Towards Device-Independent Information Processing on General Quantum Networks

Ciarán M. Lee[1,*] and Matty J. Hoban[2,3]
[1]*Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom*
[2]*Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, OX1 3QD, United Kingdom*
[3]*School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*

(Received 21 June 2017; published 10 January 2018)

The violation of certain Bell inequalities allows for device-independent information processing secure against nonsignaling eavesdroppers. However, this only holds for the Bell network, in which two or more agents perform local measurements on a single shared source of entanglement. To overcome the practical constraints that entangled systems can only be transmitted over relatively short distances, large-scale multisource networks have been employed. Do there exist analogs of Bell inequalities for such networks, whose violation is a resource for device independence? In this Letter, the violation of recently derived polynomial Bell inequalities will be shown to allow for device independence on multisource networks, secure against nonsignaling eavesdroppers.

DOI: 10.1103/PhysRevLett.120.020504

The violation of Bell inequalities has been shown to have immense practical importance for quantum information processing [1–3]. Indeed, violation of certain Bell inequalities is a resource for unconditionally secure key distribution [1–7] and randomness amplification [8–10], and for achieving certain computational advantages [11–15]. Moreover, these protocols are *device independent*, meaning they depend only on the observed output statistics of devices used to implement them. In the case of key distribution, for certain protocols the violation of a Bell inequality can be used to lower bound the secure key rate [3]. Furthermore, monogamy relations have been derived between the violation of certain Bell inequalities and the amount of information an eavesdropper can obtain about the generated key; the higher the violation, the lower the information [17–19].

However, these results only hold for the Bell network depicted in Fig. 1(a), in which two agents perform local measurements on a single shared source of entangled systems. The utility of these networks is limited by practical constraints: entangled systems can only be transmitted over relatively short distances, and only a small number of agents can share an entangled state distributed by a single source [20–22]. To overcome this, large-scale multisource quantum networks, such as that schematically illustrated in Fig. 2, have been employed [20,21,23–31]. Yet having multiple intermediate nodes in the network opens the door for novel eavesdropping attacks not seen in the Bell network. Do there exist analog of Bell inequalities for such multisource networks whose violation is a resource for device-independence and which can prevent novel eavesdropper attacks?

Recently, polynomial Bell inequalities have been derived [32–40] on the correlations classically achievable in multisource networks. Violation of these polynomial inequalities witnesses nonclassical behavior in such networks. Can such violations be connected to advantages in information processing on large quantum networks, as was the case in the Bell network? The main obstacle to establishing such a connection is that the set of classical correlations of a given general network forms a nonconvex semialgebraic set [35]; thus, methods establishing standard Bell inequality violation as an information-theoretic resource are no longer applicable [41].

Such bounds on the correlations generated in multisource networks were originally studied in the field of causal inference [44,45]. Recently, the tools and formalism pioneered in this field have begun to see applications in quantum information [46–51]. Indeed, this formalism subsumes and generalizes standard cryptographic constraints such as no-signaling and the assumption that agents each have a secure laboratory, as is discussed in more detail in the Supplemental Material [52]. In this formalism, agents and

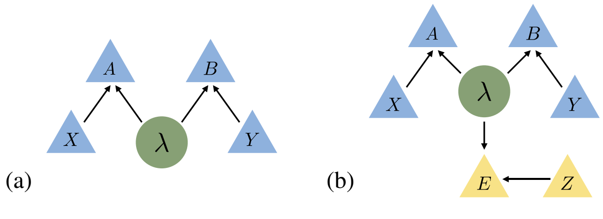

FIG. 1. (a) Bell network: X, Y and A, B denote inputs and outcomes of the agents. (b) Bell network with eavesdropper.

