Genuine Multipartite Entanglement is Not Necessary for Standard Device-Independent Conference Key Agreement

Lewis Wooltorton,[1,2,3,*] Peter Brown,[4,†] and Roger Colbeck[1,‡,§]
[1]*Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom*
[2]*Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and*
Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1FD, United Kingdom
[3]*Inria, ENS de Lyon, LIP, 46 Allee d'Italie, 69364 Lyon Cedex 07, France*
[4]*Télécom Paris, Inria, LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France*

(Received 1 April 2025; accepted 25 September 2025; published 26 November 2025)

Conference key agreement aims to establish shared, private randomness among many separated parties in a network. Device-independent conference key agreement (DICKA) is a variant in which the source and the measurement devices used by each party need not be trusted. So far, DICKA protocols largely fall into two categories: those that rely on violating a joint Bell inequality using genuinely multipartite entangled states and those that concatenate many bipartite protocols. The question of whether a hybrid protocol exists, where a multipartite Bell inequality can be violated using only bipartite entanglement, was asked by Grasselli *et al.* [Quantum **7**, 980 (2023)]. We answer this question affirmatively, by constructing an asymptotically secure DICKA protocol achieving the same rate as the concatenation of bipartite device-independent quantum key distribution, yet relying on a single joint Bell violation. Our results prompt further discussion on the benefits of multipartite entanglement for DICKA over its bipartite alternative, and we give an overview of different arguments for near-term devices.

DOI: 10.1103/v4s8-3zl5

Introduction—Information-theoretically secure communication between two separated parties requires a source of shared, private randomness, called a key. Conference key agreement (CKA) is an extension of key distribution to many parties, i.e., it aims to set up a key shared between $N > 2$ parties which could then be used to secure communication among the N parties. Quantum solutions exist [1–9] and, as in ordinary quantum key distribution (QKD), they can be made device independent (DI) [10–13]. In other words, by witnessing certain nonlocal correlations [14–16], one can show that a device independent conference key agreement (DICKA) protocol is secure without any device characterization [17–21].

A key question is to find the most efficient way to perform DICKA. Each network topology will determine which protocols can be performed, and a popular choice is the star network. Here, a central node distributes part of a multipartite state to each party every round. One can then consider which states permit DICKA with this setup. Current literature has focused around the use of states with genuine multipartite entanglement (GME), that is, states that are not biseparable [22], such as the Greenberger-Horne-Zeilinger (GHZ) state. In Refs. [10–12], the parity Clauser-Horne-Shimony-Holt (CHSH) inequality was introduced as a multipartite Bell inequality for DICKA maximally violated by the GHZ state. This was later generalized to another tailored inequality [13], and in Ref. [23] analytical bounds on the von Neumann entropy, conditioned on witnessing their violation, were derived using techniques from Refs. [10,24,25]. In Ref. [23], a comparison is also made to benchmark different DICKA protocols, including ones that are formed by concatenating bipartite device independent quantum key distribution (DIQKD), as described in Ref. [3]. Upper bounds on DICKA rates were also studied in Refs. [26,27].

Many of the above protocols have the following structure, which we refer to as "standard": the central node distributes part of a multipartite state to each party, and rounds are divided into test and generation. On test rounds, all parties test a multipartite Bell expression, and on generation rounds they generate raw key. Reconciliation is performed where one party, say Alice, releases some error correction information that the other parties use to correct their strings. Privacy amplification then follows to ensure that an adversary has negligible information about the final key. The conference key rate is often defined as the difference

[*] Contact author: lewis.wooltorton@ens-lyon.fr
[†] Contact author: peter.brown@telecom-paris.fr
[‡] Contact author: roger.colbeck@kcl.ac.uk
[§] Present address: Department of Mathematics, King's College London, Strand, London, WC2R 2LS, United Kingdom.

between the entropy of Alice's raw string conditioned on the possible side information of an adversary and the highest cost of error correction between every other party and Alice, divided by the number of rounds [23].

Shared key can also be established using many independent bipartite protocols. Consider the same network, except that now the source distributes bipartite entanglement between Alice and every other party. Alice then engages in $N - 1$ bipartite DIQKD protocols and by the end holds a distilled key from each. She selects one of these as her final key and publicly releases the exclusive OR (XOR) of the selected key with every other secret key she holds. Each party can then obtain the selected key using their private key. We refer to this type of protocol as a concatenation of bipartite DIQKD, and note that Alice should, in principle, use a separate device for each bipartite exchange to avoid opening memory loopholes [28] (or else make some additional assumption about her measurement device).

Concatenating bipartite DIQKD requires bipartite entanglement distribution only. However, it deviates from the standard protocol structure because it is based upon bipartite subprotocols, whose security is proven independently. This raises the question asked in Ref. [23] of whether a standard realization of DICKA exists in which only biseparable states need to be distributed. An affirmative answer is known for device-dependent CKA [29], where the following protocol structure was considered. Every round, rather than distributing $N - 1$ bipartite entangled states, the source probabilistically chooses which party shares entanglement with Alice, and no trusted information about who was chosen is released. Then, the parties perform local measurements each round to generate raw key and use standard QKD reconciliation. It is not *a priori* clear if nonzero conference key rate can be achieved with this protocol, and Ref. [29] showed it to be possible in the device-dependent setting. Specifically, Ref. [29] provided a family of biseparable states that lead to nonzero conference key in the N-BB84 protocol [4].

