus cy \oplus bz) == 1$
37	$\frac{1}{2}$	$b(1 \oplus x)(y \oplus c(1 \oplus z \oplus yz)) \oplus a((1 \oplus c)(1 \oplus y) \oplus b(1 \oplus xyz \oplus c(y \oplus z \oplus yz \oplus x(1 \oplus y \oplus z)))) == 1$
	$\frac{1}{4}$	$c(a \oplus x)y \oplus b((1 \oplus a \oplus y \oplus axy)z \oplus c(x \oplus axyz)) == 1$
	$\frac{3}{4}$	$ab(1 \oplus c)xyz == 1$
38	$\frac{1}{2}$	$bcx(y \oplus z) \oplus a((1 \oplus b \oplus y \oplus bxy)z \oplus c(1 \oplus b \oplus y \oplus bxz)) == 1$
	$\frac{1}{4}$	$a(b \oplus cy \oplus bz) \oplus b(c \oplus x \oplus cx \oplus y \oplus xz \oplus yz \oplus xyz) == 1$
39	$\frac{1}{2}$	$bx(c \oplus y)z \oplus a((1 \oplus b \oplus y)z \oplus c(1 \oplus b \oplus y \oplus bxy \oplus bxz)) == 1$
	$\frac{1}{4}$	$a(b \oplus cy \oplus bz) \oplus b(c(1 \oplus x) \oplus (x \oplus y \oplus xy)(1 \oplus z)) == 1$
40	$\frac{1}{2}$	$c(a \oplus x)y \oplus b((a \oplus x \oplus ay \oplus xy \oplus axy)z \oplus c(a(y \oplus z \oplus yz) \oplus x(1 \oplus a(1 \oplus y \oplus z)))) == 1$
	$\frac{1}{4}$	$a(b \oplus c \oplus cy \oplus bz) \oplus b(1 \oplus x)(c \oplus yz) == 1$

(*Continued*.)

Class	Probability	Condition for RC extremal boxes beyond no-signaling polytope
41	$\frac{1}{2}$	$b(1\oplus x)(c\oplus y\oplus yz)\oplus a(c(1\oplus x)y(1\oplus z)\oplus b(1\oplus z\oplus c(x\oplus z\oplus xyz)))==1$
	$\frac{1}{4}$	$cxy\oplus ayz\oplus b((a\oplus x\oplus xy)z\oplus cx(1\oplus a(1\oplus y)z))==1$
	$\frac{3}{4}$	$abcx(1\oplus y)z==1$
42	$\frac{1}{2}$	$b(1\oplus c)x(1\oplus y)z\oplus a(b(x\oplus y\oplus xy)z\oplus c(1\oplus b\oplus y\oplus bxy\oplus bxz))==1$
	$\frac{1}{4}$	$cxy\oplus a(b\oplus cy\oplus bz)\oplus b(c\oplus x\oplus cx\oplus y\oplus z\oplus xyz)==1$
43	$\frac{1}{2}$	$b(1\oplus x)(c\oplus y\oplus yz\oplus cyz)\oplus a(cy\oplus b((1\oplus xy)(1\oplus z)\oplus c(x\oplus z\oplus xyz)))==1$
	$\frac{1}{4}$	$b((a\oplus y)z\oplus x(y\oplus z\oplus yz)\oplus cx(1\oplus a(1\oplus y)z))==1$
	$\frac{3}{4}$	$abcx(1\oplus y)z==1$
44	$\frac{1}{3}$	$cx\oplus y\oplus cy\oplus xy\oplus xz\oplus yz\oplus a(b\oplus c\oplus bc\oplus y\oplus z)\oplus b(c\oplus xz\oplus y(1\oplus x\oplus z))==1$
	$\frac{2}{3}$	$abc(xz\oplus y(1\oplus x\oplus z))==1$
45	$\frac{1}{3}$	$xy(c\oplus z)\oplus a(1\oplus b\oplus c\oplus bc\oplus y\oplus z)\oplus b(c\oplus y(1\oplus x\oplus z))==1$
	$\frac{2}{3}$	$abcxyz==1$
46	$\frac{1}{3}$	$y(c\oplus z)\oplus a(c\oplus yz)\oplus b(1\oplus a\oplus ac\oplus cx\oplus y\oplus xz\oplus yz\oplus xyz)==1$
	$\frac{2}{3}$	$abcxyz==1$
47	$\frac{1}{2}$	$bcxyz\oplus a(y(c\oplus z)\oplus b(yz\oplus c(1\oplus z\oplus yz\oplus x(1\oplus y\oplus z))))==1$
	$\frac{1}{4}$	$c(1\oplus b\oplus bx\oplus y)\oplus a(1\oplus b\oplus y\oplus bz)\oplus x(by\oplus z\oplus yz\oplus byz)==1$
48	$\frac{1}{2}$	$b(1\oplus c)x(1\oplus y)z\oplus a(bx(1\oplus y)z\oplus c(1\oplus yz\oplus xy(1\oplus z)\oplus b(1\oplus yz\oplus x(y\oplus z))))==1$