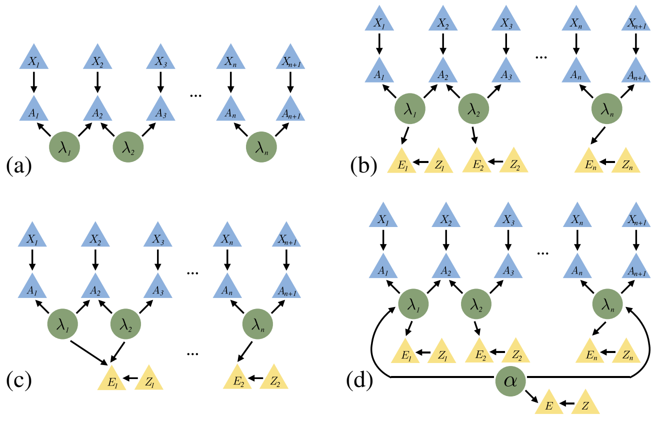
(a)
X_1 X_2 X_3 ... X_n X_{n+1}
A_1 A_2 A_3 A_n A_{n+1}
λ_1 λ_2 λ_n
(b)
E_1 Z_1 E_2 Z_2 E_n Z_n
(c)
(d)
α
E Z

FIG. 2. (a) Repeater network: x_i and A_i denote the possible inputs and outcomes of agent i. (b) Repeater network with eavesdropper holding a system correlated with each source: z_i and E_i denote the possible inputs and outcomes of the measurement on each eavesdropper's system. (c) Eavesdropper holding system correlated with all but last source. (d) Eavesdropper correlating first and last sources.

sources are represented by nodes in directed acyclic graphs (DAGs), with the arrows denoting the causal relationship between nodes. For example, the DAG in Fig 1(a) corresponds to the causal structure of the Bell network. As in standard device independence, this work assumes that both measurement devices used by agents, and the sources they measure, are supplied by an untrusted adversary, or eavesdropper [60].

In the Bell network, violation of a Bell inequality rules out quantum [4] and postquantum [3,5] eavesdroppers. In these attacks, the systems measured by the agents could be correlated with a system held by the eavesdropper, as depicted in Fig. 1(b). These need not be quantum systems, as long as the DAG of Fig. 1(b) holds. Measuring this system using a device with input Z and outcome E, an eavesdropper could gain information about agents' outcomes. That is, it may be that $P(E|A,B,Z) \neq P(E|Z)$. By violating the chained Bell inequality, however [17,19], agents can limit the information such an eavesdropper can gain about their outcomes.

However, for the general networks considered here, there are new avenues for eavesdropping attacks. The eavesdropper supplying the sources can hold systems correlated with more than a single source, as in Fig. 2(c). Additionally, the eavesdropper could even introduce correlations [61] between sources, as in Fig. 2(d). The main findings of the current work are as follows: (1) For an eavesdropper holding independent postquantum systems that can each be correlated with a single source, the violation of certain polynomial inequalities bounds this eavesdropper's information about agents' outcomes. (2) By introducing correlations between sources assumed by the agents to be independent, an eavesdropper can simulate quantum correlations consistent with the original DAG, hence gaining complete knowledge of agents' outcomes. However, increasing the measurement settings can combat this. (3) A new intermediate device-independence scenario: trusting a subset of sources are not correlated with a single system held by an eavesdropper. Given this assumption, the attack of item (2) can be prevented. It should be emphasized here that, as in the work of Ref. [5], security will be established against *nonsignaling* eavesdroppers by bounding their predictive power to learn the outcome of agents' devices. In the case of Fig. 1(b), letting $D(P,Q) \coloneqq \frac{1}{2}\sum_x |P(x) - Q(x)|$ denote the total variational distance, this corresponds to bounding $D(P(E|A,X,Z), P(E|Z))$. Another way of bounding this is through the device-independent guessing probability (see, e.g., [62]), that is, through establishing a bound on $P(E=A)$. Informally, the difference between these two approaches is that, in the former, one is bounding the amount of information an eavesdropper can infer about agents' outcomes from the result of their chosen measurement, and, in the latter, one is bounding the probability that the eavesdropper correctly guesses agents' outcomes.

Each of the above three points will now be illustrated with concrete examples involving repeater and star networks. The derivations of all results in the remainder of the paper are presented in the Supplemental Material.

Repeater networks.—Consider a repeater network in which n sources are each shared between two out of $n+1$ agents, who each perform local measurements with their devices. The crucial information about agents' inputs and outputs is captured by the DAG of Fig. 2(a). The devices held by agents A_1 and A_{n+1} have two inputs, denoted x_1 and x_{n+1}, with x_1, $x_{n+1} \in \{0,1\}$, and two possible outputs $A_1 = a_1$ and $A_{n+1} = a_{n+1}$, again with a_1, $a_{n+1} \in \{0,1\}$. All remaining agents have devices with a single input and four possible outputs, denoted $A_i = a_i^0 a_i^1$ with $a_i^j \in \{0,1\}$. If all λ_i from Fig. 2(a) are classical random variables, then an inequality bounding the classically achievable correlations is

$$\mathcal{R} \coloneqq \sqrt{I} + \sqrt{J} \leq 1, \tag{1}$$

where $I = \frac{1}{4}\sum_{x_1,x_{n+1}} \langle A_1 A_2^0 \cdots A_n^0 A_{n+1} \rangle$,

$$J = \frac{1}{4}\sum_{x_1,x_{n+1}} (-1)^{x_1+x_{n+1}} \langle A_1 A_2^1 \cdots A_n^1 A_{n+1} \rangle,$$

and $\langle A_1 A_2^{x_2} \cdots A_{n+1} \rangle = \sum (-1)^{a_1+a_{n+1}+\sum_{i=2}^{n} a_i^{x_i}}$

$$P(a_1, a_2^0 a_2^1, \ldots, a_{n+1}|x_1, x_{n+1}), \tag{2}$$

where the above sum ranges over a_1, $a_{n+1}, \ldots, a_n^0 a_n^1$. Inequality (1) was derived in [36,37,40], and is the analog of a Bell inequality for this particular DAG. Note that is nonlinear in the joint conditional probability distribution—hence the name *polynomial* Bell inequality.

Now, if all sources are claimed by the eavesdropper to emit singlet states $|\psi^-\rangle$, devices held by agents A_1 and A_{n+1} to be carrying out measurements $(\sigma_z + \sigma_x)/\sqrt{2}$ for $x_1 = 0 = x_{n+1}$ and $(\sigma_z - \sigma_x)/\sqrt{2}$ for $x_1 = 1 = x_{n+1}$ and all remaining devices to be carrying out Bell state measurements (BSMs), the generated correlations are [40]

$$\frac{1+(-1)^{a_1+a_{n+1}}\frac{\left((-1)^{\sum_{i=2}^{n}a_i^0}+(-1)^{\sum_{i=2}^{n}a_i^1+x_1+x_{n+1}}\right)}{2}}{2^{2n}}. \quad (3)$$

Plugging this into Eq. (2) yields $I = J = 1/2$ [40], which results in $\mathcal{R} = \sqrt{2} > 1$, a violation of Eq. (1).

Suppose, as depicted in Fig. 2(b), the eavesdropper holds n independent systems each correlated with one of the n sources. Furthermore, we allow the systems held by the eavesdropper to be postquantum (that is, nonsignaling), as long as the form of the DAG from Fig 2(b) is enforced. Each system can be measured by a device with input z_i and output E_i. As the purpose of repeater networks is to allow agents 1 and $n+1$ to communicate, can such an eavesdropper learn the outputs of agents A_1 and A_{n+1}?

Result 1. A violation of inequality (1) constitutes a bound on an eavesdropper's information about agents' outcomes for the network of Fig 2(b): letting $D(P,Q) \coloneqq \frac{1}{2}\sum_x |P(x) - Q(x)|$ denote the total variational distance, this bound on the information corresponds to

$$D[P(E_1\cdots E_n|A_1, A_{n+1}x_1, x_{n+1}, z_1, \ldots, z_n),$$
$$P(E_1|z_1)\cdots P(E_n|z_n)] \leq 2(2-\mathcal{R}). \quad (4)$$

While the above bound is quite weak [63], it formally relates polynomial inequality violation to the amount of information an eavesdropper can possess about agents' outcomes. It will be shown in the star network section that increasing the number of measurement settings increases the amount of violation; hence, the more measurement settings one has, the more stringent the bound on the eavesdropper's information.