	$\frac{1}{4}$	$cxy\oplus a(b\oplus bz\oplus yz)\oplus b(c\oplus x\oplus cx\oplus y\oplus z\oplus xyz)==1$
49	$\frac{1}{2}$	$ac(xz\oplus y(1\oplus x\oplus z))\oplus b(acxz\oplus y((1\oplus x)(1\oplus c\oplus z)\oplus a(1\oplus z\oplus c(x\oplus z))))==1$
	$\frac{1}{4}$	$c(1\oplus x\oplus bx\oplus y)\oplus bx(1\oplus y)z\oplus a(1\oplus y\oplus z\oplus bz)==1$
50	$\frac{1}{2}$	$bc(1\oplus x)yz\oplus a(y(c\oplus z)\oplus b(yz\oplus c(x\oplus y\oplus xy\oplus xz\oplus yz)))==1$
	$\frac{1}{4}$	$by\oplus bxy\oplus c(1\oplus bx\oplus y)\oplus bz\oplus xz\oplus xyz\oplus bxyz\oplus a(1\oplus b\oplus y\oplus bz)==1$
51	$\frac{1}{2}$	$bcxy\oplus a((1\oplus c)xyz\oplus b(xyz\oplus c(1\oplus z\oplus yz\oplus x(1\oplus y\oplus z))))==1$
	$\frac{1}{4}$	$c(1\oplus b\oplus bx\oplus xy)\oplus(1\oplus b\oplus x\oplus bxy)z\oplus a(1\oplus b\oplus bz\oplus yz)==1$
52	$\frac{1}{2}$	$bcx(1\oplus y)z\oplus a((1\oplus b)(1\oplus y)z\oplus c(1\oplus y\oplus b(1\oplus yz\oplus x(y\oplus z))))==1$
	$\frac{1}{4}$	$y\oplus cy\oplus xyz\oplus a(b\oplus y\oplus bz)\oplus b(c(1\oplus x)\oplus y\oplus x(1\oplus y)(1\oplus z))==1$
53	$\frac{1}{3}$	$(1\oplus c)xy\oplus a(1\oplus c\oplus b(1\oplus c\oplus z))\oplus b(c\oplus yz\oplus x(y\oplus z))==1$
	$\frac{2}{3}$	$abcxy(1\oplus z)==1$
54	$\frac{2}{3}$	$ac(1\oplus y\oplus b(1\oplus y\oplus yz\oplus xyz))==1$
	$\frac{1}{3}$	$bx(1\oplus c\oplus y)\oplus a(b(1\oplus c)\oplus y(c\oplus z))==1$
55	$\frac{2}{3}$	$ac(1\oplus y\oplus b(1\oplus y\oplus xyz))==1$
	$\frac{1}{3}$	$(a\oplus x)y(c\oplus z)\oplus b(1\oplus a\oplus c\oplus ac\oplus y\oplus xyz)==1$
56	$\frac{1}{2}$	$c(1\oplus x)y\oplus a(b\oplus cy)\oplus b(c\oplus xy)==1$
57	$\frac{1}{2}$	$bx(c\oplus y)\oplus a(b\oplus cy)==1$
58	$\frac{1}{2}$	$b(c\oplus yz)\oplus a(1\oplus b\oplus c\oplus yz)==1$
59	$\frac{1}{2}$	$bx(1\oplus c\oplus y)\oplus a(b\oplus c\oplus y)==1$
60	$\frac{1}{3}$	$xy(c\oplus z)\oplus a(b\oplus c\oplus bc\oplus yz)\oplus b(c\oplus xyz)==1$
	$\frac{2}{3}$	$abcxyz==1$
61	$\frac{1}{3}$	$ay(c\oplus z)\oplus b(1\oplus a\oplus ac\oplus cx\oplus xy\oplus z\oplus xz)==1$
	$\frac{2}{3}$	$bc((1\oplus x)z\oplus a(z\oplus x(1\oplus y\oplus z)))==1$
62	$\frac{1}{3}$	$x(1\oplus y)(c\oplus z)\oplus a(b(1\oplus c)\oplus(1\oplus y)(c\oplus z))\oplus b(c\oplus yz\oplus x(y\oplus z))==1$
	$\frac{2}{3}$	$abc(yz\oplus x(y\oplus z))==1$
63	$\frac{1}{3}$	$(1\oplus c)xy\oplus a(1\oplus c\oplus bc\oplus z\oplus bz\oplus yz)\oplus b(c\oplus y\oplus xz\oplus yz)==1$
	$\frac{2}{3}$	$abcxyz==1$
64	$\frac{1}{3}$	$xy(c\oplus z)\oplus a(b\oplus c\oplus bc\oplus yz)\oplus b(c\oplus x\oplus xy\oplus z\oplus xz\oplus yz)==1$
	$\frac{2}{3}$	$abcxyz==1$
65	$\frac{1}{3}$	$(a\oplus x)y(c\oplus z)\oplus b(1\oplus a\oplus c\oplus ac\oplus y\oplus xyz)==1$
	$\frac{2}{3}$	$abc(1\oplus y\oplus xyz)==1$