Result 2. By correlating *only* the $i = 1$ and n sources, an eavesdropper can simulate the correlations of Eq. (3).

By introducing such correlations, an eavesdropper can learn all agents' outcomes without alerting them [64]. Moreover, the sources only need to emit classical variables. Such a model is provided in the Supplemental Material and shown to correspond exactly to the quantum correlations Eq. (3). As the eavesdropper manufactured the devices and holds a copy of each source, they can infer each agent's output.

There are two ways to combat this: (i) having agents perform measurements that maximally violate the Clauser-Horne-Shimony-Holt (CHSH) inequality ensures their outputs are uncorrelated from an eavesdropper; (ii) take as a security assumption that the eavesdropper does not hold a system correlated with both first and last sources, as depicted in Fig. 2(d). Even by holding a system correlated with all sources excluding the last one (or the first one), an eavesdropper cannot simulate the correlations of Eq. (3). Indeed, a variant of Eq. (4), in which the left-hand side is replaced by $D(P(E_1, E_2|A_1, \ldots, z_2), P(E_1|z_1)P(E_2|z_2))$, with E and E_1 as depicted in Fig. 2(c), easily follows from the proof of Eq. (4) in the Supplemental Material.

Given the above, one might wonder why violating the CHSH inequality is not always advocated over violating inequality (1). If the sources are replaced with "noisy" Bell states $\rho_i = v_i|\phi^-\rangle\langle\phi^-| + (1-v_i)\mathbb{1}/4$, the above two cases provide an interesting trade-off between source visibility v_i and security. Indeed, postselecting intermediate BSMs results in another noisy Bell state shared between agents A_1 and A_{n+1}, but with lower visibility $V = \prod_{i=1}^{n} v_i$. The CHSH inequality can only be violated by this induced noisy Bell state if $V > 1/\sqrt{2}$. For visibilities below this threshold no security can be established. Equation (1), however, can be violated for visibilities $V > 1/2$ [36,40]. Hence, noisy sources that do not ensure security in the Bell network can in principle establish some security in repeater networks.

Star networks.—Consider the *star* network depicted in Fig. 3(a), first studied in [36,37,39], consisting of n independent sources, each shared between a central agent B and one of n external agents A_i. The devices held by each agent have k possible inputs, denoted y for the central agent and x_i for the external agents, and two potential outputs, denoted b and a_i for external and internal.

Result 3. The following inequality bounds the classically achievable correlations in Fig. 3(a):

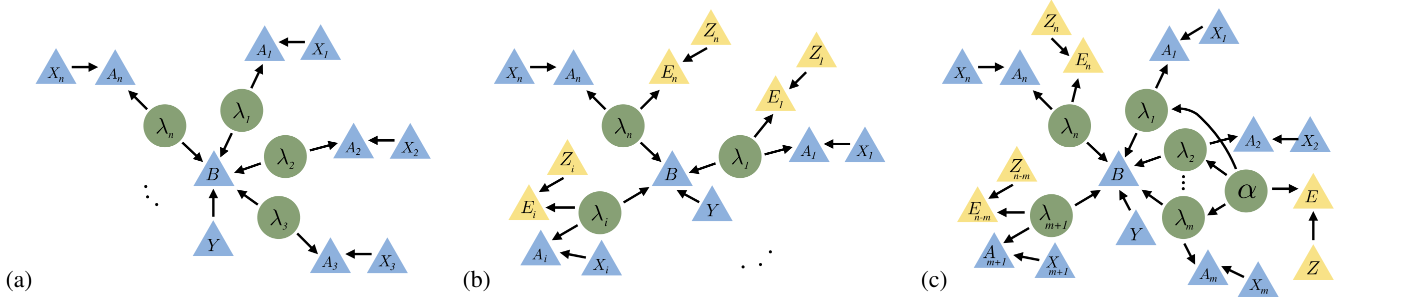

FIG. 3. (a) Star network: y and B denote input and output of central agent and x_i and A_i denote the inputs and outcomes of each remaining agent. (b) Star network with eavesdropper holding system correlated with each source: z_i and E_i denote possible inputs and outputs of eavesdroppers' measurements. (c) Eavesdropper holding system correlated with multiple sources.

$$\mathcal{S} \coloneqq \sum_{i=0}^{k-1} |I_i|^{1/n} \leq k-1, \tag{5}$$

where, $I_i = (1/2^n)\sum_{x_1,\ldots,x_n=i}^{i+1}\langle A_{x_1}^1 \cdots A_{x_n}^n B_i\rangle$, for i ranging from 0 to $k-1$, with $A_k^i = -A_0^i$ and $\langle A_{x_1}^1 \cdots A_{x_n}^n B_y\rangle = \sum(-1)^{b+\sum_{i=2}^n a_i} P(a_1,\ldots,a_n b|x_1,\ldots,x_n,y)$.

All sources are claimed to be in the singlet state $|\psi^-\rangle$. The supplied devices are claimed to function by projecting onto the basis $[\cos(r\pi/2k)|0\rangle + \sin(r\pi/2k)|1\rangle, -\sin(r\pi/2k)|0\rangle + \cos(r\pi/2k)|1\rangle]$, where r is an integer equal to x_i for the ith external agent and y for central agent, outputting 0 for the first basis element and 1 for the second. Here, the central agent performs a separable measurement consisting of simultaneously performing the *same* basis measurement on each of their joint systems, outputting the parity of individual outcomes. This implies that the operator corresponding to the central agent's measurement factorizes [65] as $B_y = B_y^1 \otimes \cdots \otimes B_y^n$ resulting in $\langle A_{x_1} \cdots A_{x_n} B_y\rangle = \langle A_x^1 B_y^1\rangle \cdots \langle A_x^n B_y^n\rangle$. Inequality (5) is upper bounded by $k\cos(\pi/2k)$ [66]. This upper bound is achieved by the above measurements [67,68].

In what follows the simplifying assumption that the central agents measurement device implements a separable measurement will be made. Note that, using the same approach as Sec. III A 3 of [39], it can been shown that all possible violations of Eq. (5) can be achieved using separable measurements on the center node. Hence our assumption of separable measurements is not unjustified.

Suppose, as depicted in Fig. 3(b), the eavesdropper holds n independent (possibly postquantum) systems, each correlated with a single source. By using devices with inputs z_i and outputs E_i to measure these systems, can an eavesdropper learn the outputs of agents A_i?

Result 4. Violating inequality (5) bounds an eavesdropper's information:

$$\begin{aligned} &D[P(E_1 \cdots E_n|A_1,\ldots,A_n,x_1,\ldots,x_n,z_1,\ldots,z_n),\\ &P(E_1|z_1)\cdots P(E_n|z_n)] \leq n(k-\mathcal{S}) \underset{k\to\infty}{\approx} O\left(\frac{1}{k}\right). \end{aligned} \tag{6}$$

Hence, as the number of measurement settings grows, the eavesdropper becomes increasingly uncorrelated from each agent's outcome.

In the repeater network section, an eavesdropper was able to learn agents' outcomes by introducing a bit α which correlated the first and last sources, depicted in Fig. 2(d). Could a similar eavesdropping attack work here? In fact, the same level of security as Eq. (8) can be established against an eavesdropper who correlates $m \leq n$ sources by sharing a random variable with $q < k$ values—each taken with probability p_l—among the m sources, as illustrated in Fig. 3(c). This is formalized by demanding that an eavesdropper's information about agents' outcomes takes the following form:

$$P_{E|A_1\cdots A_m} = \sum_{l=1}^{q} p_l P_{E_1^l|A_1}\ldots P_{E_m^l|A_m}. \tag{7}$$

With this formalization of the eavesdroppers attack, our final result can now be stated.

Result 5. Given Eq. (7), the following bound can be derived:

$$\begin{aligned} &D[P(EE_{n-m}\cdots E_n|A_1,x_1,\ldots,z,z_{n-m}\ldots,z_n),\\ &P(E|z)\cdots P(E_n|z_n)] \leq [n+m(q-1)](k-\mathcal{S}). \end{aligned} \tag{8}$$

As in Eq. (6), this bound goes as $1/k$ for large k. Thus, if an eavesdropper introduces correlations between sources, their information of agents' outcomes can be bounded as long as the number of measurement settings is large enough.