(*Continued*.)

Class	Probability	Condition for RC extremal boxes beyond no-signaling polytope
66	$\frac{1}{3}$	$xy(c \oplus z) \oplus a(b \oplus c \oplus bc \oplus yz) \oplus b(c \oplus x(1 \oplus y \oplus z)) == 1$
	$\frac{2}{3}$	$abcxyz == 1$
67	$\frac{1}{3}$	$(a \oplus x)y(c \oplus z) \oplus b(1 \oplus a \oplus c \oplus ac \oplus y \oplus xz) == 1$
	$\frac{2}{3}$	$abc(1 \oplus y \oplus xz) == 1$
68	$\frac{1}{3}$	$xy(c \oplus z) \oplus b(1 \oplus a \oplus c \oplus ac \oplus y \oplus xz) \oplus a(c \oplus yz) == 1$
	$\frac{2}{3}$	$abcxyz == 1$
69	$\frac{1}{3}$	$(1 \oplus c)xy \oplus a(1 \oplus c \oplus bc \oplus z \oplus bz \oplus yz) \oplus b(c \oplus x \oplus y \oplus xy \oplus xz \oplus yz) == 1$
	$\frac{2}{3}$	$abcxyz == 1$
70	$\frac{1}{2}$	$a(b \oplus c \oplus cy) \oplus bx(1 \oplus c \oplus yz) == 1$
71	$\frac{1}{2}$	$bx(1 \oplus c \oplus yz) \oplus a(b \oplus c \oplus yz) == 1$
72	$\frac{1}{2}$	$bx(c \oplus yz) \oplus a(c \oplus (1 \oplus b \oplus y)z) == 1$
73	$\frac{1}{2}$	$cy \oplus a(b \oplus cy) \oplus b(c \oplus x(1 \oplus y)z) == 1$
74	$\frac{1}{2}$	$a(b \oplus cy) \oplus b(c \oplus y \oplus xz \oplus xyz) == 1$
75	$\frac{1}{2}$	$ac(1 \oplus y) \oplus b(1 \oplus a \oplus c \oplus xy \oplus yz) == 1$
76	$\frac{1}{2}$	$xy(c \oplus z) \oplus a(c \oplus yz) \oplus b(1 \oplus a \oplus c \oplus xy \oplus yz) == 1$
77	$\frac{1}{2}$	$b(c \oplus y) \oplus a(1 \oplus b \oplus c \oplus y) == 1$
78	$\frac{1}{2}$	$b(c \oplus y) \oplus a(b \oplus cy) == 1$
79	$\frac{1}{2}$	$a(cxyz \oplus b(1 \oplus y \oplus xyz)) \oplus b(x(1 \oplus y \oplus z) \oplus c(1 \oplus y \oplus xyz)) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus c \oplus cx \oplus az \oplus bxz) == 1$
80	$\frac{1}{2}$	$b(c \oplus cy \oplus xz \oplus cxyz) \oplus a(cxyz \oplus b(1 \oplus y \oplus xyz)) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus c \oplus cx \oplus az \oplus bxz) == 1$
81	$\frac{1}{2}$	$b(c \oplus cy \oplus xyz \oplus cxyz) \oplus a(cxyz \oplus b(1 \oplus y \oplus xyz)) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus c \oplus cx \oplus az \oplus bxz) == 1$
82	$\frac{1}{3}$	$bx(1 \oplus c \oplus y) \oplus a(b(1 \oplus c) \oplus y(c \oplus z)) == 1$
	$\frac{2}{3}$	$abc(1 \oplus y(1 \oplus z \oplus xz)) == 1$
83	$\frac{1}{2}$	$b(a \oplus c \oplus y(x \oplus z)) == 1$
84	$\frac{1}{2}$	$b(a \oplus c \oplus y \oplus xyz) == 1$
85	$\frac{1}{2}$	$b(a \oplus c \oplus xy \oplus xz \oplus yz) == 1$
86	$\frac{1}{2}$	$b(a \oplus c \oplus (x \oplus y)z) == 1$
87	$\frac{1}{2}$	$b(a \oplus c \oplus yz) == 1$
88	$\frac{1}{2}$	$b(a \oplus c \oplus y \oplus xz) == 1$
89	$\frac{1}{2}$	$b(a \oplus c \oplus y) == 1$
90	$\frac{1}{2}$	$b(a \oplus c \oplus xyz) == 1$
91	$\frac{2}{3}$	$ab(1 \oplus c)(1 \oplus y) == 1$
	$\frac{1}{3}$	$ay(c \oplus z) \oplus b(c \oplus ac \oplus y \oplus xyz) == 1$
92	$\frac{2}{3}$	$abcy == 1$
	$\frac{1}{3}$	$cx(1 \oplus y) \oplus b(c \oplus y) \oplus a(b \oplus c \oplus bc \oplus cy) == 1$
93	$\frac{1}{2}$	$b(a \oplus x(c \oplus yz)) == 1$
94	$\frac{1}{2}$	$b(a \oplus x(c \oplus y)) == 1$
95	$\frac{1}{2}$	$b(1 \oplus y)(a \oplus c \oplus xz) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus cx \oplus bxz) == 1$
96	$\frac{1}{2}$	$b(1 \oplus y)(a \oplus c \oplus xz) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus c \oplus az) == 1$
97	$\frac{1}{2}$	$b(1 \oplus y)(a \oplus c \oplus xz) == 1$
	$\frac{1}{4}$	$y(1 \oplus b \oplus c \oplus az \oplus bxz) == 1$
98	$\frac{1}{2}$	$b(1 \oplus y)(a \oplus c \oplus xz) == 1$
	$\frac{1}{4}$	$(a \oplus b \oplus cx)y == 1$