Conclusion.—Monogamy relations using the degree of violation of a Bell inequality to bound an eavesdropper's information are central to standard device-independent information processing [8,17,18,69]. Thus, the results presented in this work pave the way for device-independent information processing on multisource quantum networks. Indeed, Eq. (3) states that once intermediate outcomes are announced, agents A_1 and A_{n+1} share a bit. Moreover, an eavesdropper's information about this bit is bounded by the degree of violation of polynomial Bell inequality (1). Hence device-independent key distribution is possible in repeater networks. Moreover, security can be established using entangled sources with lower visibilities than that required for key distribution in the Bell network. Future work will focus on establishing a full security proof for device-independent key distribution on repeater networks.

However, for multisource quantum networks, there are new avenues for eavesdropping attacks; by correlating sources an eavesdropper can simulate quantum correlations consistent with the original DAG. Fortunately, it was demonstrated that increasing the number of measurement settings, or ensuring the eavesdropper does not hold a system correlated with a specified subset of sources, can prevent this attack. As large-scale quantum networks—a primer for a quantum internet—are becoming possible with current technology, developing novel information processing protocols on such networks is critical. Moreover, as component networks making up future large quantum networks are likely to consist of diverse technologies, having protocols that are independent of specific technological implementations is critical.

Beyond generalized monogamy relations, can violation of polynomial Bell inequalities be related to advantages in other information processing tasks? References [11–13] have related nonlocal correlations in the Bell network to quantum advantages over classical computers. This was established in the measurement-based paradigm—where adaptive measurements are performed on a single source. Relating computational advantages to violation of polynomial inequalities would be quite practical: it is more feasible to create an entangled state consisting of multiple sources of few-body entangled systems than of a single source of many-body entangled systems.

C. M. L. thanks D. Browne for helpful discussions and J. J. Barry for encouragement. This work was supported by the EPSRC through the UCL Doctoral Prize Fellowship, and the Networked Quantum Information Technologies (NQIT) Hub (M013243/1).

*ciaran.lee@ucl.ac.uk

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

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

[3] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[4] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).

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

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

[7] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).

[8] R. Colbeck and R. Renner, Free randomness can be amplified, Nat. Phys. **8**, 450 (2012).

[9] R. Ramanathan, F. G. Brandão, K. Horodecki, M. Horodecki, P. Horodecki, and H. Wojewódka, Randomness Amplification under Minimal Fundamental Assumptions on the Devices, Phys. Rev. Lett. **117**, 230501 (2016).

[10] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning *et al.*, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[11] J. Anders and D. E. Browne, Computational Power of Correlations, Phys. Rev. Lett. **102**, 050502 (2009).

[12] M. J. Hoban, E. T. Campbell, K. Loukopoulos, and D. E. Browne, Non-adaptive measurement-based quantum computation and multi-party Bell inequalities, New J. Phys. **13**, 023014 (2011).

[13] M. J. Hoban and D. E. Browne, Stronger Quantum Correlations with Loophole-Free Post-Selection, Phys. Rev. Lett. **107**, 120402 (2011).

[14] J. J. Wallman and E. Adlam, Nonlocality in instantaneous quantum circuits, arXiv:1412.4131.

[15] See also [16] for a connection between other physical phenomena and computation.

[16] C. M. Lee and J. H. Selby, Deriving Grover's lower bound from simple physical principles, New J. Phys. **18**, 093047 (2016).

[17] J. Barrett, A. Kent, and S. Pironio, Maximally Nonlocal and Monogamous Quantum Correlations, Phys. Rev. Lett. **97**, 170409 (2006).

[18] L. Aolita, R. Gallego, A. Cabello, and A. Acín, Fully Nonlocal, Monogamous, and Random Genuinely Multipartite Quantum Correlations, Phys. Rev. Lett. **108**, 100401 (2012).