(*Continued*.)

Class	Probability	Condition for RC extremal boxes beyond no-signaling polytope
99	$\frac{2}{3}$	$abcy(x \oplus z \oplus xz) == 1$
	$\frac{1}{3}$	$b(c \oplus x \oplus xz \oplus yz) \oplus a(b(1 \oplus c) \oplus (1 \oplus y)(c \oplus z)) == 1$
100	$\frac{2}{3}$	$abcy(1 \oplus xz) == 1$
	$\frac{1}{3}$	$a(b(1 \oplus c) \oplus (1 \oplus y)(c \oplus z)) \oplus b(c \oplus y \oplus x(1 \oplus y \oplus z)) == 1$
101	$\frac{1}{2}$	$b(a \oplus c)(1 \oplus y) == 1$
	$\frac{1}{4}$	$y(b \oplus c \oplus (a \oplus x)z) == 1$
102	$\frac{1}{2}$	$b(a \oplus c)(1 \oplus y) == 1$
	$\frac{1}{4}$	$y(a \oplus b \oplus x \oplus cx \oplus bxz) == 1$
103	$\frac{2}{3}$	$abcy(1 \oplus xz) == 1$
	$\frac{1}{3}$	$b(c \oplus y \oplus xz) \oplus a(b(1 \oplus c) \oplus (1 \oplus y)(1 \oplus c \oplus z)) == 1$
104	$\frac{3}{4}$	$abc(1 \oplus y) == 1$
	$\frac{1}{4}$	$c(1 \oplus x)y \oplus b(1 \oplus c \oplus y \oplus a(1 \oplus c \oplus cy)) \oplus ayz == 1$
	$\frac{1}{2}$	$acy(bz \oplus x(1 \oplus b \oplus z)) == 1$
105	$\frac{2}{3}$	$abcy(1 \oplus xz) == 1$
	$\frac{1}{3}$	$cx(1 \oplus y) \oplus a(b \oplus c \oplus bc \oplus cy) \oplus b(c \oplus y \oplus xyz) == 1$
106	$\frac{3}{5}$	$ab(1 \oplus c)(1 \oplus y) == 1$
	$\frac{2}{5}$	$ac(1 \oplus x)yz \oplus b((1 \oplus a \oplus x)y \oplus c(1 \oplus a \oplus xy \oplus ayz \oplus axyz)) == 1$
	$\frac{1}{5}$	$xy(1 \oplus b \oplus c \oplus z) \oplus ay(1 \oplus b \oplus bc \oplus z) == 1$
107	$\frac{2}{3}$	$abcy(1 \oplus xz) == 1$
	$\frac{1}{3}$	$cx(1 \oplus y) \oplus a(1 \oplus b \oplus bc \oplus y) \oplus b(c \oplus y \oplus xyz) == 1$
108	$\frac{2}{3}$	$abc(1 \oplus y)(1 \oplus xz) == 1$
	$\frac{1}{3}$	$c(a \oplus x)y \oplus b(1 \oplus a \oplus c \oplus ac \oplus xy \oplus xz \oplus yz) == 1$
109	$\frac{1}{3}$	$a(1 \oplus c \oplus bc \oplus yz) \oplus b(c \oplus z \oplus x(y \oplus z)) == 1$
110	$\frac{1}{3}$	$a(1 \oplus c \oplus bc \oplus yz) \oplus b(c \oplus yz \oplus x(y \oplus z)) == 1$
111	$\frac{1}{3}$	$a(1 \oplus c \oplus bc \oplus yz) \oplus b(c \oplus x \oplus xz \oplus yz) == 1$
112	$\frac{1}{3}$	$a(b \oplus c \oplus bc) \oplus cxy \oplus b(c \oplus (x \oplus y)z) == 1$
113	$\frac{1}{3}$	$a(b \oplus c \oplus bc \oplus y \oplus yz) \oplus b(c \oplus (x \oplus y)z) == 1$
114	$\frac{1}{3}$	$b(c \oplus y \oplus xz) \oplus a(1 \oplus c \oplus bc \oplus y \oplus yz) == 1$
115	$\frac{1}{3}$	$a(b \oplus c \oplus bc) \oplus cxy \oplus b(c \oplus yz \oplus x(1 \oplus y \oplus z)) == 1$
116	$\frac{1}{3}$	$b(c \oplus x \oplus xy) \oplus a(b \oplus c \oplus bc \oplus yz) == 1$
117	$\frac{1}{3}$	$a(1 \oplus c \oplus bc \oplus yz) \oplus b(c \oplus x \oplus y \oplus xyz) == 1$
118	$\frac{1}{3}$	$a(1 \oplus c \oplus bc \oplus y \oplus yz) \oplus b(c \oplus y \oplus z \oplus xyz) == 1$
119	$\frac{1}{3}$	$a(1 \oplus c \oplus bc \oplus y \oplus yz) \oplus b(c \oplus y \oplus xz \oplus xyz) == 1$
120	$\frac{1}{3}$	$a(1 \oplus c \oplus bc \oplus yz) \oplus b(c \oplus y \oplus xz \oplus xyz) == 1$
121	$\frac{1}{3}$	$a(b \oplus c \oplus bc \oplus z \oplus yz) \oplus b(c \oplus y(x \oplus z)) == 1$
122	$\frac{1}{3}$	$a(b \oplus c \oplus bc) \oplus cxy \oplus b(c \oplus x \oplus y \oplus z \oplus xyz) == 1$
123	$\frac{1}{2}$	$b(1 \oplus c)(a \oplus xy) == 1$
	$\frac{1}{4}$	$cx(1 \oplus y) \oplus b(c \oplus cx \oplus z \oplus yz) \oplus a(c \oplus (b \oplus y)z) == 1$
124	$\frac{1}{2}$	$b(1 \oplus a \oplus x)(c \oplus yz) == 1$
	$\frac{1}{4}$	$bx(c \oplus y \oplus z) \oplus a(1 \oplus b \oplus c \oplus y \oplus bz) == 1$
125	$\frac{1}{3}$	$a(b \oplus c \oplus bc) \oplus cx(1 \oplus y) \oplus b(c \oplus xyz) == 1$
126	$\frac{1}{3}$	$a(b \oplus c \oplus bc \oplus y \oplus yz) \oplus b(c \oplus x(1 \oplus y)z) == 1$
127	$\frac{1}{3}$	$a(b \oplus c \oplus bc) \oplus cxy \oplus b(c \oplus (1 \oplus x)yz) == 1$
128	$\frac{1}{2}$	$bc(1 \oplus a \oplus xy) == 1$
	$\frac{1}{4}$	$xy(b \oplus c \oplus z) \oplus a(b \oplus c \oplus yz) == 1$
129	$\frac{1}{2}$	$b(1 \oplus c \oplus y \oplus cyz \oplus a(1 \oplus xy \oplus c(1 \oplus y(1 \oplus x \oplus z)))) == 1$
	$\frac{1}{4}$	$b(y(x \oplus z) \oplus c(x \oplus xyz)) \oplus a((1 \oplus b \oplus y \oplus bxy)z \oplus c(1 \oplus y \oplus bxyz)) == 1$
	$\frac{3}{4}$	$(1 \oplus a)b(1 \oplus c)xyz == 1$

(*Continued*.)

Class	Probability	Condition for RC extremal boxes beyond no-signaling polytope
130	$\frac{1}{2}$	$b((1\oplus a)(1\oplus x)yz\oplus c(1\oplus a\oplus x\oplus axy\oplus ayz))==1$
	$\frac{1}{4}$	$bx(c\oplus y\oplus z\oplus yz)\oplus a((1\oplus c)(1\oplus y)\oplus b(1\oplus cxy)(1\oplus z))==1$
	$\frac{3}{4}$	$abcxy(1\oplus z)==1$
131	$\frac{1}{2}$	$b((1\oplus a\oplus x)yz\oplus c(1\oplus a\oplus x\oplus axy\oplus ayz))==1$
	$\frac{1}{4}$	$bx(c\oplus y\oplus z)\oplus a((1\oplus c)(1\oplus y)\oplus b(1\oplus cxy)(1\oplus z))==1$
	$\frac{3}{4}$	$abcxy(1\oplus z)==1$
132	$\frac{1}{2}$	$bc(1\oplus a\oplus x\oplus y\oplus ay\oplus xy\oplus axyz)==1$
	$\frac{1}{4}$	$a(1\oplus c\oplus cy\oplus bz)\oplus y(c\oplus z\oplus xz)\oplus b(y\oplus x(1\oplus c\oplus z\oplus yz))==1$
133	$\frac{1}{2}$	$(1\oplus a)bc(1\oplus y\oplus xyz)==1$
	$\frac{1}{4}$	$y(c\oplus x\oplus xz)\oplus a(1\oplus c\oplus cy\oplus z\oplus bz\oplus yz)\oplus b(x\oplus cx\oplus y\oplus yz\oplus xyz)==1$
134	$\frac{1}{2}$	$ab((x\oplus y\oplus xy)z\oplus c(y\oplus xz\oplus xyz))==1$
	$\frac{1}{4}$	$a\oplus c\oplus bcx\oplus y\oplus acy\oplus bxy\oplus bz\oplus abz\oplus xz\oplus xyz\oplus bxyz==1$
135	$\frac{1}{2}$	$abc(y\oplus xz\oplus xyz)==1$
	$\frac{1}{4}$	$a\oplus c\oplus bcx\oplus y\oplus acy\oplus bxy\oplus abz\oplus xz\oplus bxz\oplus yz\oplus ayz\oplus byz\oplus xyz\oplus bxyz==1$
136	$\frac{1}{3}$	$cxy\oplus a(b\oplus bc\oplus cy)\oplus b(c\oplus x\oplus y\oplus yz\oplus xyz)==1$
	$\frac{2}{3}$	$abcx(1\oplus y)==1$
137	$\frac{1}{3}$	$a(1\oplus c\oplus bc\oplus y\oplus bz)\oplus b(c\oplus y\oplus xyz)==1$
138	$\frac{1}{3}$	$(1\oplus c)xy\oplus a(1\oplus c(1\oplus b\oplus y)\oplus bz)\oplus b(c\oplus y\oplus yz\oplus xyz)==1$
139	$\frac{1}{3}$	$b(c\oplus x\oplus y\oplus yz\oplus xyz)\oplus a(b(1\oplus c)\oplus y(c\oplus z))==1$
	$\frac{2}{3}$	$abcx(1\oplus y)==1$
140	$\frac{1}{4}$	$a(c\oplus cy\oplus bz)\oplus b(c\oplus y\oplus z\oplus xyz)==1$
	$\frac{1}{2}$	$a(y(c\oplus z)\oplus b(1\oplus c\oplus y\oplus yz))==1$
141	$\frac{1}{3}$	$b(c\oplus xy)\oplus a(b(1\oplus c)\oplus(1\oplus y)(c\oplus z))==1$
	$\frac{2}{3}$	$abcxy==1$
142	$\frac{1}{4}$	$b(c\oplus x\oplus cx\oplus y\oplus z\oplus xz)\oplus a(b\oplus y(c\oplus z))==1$
	$\frac{1}{2}$	$bcxy\oplus ac(1\oplus b\oplus y)==1$
143	$\frac{1}{3}$	$b(c\oplus x\oplus y\oplus z\oplus xyz)\oplus a(b(1\oplus c)\oplus y(c\oplus z))==1$
	$\frac{2}{3}$	$abc(1\oplus y)(x\oplus z)==1$
144	$\frac{1}{4}$	$b(a\oplus c\oplus x\oplus cx\oplus y\oplus z\oplus xz)==1$
	$\frac{1}{2}$	$(1\oplus b)c(a\oplus xy)==1$
145	$\frac{1}{4}$	$b(a\oplus c\oplus x\oplus cx\oplus y\oplus yz\oplus xyz)==1$
	$\frac{1}{2}$	$(1\oplus b)c(a\oplus xy)==1$
146	$\frac{1}{3}$	$c(1\oplus x)y\oplus b(c\oplus xy)\oplus a(b\oplus c\oplus bc\oplus z\oplus yz)==1$
147	$\frac{1}{2}$	$b(1\oplus c)(xy\oplus a(1\oplus(1\oplus x)yz))==1$
	$\frac{1}{4}$	$cx(1\oplus y)\oplus b(c\oplus cx\oplus z\oplus xyz)\oplus a(c\oplus(b\oplus y)z)==1$
148	$\frac{1}{2}$	$bc(a\oplus x\oplus xy\oplus ayz\oplus axyz)==1$
	$\frac{1}{4}$	$xy(c\oplus z)\oplus a(1\oplus b\oplus c\oplus y\oplus bz\oplus yz)\oplus b(c\oplus cx\oplus y\oplus z\oplus xz\oplus xyz)==1$
149	$\frac{1}{2}$	$bc(a\oplus x\oplus xy\oplus axyz)==1$
	$\frac{1}{4}$	$xy(c\oplus z)\oplus a(1\oplus b\oplus c\oplus y\oplus bz\oplus yz)\oplus b(c\oplus cx\oplus y\oplus z\oplus xz\oplus yz\oplus xyz)==1$
150	$\frac{1}{2}$	$b(1\oplus c)(a\oplus axyz\oplus xy(1\oplus z))==1$
	$\frac{1}{4}$	$cx(1\oplus y)\oplus b(c\oplus cx\oplus z\oplus yz\oplus xyz)\oplus a(c\oplus(b\oplus y)z)==1$
151	$\frac{1}{2}$	$bc(1\oplus a\oplus y\oplus xy\oplus ayz\oplus axyz)==1$
	$\frac{1}{4}$	$y(1\oplus c\oplus z)\oplus a(1\oplus c\oplus z\oplus bz)\oplus bx(1\oplus c\oplus yz)==1$
152	$\frac{1}{2}$	$bc(1\oplus a\oplus x\oplus y\oplus ay\oplus xy\oplus axyz)==1$
	$\frac{1}{4}$	$a(1\oplus c\oplus cy\oplus bz)\oplus y(1\oplus c\oplus z\oplus xz)\oplus bx(1\oplus c\oplus z\oplus yz)==1$
153	$\frac{1}{2}$	$b((1\oplus a\oplus x)yz\oplus c(1\oplus a\oplus x\oplus axy\oplus axyz))==1$
	$\frac{1}{4}$	$a(1\oplus b\oplus c\oplus y\oplus bz)\oplus bx(c\oplus z\oplus yz)==1$

(*Continued*.)