[19] R. Colbeck and R. Renner, Hidden Variable Models for Quantum Theory Cannot Have Any Local Part, Phys. Rev. Lett. **101**, 050403 (2008).

[20] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. **83**, 33 (2011).

[21] A. Seri, A. Lenhard, D. Rieländer, M. Gündoğan, P. M. Ledingham, M. Mazzera, and H. de Riedmatten, Quantum Correlations between Single Telecom Photons and a Multimode On-Demand Solid-State Quantum Memory, Phys. Rev. X **7**, 021028 (2017).

[22] J. Yin *et al.*, Satellite-based entanglement distribution over 1200 kilometers, Science, **356**, 1140 (2017).

[23] S. B. van Dam, P. C. Humphreys, F. Rozpedek, S. Wehner, and R. Hanson, Multiplexed entanglement generation over quantum networks using multi-qubit nodes, Quant. Sci. Technol. **2**, 034002 (2017).

[24] A. Reiserer, N. Kalb, M. S. Blok, K. J. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, Robust quantum-Network Memory Using Decoherence-Protected Subspaces of Nuclear Spins, Phys. Rev. X **6**, 021040 (2016).

[25] K. Goodenough, D. Elkouss, and S. Wehner, Assessing the performance of quantum repeaters for all phase-insensitive gaussian bosonic channels, New J. Phys. **18**, 063005 (2016).

[26] F. Rozpedek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, Realistic parameter regimes for a single sequential quantum repeater, arXiv:1705.00043.

[27] T. Satoh, S. Nagayama, and R. Van Meter, The network impact of hijacking a quantum repeater, arXiv:1701.04587.

[28] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai *et al.*, Quantum teleportation with independent sources and prior entanglement distribution over a network, Nat. Photonics **10**, 671 (2016).

[29] R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, Quantum teleportation across a metropolitan fibre network, Nat. Photonics **10**, 676 (2016).

[30] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[31] S. Pirandola, Capacities of repeater-assisted quantum communications, arXiv:1601.00966.

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

[33] D. Rosset, C. Branciard, T. J. Barnea, G. Pütz, N. Brunner, and N. Gisin, Nonlinear Bell Inequalities Tailored for Quantum Networks, Phys. Rev. Lett. **116**, 010403 (2016).

[34] E. Wolfe, R. W. Spekkens, and T. Fritz, The inflation technique for causal inference with latent variables, arXiv:1609.00672.

[35] C. M. Lee and R. W. Spekkens, Causal inference via algebraic geometry: Feasibility tests for functional causal structures with two binary observed variables, J. Causal Inference **5** (2017)

[36] C. Branciard, D. Rosset, N. Gisin, and S. Pironio, Bilocal versus nonbilocal correlations in entanglement-swapping experiments, Phys. Rev. A **85**, 032119 (2012).

[37] C. Branciard, N. Gisin, and S. Pironio, Characterizing the Nonlocal Correlations Created via Entanglement Swapping, Phys. Rev. Lett. **104**, 170401 (2010).

[38] A. Tavakoli, Bell-type inequalities for arbitrary noncyclic networks, Phys. Rev. A **93**, 030101 (2016).

[39] A. Tavakoli, P. Skrzypczyk, D. Cavalcanti, and A. Acín, Nonlocal correlations in the star-network configuration, Phys. Rev. A **90**, 062109 (2014).

[40] K. Mukherjee, B. Paul, and D. Sarkar, Correlations in n-local scenario, Quantum Inf. Process. **14**, 2025 (2015).

[41] Although, it should be noted that there do exist families of networks more general than the Bell network—involving sequential measurements on a single shared source of entanglement—that each give rise to a convex set of classical correlations [42,43].

[42] R. Gallego, L. E. Würflinger, R. Chaves, A. Acín, and M. Navascués, Nonlocality in sequential correlation scenarios, New J. Phys. **16**, 033037 (2014).

[43] F. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín, Unbounded randomness certification using sequences of measurements, Phys. Rev. A **95**, 020102 (R) (2017).

[44] J. Pearl, *Causality: Models, Reasoning, and Inference*, 2nd ed. (Cambridge University Press, Cambridge, England, 2009).