Class	Probability	Condition for RC extremal boxes beyond no-signaling polytope
154	$\frac{1}{2}$	$bc((1 \oplus x)(1 \oplus y) \oplus a(1 \oplus y \oplus xy \oplus xyz)) == 1$
	$\frac{1}{4}$	$cy \oplus xyz \oplus a(1 \oplus b \oplus c \oplus cy \oplus bz) \oplus b(cx \oplus (x \oplus y \oplus xy)z) == 1$
155	$\frac{1}{2}$	$ab(1 \oplus c \oplus y \oplus cxy \oplus yz \oplus cxyz) == 1$
	$\frac{1}{4}$	$x(c \oplus y) \oplus a(c \oplus y \oplus bz) \oplus b(c \oplus cx \oplus y \oplus z \oplus xyz) == 1$
156	$\frac{1}{2}$	$bc(1 \oplus a \oplus x \oplus y \oplus ay \oplus xy \oplus axyz) == 1$
	$\frac{1}{4}$	$cy \oplus xyz \oplus a(1 \oplus c \oplus cy \oplus bz) \oplus b(y(1 \oplus z) \oplus x(1 \oplus c \oplus z \oplus yz)) == 1$
157	$\frac{1}{2}$	$ac(bxz \oplus y(1 \oplus b \oplus bxz)) == 1$
	$\frac{1}{4}$	$a \oplus c \oplus x \oplus bx \oplus bcx \oplus y \oplus acy \oplus cxy \oplus abz \oplus xz \oplus bxz \oplus byz \oplus xyz \oplus bxyz == 1$
158	$\frac{1}{3}$	$cxy \oplus a(b \oplus c \oplus bc \oplus z \oplus yz) \oplus b(c \oplus yz \oplus x(1 \oplus y \oplus z)) == 1$
159	$\frac{1}{3}$	$c(a \oplus y) \oplus b(1 \oplus a \oplus ac \oplus cx \oplus xy \oplus xz \oplus yz) == 1$
160	$\frac{1}{2}$	$bc(1 \oplus a \oplus y \oplus axy \oplus xyz \oplus axyz) == 1$
	$\frac{1}{4}$	$y(b \oplus c \oplus cx \oplus bxz) \oplus a(b \oplus c \oplus z \oplus yz) == 1$
161	$\frac{1}{2}$	$bc(1 \oplus a \oplus y \oplus xy \oplus xyz \oplus axyz) == 1$
	$\frac{1}{4}$	$y(b \oplus c \oplus bx \oplus cx \oplus bxz) \oplus a(b \oplus c \oplus z \oplus yz) == 1$
162	$\frac{1}{2}$	$bc(1 \oplus a \oplus xy \oplus axy \oplus axyz) == 1$
	$\frac{1}{4}$	$xy(c \oplus bz) \oplus a(b \oplus c \oplus z \oplus yz) == 1$
163	$\frac{1}{2}$	$bc(1 \oplus a \oplus xy \oplus axyz) == 1$
	$\frac{1}{4}$	$xy(b \oplus c \oplus bz) \oplus a(b \oplus c \oplus z \oplus yz) == 1$
164	$\frac{1}{2}$	$ab(1 \oplus c \oplus y \oplus yz \oplus xyz \oplus cxyz) == 1$
	$\frac{1}{4}$	$x(c \oplus y) \oplus a(c \oplus y \oplus bz) \oplus b(c \oplus cx \oplus y \oplus xy \oplus z \oplus xyz) == 1$
165	$\frac{1}{2}$	$ab(1 \oplus c \oplus cxy \oplus z \oplus cyz) \oplus bx(1 \oplus c \oplus y \oplus z \oplus yz \oplus cyz) == 1$
	$\frac{1}{4}$	$b(c \oplus cx \oplus yz) \oplus a((1 \oplus b \oplus y)z \oplus c(1 \oplus y \oplus byz \oplus bxyz)) == 1$
	$\frac{3}{4}$	$abc(1 \oplus x)yz == 1$
166	$\frac{3}{5}$	$bc(a \oplus x)(1 \oplus y) == 1$
	$\frac{1}{5}$	$a(1 \oplus b \oplus c \oplus y \oplus cy \oplus bcy \oplus bz) \oplus b(c \oplus cx \oplus y \oplus cxy \oplus z \oplus xz \oplus xyz) == 1$
	$\frac{2}{5}$	$bxy(c \oplus z) \oplus ay(c \oplus bz) == 1$
167	$\frac{3}{5}$	$abc(1 \oplus y) == 1$
	$\frac{1}{5}$	$(1 \oplus c)x(1 \oplus y) \oplus a(1 \oplus b \oplus c \oplus y \oplus cy \oplus bcy \oplus bz) \oplus b(c \oplus x \oplus cx \oplus y \oplus z \oplus xyz) == 1$
	$\frac{2}{5}$	$bcxy \oplus ay(c \oplus z \oplus bz) == 1$
168	$\frac{2}{5}$	$ay(1 \oplus c \oplus z) \oplus b((1 \oplus y)(1 \oplus xz) \oplus c(1 \oplus yz \oplus xy(1 \oplus z)) \oplus a(1 \oplus yz \oplus c(1 \oplus xz \oplus y(1 \oplus x \oplus z)))) == 1$
	$\frac{1}{5}$	$y(cx \oplus (b \oplus x)z) \oplus a(yz \oplus c(y \oplus by \oplus bxz \oplus bxyz)) == 1$
	$\frac{3}{5}$	$abc(1 \oplus y)(1 \oplus xz) == 1$
169	$\frac{2}{5}$	$(1 \oplus a)cxy(1 \oplus z) \oplus b((1 \oplus y)(1 \oplus xz) \oplus a(1 \oplus c \oplus cxy \oplus cxz \oplus yz) \oplus c(1 \oplus y \oplus xy \oplus xyz)) == 1$
	$\frac{1}{5}$	$(a \oplus b \oplus x)yz \oplus c(abxz \oplus y(1 \oplus ab \oplus x \oplus abxz)) == 1$
	$\frac{3}{5}$	$abc(1 \oplus y)(1 \oplus xz) == 1$
170	$\frac{2}{5}$	$c(a \oplus x)y \oplus b(1 \oplus c \oplus y \oplus cy \oplus cxy \oplus xz \oplus xyz \oplus a(1 \oplus c \oplus y \oplus xy \oplus cxy \oplus cxz \oplus xyz)) == 1$
	$\frac{1}{5}$	$(1 \oplus a \oplus x)y(c \oplus z) \oplus b(acxz \oplus y(1 \oplus ac \oplus x \oplus acxz)) == 1$
	$\frac{3}{5}$	$abc(1 \oplus y)(1 \oplus xz) == 1$
171	$\frac{2}{5}$	$a(1 \oplus c)xyz \oplus b(1 \oplus c \oplus y \oplus cy \oplus cxy \oplus xz \oplus xyz \oplus a(1 \oplus c \oplus y \oplus cxz \oplus xyz)) == 1$
	$\frac{1}{5}$	$(1 \oplus x)y(b \oplus c \oplus z) \oplus a(bcxz \oplus y(1 \oplus bc \oplus z \oplus bcxz)) == 1$
	$\frac{3}{5}$	$abc(1 \oplus y)(1 \oplus xz) == 1$
172	$\frac{2}{5}$	$a(b \oplus y \oplus cy \oplus bcy \oplus bcxyz) \oplus b(x(1 \oplus y)z \oplus c(1 \oplus y \oplus xyz)) == 1$
	$\frac{1}{5}$	$y(b \oplus c \oplus cx \oplus bz) \oplus a(1 \oplus c \oplus y \oplus z \oplus yz \oplus b(1 \oplus c \oplus z)) == 1$
173	$\frac{2}{5}$	$a(1 \oplus c)y \oplus b((1 \oplus y)(1 \oplus xz) \oplus c(1 \oplus yz \oplus xy(1 \oplus z)) \oplus a(1 \oplus cy(x \oplus z \oplus xz))) == 1$
	$\frac{1}{5}$	$cxy \oplus byz \oplus a((1 \oplus b)c \oplus (1 \oplus b \oplus y)z) == 1$
174	$\frac{2}{5}$	$(1 \oplus b)(c \oplus y \oplus xz \oplus xyz) \oplus a(1 \oplus cy \oplus b(1 \oplus cy(1 \oplus z \oplus xz))) == 1$
	$\frac{1}{5}$	$bx(1 \oplus c \oplus y) \oplus a(b(1 \oplus c) \oplus y(c \oplus z)) == 1$

APPENDIX I: LIST OF EXTREMAL BOXES

Class	Probability	Condition for RC extremal boxes beyond no-signaling polytope
175	$\frac{2}{5}$	$b(c \oplus cxy \oplus (x \oplus y)z) \oplus a(c(1 \oplus x)yz \oplus b(1 \oplus y(1 \oplus c \oplus z \oplus cz \oplus cxz))) == 1$
	$\frac{1}{5}$	$(b \oplus c)xy \oplus a(y \oplus c(1 \oplus b \oplus y) \oplus z \oplus bz) == 1$
176	$\frac{2}{5}$	$b(x(1 \oplus y)(1 \oplus z) \oplus c(1 \oplus yz \oplus xy(1 \oplus z))) \oplus a((1 \oplus c)y \oplus b(1 \oplus cy(x \oplus z \oplus xz))) == 1$
	$\frac{1}{5}$	$cxy \oplus byz \oplus a((1 \oplus b)c \oplus (1 \oplus b \oplus y)z) == 1$
177	$\frac{2}{5}$	$b(x(1 \oplus y)z \oplus c(1 \oplus yz \oplus xy(1 \oplus z))) \oplus a(y(1 \oplus c \oplus z) \oplus b(1 \oplus yz \oplus cy(x \oplus z \oplus xz))) == 1$
	$\frac{1}{5}$	$y(cx \oplus (b \oplus x)z) \oplus a(c \oplus bc \oplus yz) == 1$
178	$\frac{2}{5}$	$b(x(1 \oplus y)(1 \oplus z) \oplus c(1 \oplus yz \oplus xy(1 \oplus z))) \oplus a(y(1 \oplus c \oplus z) \oplus b(1 \oplus yz \oplus cy(x \oplus z \oplus xz))) == 1$
	$\frac{1}{5}$	$y(cx \oplus (b \oplus x)z) \oplus a(c \oplus bc \oplus yz) == 1$
179	$\frac{2}{5}$	$cy \oplus b(c \oplus x(1 \oplus y)z) \oplus a(cy \oplus b(1 \oplus (1 \oplus c)yz \oplus (1 \oplus c)xy(1 \oplus z))) == 1$
	$\frac{1}{5}$	$bxy \oplus cx(1 \oplus b \oplus y) \oplus a(c \oplus bc \oplus yz) == 1$
180	$\frac{1}{2}$	$a(c(1 \oplus b \oplus y) \oplus byz) == 1$
	$\frac{1}{4}$	$cxy \oplus a(b \oplus cy \oplus bz) \oplus b(c \oplus y \oplus xy \oplus z \oplus xyz) == 1$
181	$\frac{3}{5}$	$abcy == 1$
	$\frac{1}{5}$	$(1 \oplus c)(a \oplus x)y \oplus b(y \oplus c(1 \oplus a \oplus ay)) == 1$
	$\frac{2}{5}$	$a(1 \oplus y)(b \oplus c \oplus z) == 1$
182	$\frac{1}{2}$	$b(a \oplus x)(c \oplus yz) == 1$
	$\frac{1}{4}$	$cy \oplus b(1 \oplus a \oplus c \oplus y \oplus az) \oplus a(c \oplus z \oplus yz) == 1$
183	$\frac{1}{2}$	$ab(c \oplus yz) == 1$
	$\frac{1}{4}$	$cxy \oplus a(1 \oplus b \oplus c \oplus y \oplus bz) \oplus b(c \oplus y \oplus xy \oplus z \oplus xyz) == 1$
184	$\frac{1}{3}$	$a(b(1 \oplus c) \oplus (1 \oplus y)(c \oplus z)) \oplus b(c \oplus y(x \oplus z)) == 1$
	$\frac{2}{3}$	$abcy(x \oplus z) == 1$
185	$\frac{1}{4}$	$y(a \oplus c \oplus cx \oplus az) \oplus b(1 \oplus c \oplus y \oplus xz \oplus xyz \oplus a(1 \oplus c(1 \oplus y)(1 \oplus xz))) == 1$
	$\frac{1}{2}$	$ac(xyz \oplus b(xz \oplus (1 \oplus x)y(1 \oplus z))) == 1$
	$\frac{3}{4}$	$abc(1 \oplus y)(1 \oplus xz) == 1$
186	$\frac{1}{4}$	$cxy \oplus ay(1 \oplus z) \oplus b(1 \oplus c \oplus y \oplus xz \oplus xyz \oplus a(1 \oplus c(1 \oplus y)(1 \oplus xz))) == 1$
	$\frac{1}{2}$	$ac((1 \oplus x)yz \oplus b(yz \oplus x(y \oplus z \oplus yz))) == 1$
	$\frac{3}{4}$	$abc(1 \oplus y)(1 \oplus xz) == 1$
187	$\frac{1}{4}$	$cxy \oplus ayz \oplus b(1 \oplus a \oplus c \oplus y \oplus xz \oplus xyz) == 1$
	$\frac{1}{2}$	$ac(1 \oplus b \oplus xy \oplus bxy \oplus yz \oplus byz \oplus xyz) == 1$
188	$\frac{1}{4}$	$cxy \oplus a(b \oplus y \oplus yz) \oplus b(c \oplus x(1 \oplus y)z) == 1$
	$\frac{1}{2}$	$ac(1 \oplus y \oplus yz \oplus xyz \oplus b(1 \oplus y(1 \oplus x \oplus z))) == 1$
189	$\frac{1}{4}$	$cxy \oplus ayz \oplus b(a \oplus c \oplus (1 \oplus y)(1 \oplus z \oplus xz)) == 1$
	$\frac{1}{2}$	$ac(1 \oplus b \oplus xy \oplus bxy \oplus yz \oplus byz \oplus xyz) == 1$
190	$\frac{1}{4}$	$cxy \oplus a(b \oplus yz) \oplus b(c \oplus x(1 \oplus y)z) == 1$
	$\frac{1}{2}$	$ac(1 \oplus b \oplus xy \oplus bxy \oplus yz \oplus byz \oplus xyz) == 1$
1	1	$abc == 1$
2	$\frac{1}{3}$	$(1 \oplus x)y(c \oplus z) \oplus b(c \oplus z \oplus xz) \oplus a(b \oplus c \oplus bc \oplus yz) == 1$
	$\frac{2}{3}$	$abc(1 \oplus x)yz == 1$
3	$\frac{1}{2}$	$a(b \oplus c \oplus yz) == 1$
4	$\frac{1}{2}$	$b(a \oplus c \oplus xz) == 1$
5	$\frac{1}{3}$	$a(b \oplus c \oplus bc) \oplus cxy \oplus b(c \oplus z \oplus xz) == 1$
6	$\frac{1}{3}$	$c(b \oplus y \oplus xy) \oplus a(b \oplus c \oplus bc \oplus z \oplus yz) == 1$

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 1984* (IEEE Computer Society Press, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (2005).