[45] P. Spirtes, C. Glymour, and R. Scheines, *Causation, Prediction, and Search*, 2nd ed. (MIT Press, Cambridge, MA, 2001).

[46] C. J. Wood and R. W. Spekkens, The lesson of causal discovery algorithms for quantum correlations: Causal explanations of bell-inequality violations require fine-tuning, New J. Phys. **17**, 033002 (2015).

[47] J.-M. A. Allen, J. Barrett, D. C. Horsman, C. M. Lee, and R. W. Spekkens, Quantum Common Causes and Quantum Causal Models, Phys. Rev. X **7**, 031021 (2017).

[48] R. Chaves, J. B. Brask, and N. Brunner, Device-Independent Tests of Entropy, Phys. Rev. Lett. **115**, 110501 (2015).

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

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

[51] J. B. Brask and R. Chaves, Bell scenarios with communication, J. Phys. A **50**, 094001 (2017).

[52] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.120.020504 for a discussion of the causal model framework, and a detailed derivation of Eqs. (4), (5), (6), and (8), together with a rigorous treatment of the classical model that simulates the quantum correlations of Eq. (3). This includes Refs. [53–59].

[53] R. Colbeck and R. Renner, No extension of quantum theory can have improved predictive power, Nat. Commun. **2**, 411 (2011).

[54] F. Andreoli, G. Carvacho, L. Santodonato, R. Chaves, and F. Sciarrino, Maximal violation of n-locality inequalities in a star-shaped quantum network, Phys. Rev. A **95**, 062315 (2017).

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

[56] R. Rabelo, M. Ho, D. Cavalcanti, N. Brunner, and V. Scarani, Device-Independent Certification of Entangled Measurements, Phys. Rev. Lett. **107**, 050502 (2011).

[57] A. Tavakoli, M. O. Renou, N. Gisin, and N. Brunner, Correlations in star networks: From bell inequalities to network inequalities, New J. Phys. **19**, 073003 (2017).

[58] J. Henson, R. Lal, and M. F. Pusey, Theory-independent limits on correlations from generalized Bayesian networks, New J. Phys. **16**, 113043 (2014).

[59] T. Fritz, Beyond Bell's theorem: Correlation scenarios, New J. Phys. **14**, 103001 (2012).

[60] Furthermore, it is assumed here that an eavesdropper can only apply *individual attacks*, where the eavesdropper's attack on each run of the experiment is independent of the attacks on other runs. Moreover, systems are assumed to be independently and identically generated, and finite statistical effects will not be taken into account. These assumptions allow the study of device-independent cryptography in multisource networks to be initiated. It is left open for future work to prove security under minimal assumptions.

[61] Recall that each agent is in an isolated lab isolated. All they observe is their device outcome. They are completely ignorant about whether the eavesdropper has manufactured the specified independent sources—or is trying to cheat by introducing correlations between sources.

[62] L. Masanes, S. Pironio, and A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices, Nat. Commun. **2**, 238 (2011).

[63] Note that this bound is only weak when considering quantum correlations. If agents share PR boxes and intermediate agents are allowed to perform one of two 2-outcome measurements in a given round, then the same bound as Eq. (4) can be derived. In this case, perfect security can be established, as PR boxes achieve $\mathcal{R} = 2$ [36].

[64] That is, once the agents have announced their inputs [5].

[65] This factorization is a generalization of the one in Eq. (20) of [39]. The derivation is the same as that of Ref. [39].

[66] S. Wehner, Tsirelson bounds for generalized clauser-horne-shimony-holt inequalities, Phys. Rev. A **73**, 022110 (2006).

[67] S. L. Braunstein and C. M. Caves, Wringing out better Bell inequalities, Ann. Phys. (N.Y.) **202**, 22 (1990).

[68] See the Supplemental Material http://link.aps.org/supplemental/10.1103/PhysRevLett.120.020504 for a proof.

[69] R. Augusiak, M. Demianowicz, M. Pawłowski, J. Tura, and A. Acín, Elemental and tight monogamy relations in nonsignaling theories, Phys. Rev. A **90**, 052323 (2014).