[4] J. Barrett, R. Colbeck, and A. Kent, Unconditionally secure device-independent quantum key distribution with only two devices, Phys. Rev. A **86**, 062326 (2012).

[5] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acin, Secrecy extraction from no-signaling correlations, Phys. Rev. A **74**, 042339 (2006).

[6] A. Acin, S. Massar, and S. Pironio, Efficient quantum key distribution secure against no-signaling eavesdroppers, New J. Phys. **8**, 126 (2006).

[7] A. Acin, N. Gisin, and L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (2006).

[8] L. Masanes, Universally Composable Privacy Amplification from Causality Constraints, Phys. Rev. Lett. **102**, 140501 (2009).

[9] E. Hanggi, R. Renner, and S. Wolf, Efficient device-independent quantum key distribution, in *EUROCRYPT 2010*, Lecture Notes in Computer Science Vol. 6110 (Springer, Berlin, 2010), pp. 216–234.

[10] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, Full security of quantum key distribution from no-signaling constraints, IEEE Trans. Inf. Theory **60**, 4973 (2014).

[11] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nat. Commun. **9**, 459 (2018).

[12] P. Horodecki and R. Ramanathan, The relativistic causality vs no-signaling paradigm for multi-party correlations, Nat. Commun. **10**, 1701 (2019).

[13] J. Grunhaus, S. Popescu, and D. Rohrlich, Jamming nonlocal quantum correlations, Phys. Rev. A **53**, 3781 (1996).

[14] R. M. Wald, *General Relativity* (University of Chicago Press, Chicago, 1984).

[15] M. Eckstein and T. Miller, Causality for nonlocal phenomena, Ann. Henri Poincaré **18**, 3049 (2017).

[16] B. Toner, Monogamy of non-local quantum correlations, Proc. R. Soc. A **465**, 59 (2009).

[17] M. Pawlowski and C. Brukner, Monogamy of Bell's Inequality Violations in Nonsignaling Theories, Phys. Rev. Lett. **102**, 030403 (2009).

[18] C. Pfister *et al.*, A universal test for gravitational decoherence, Nat. Commun. **7**, 13022 (2016).

[19] M. Winczewski, T. Das, and K. Horodecki, Upper bounds on secure key against non-signaling adversary via non-signaling squashed secrecy monotones, arXiv:1903.12154.

[20] E. Hanggi and R. Renner, Device-independent quantum key distribution with commuting measurements, arXiv:1009.1833.

[21] E. Gawrilow and M. Joswig, polymake: A framework for analyzing convex polytopes, in *Polytopes: Combinatorics and Computation* (Birkhäuser, Basel, 2000), pp. 43–73.

[22] Calculations were carried out at the Academic Computer Centre in Gdansk in 2020.

[23] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Possibility, impossibility and cheat-sensitivity of quantum bit string commitment, Rev. Mod. Phys. **82**, 665 (2010).

[24] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevResearch.3.033146 for a proof of our main results.

[25] R. Chaves, Polynomial Bell Inequalities, Phys. Rev. Lett. **116**, 010402 (2016).

[26] R. Chaves, R. Kung, J. B. Brask, and D. Gross, Unifying Framework for Relaxations of the Causal Assumptions in Bell's Theorem, Phys. Rev. Lett. **114**, 140403 (2015).

[27] G. Putz, D. Rosset, T. J. Barnea, Y.-C. Liang, and N. Gisin, Arbitrarily Small Amount of Measurement Independence Is Sufficient to Manifest Quantum Nonlocality, Phys. Rev. Lett. **113**, 190402 (2014).

[28] J. Barrett and N. Gisin, How Much Measurement Independence Is Needed to Demonstrate Nonlocality? Phys. Rev. Lett. **106**, 100406 (2011).

[29] M. J. W. Hall, Relaxed Bell inequalities and Kochen-Specker theorems, Phys. Rev. A **84**, 022102 (2011).

[30] M. J. W. Hall, Local Deterministic Model of Singlet State Correlations Based on Relaxing Measurement Independence, Phys. Rev. Lett. **105**, 250404 (2010).

[31] R. Chaves, D. Cavalcanti, and L. Aolita, Causal hierarchy of multipartite Bell nonlocality, Quantum **1**, 23 (2017).

[32] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[33] M. L. Almeida, J. D. Bancal, N. Brunner, A. Acin, N. Gisin, and S. Pironio, Guess Your Neighbor's Input: A Multipartite Nonlocal Game with No Quantum Advantage, Phys. Rev. Lett. **104**, 230404 (2010).

[34] W. van Dam, Nonlocality and communication complexity, Ph.D. thesis, University of Oxford, 2000, https://sites.cs.ucsb.edu/∼vandam/oxford_thesis.pdf.

[35] R. Arnon-Friedman and A. Ta-Shma, Limits of privacy amplification against nonsignaling memory attacks, Phys. Rev. A **86**, 062333 (2012).

[36] E. Hanggi, Device-independent quantum key distribution, Ph.D. thesis, ETH Zurich, 2010, arXiv:1012.3878.

[37] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof, IEEE Trans. Inf. Theory **55**, 3375 (2009).

[38] U. M. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory **39**, 733 (1993).

[39] I. Csiszar and J. Korner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory **24**, 339 (1978).

[40] U. Maurer and S. Wolf, Information-theoretic key agreement: From weak to strong secrecy for free, Lect. Notes Comput. Sci. **1807**, 351 (2000).

[41] J. D. Bancal, C. Branciard, N. Gisin, and S. Pironio, Quantifying Multipartite Nonlocality, Phys. Rev. Lett. **103**, 090503 (2009).

[42] D. Saha and M. Pawlowski, Structure of quantum and broadcasting nonlocal correlations, Phys. Rev. A **92**, 062129 (2015).

[43] R. Ramanathan, A. Soeda, P. Kurzynski, and D. Kaszlikowski, Generalized Monogamy of Contextual Inequalities from the No-Disturbance Principle, Phys. Rev. Lett. **109**, 050404 (2012).

[44] A. Fine, Hidden Variables, Joint Probability, and the Bell Inequalities, Phys. Rev. Lett. **48**, 291 (1982).