While biseparable states can be used for key agreement in the N-BB84 protocol, performing this in practice would be wasteful. If each party could learn when they share entanglement with Alice, which can be achieved with authenticated classical communication, the protocol reduces to a concatenation of bipartite QKD. This has better error reconciliation efficiency than that considered in Ref. [29] (see Supplemental Material [30] for details), resulting in a higher conference key rate.

For the DI scenario, consider the case where each party is restricted to a single device, and a single multipartite Bell expression is tested to derive security (i.e., the standard protocol structure is adopted). Can a positive conference key rate still be established with biseparable states?

In this Letter, we answer the above question affirmatively. Biseparable states can be used for DICKA with a single device per party and a single Bell inequality. Our solution is operationally equivalent to the concatenation of many bipartite DIQKD protocols and hence more straightforward to implement with existing technology than one that requires GME. An additional advantage of our protocol is that it requires only one device per party, preventing particular memory attacks. Moreover, our results suggest the need for further discussion on the realistic benefits of multi-partite entanglement for DICKA over bipartite concatenation.

Standard DICKA protocol without GME—Our protocol operates in the following way: each round, a source distributes a multipartite state, on which isolated measurements are made and a multipartite Bell inequality is tested. Witnessing its maximum violation guarantees a conference key rate equal to that of $N - 1$ concatenated bipartite DIQKD protocols. This can be achieved by a biseparable state that includes a flag register indicating who shares entanglement each round.

Importantly, security is derived entirely from the maximum violation of the introduced Bell inequality, without trusting the flag. To achieve this, each user performs one side of a CHSH test [51]. The average CHSH violation of each party with Alice is then measured, conditioned on the flag indicating said party shared entanglement; the sum of all such violations constitutes our Bell value. Any dishonesty in the flag will manifest as a reduction in the CHSH value for one of the pairings, ensuring security. Since every party has access to the flag, which must be reliable in the case of a high Bell violation, they can engage in some classical communication to each distill a secret key with Alice. Efficient reconciliation can then be conducted by Alice announcing the bitwise XOR of a chosen final key with every other secret key. An advantage of this protocol is that it is not vulnerable to the same memory attacks [28] as concatenating $N - 1$ DIQKD protocols [23], implying that one conference key can still be established with a single device per party.

Technical description—For clarity, we focus on three parties, Alice, Bob and Carole, but the generalization to n parties is straightforward. Assume the three parties are arranged in a star configuration, and each have access to one device, as shown in Fig. 1. We use random variables X for the input to Alice's device and (A, T_A) for the outputs. These take values $x \in \{0, 1\}$ and $(a, t_A) \in \{0, 1\}^2$, respectively [52]. Bob and Carole's devices have three inputs and four outcomes, described by the random variables Y, Z and $(B, T_B), (C, T_C)$, which take values $y, z \in \{0, 1, 2\}$ and $(b, t_B), (c, t_C) \in \{0, 1\}^2$, respectively. We denote the final conference key $\mathsf{K}_{\mathrm{CKA}}$. Fixing this Bell scenario, we describe the following protocol [53]: 1. Each round, an unknown tripartite state is distributed among all parties and each party announces receipt of their part of the state. Alice then randomly assigns the round as "test" or "generation" and communicates her choice to Bob and Carole. 2. On test rounds, each party uses their private random number generator to choose an input $x, y, z \in \{0, 1\}$, and on generation rounds Alice sets $X = 0$, and Bob and Carole set $Y = Z = 2$.

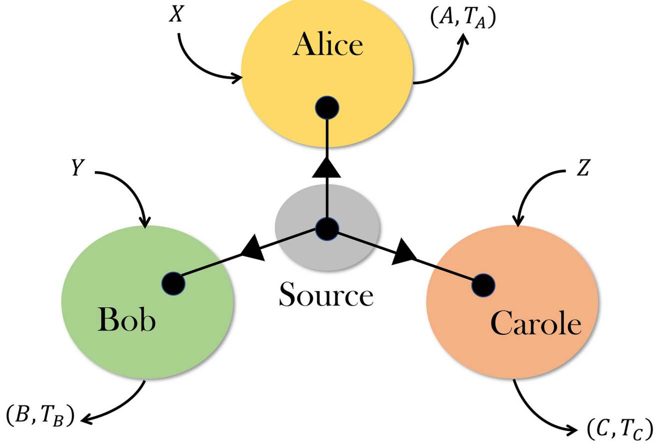

FIG. 1. Graphical representation of our DICKA protocol. Each round, every party receives part of a quantum state from an untrusted source, randomly samples an input $X/Y/Z$, and performs an untrusted measurement. They obtain two outcomes, and the joint statistics are used to estimate the value of a multipartite Bell inequality. In the honest implementation, the outcome $T_{A/B/C}$ corresponds to a classical flag indicating who shares entanglement with Alice on that round, while the outcome $A/B/C$ results from performing a CHSH-type measurement on a quantum system.

3. Each party performs their measurement and stores the outcomes in their respective classical registers [54]. 4. After a sufficient number of rounds, Alice, Bob, and Carole announce the values of their registers T_A, T_B, and T_C for all rounds. They abort if any of their strings differ or if the strings are constant. 5. Each party publicly announces all of their inputs and outputs from the test rounds, and they check for a multipartite Bell inequality violation. If the violation is less than some threshold [55], they abort [56]. 6. Using the flag data, Alice and Carole communicate to distill a private key [57] K_{AC}. Similarly, Alice and Bob distill a private key K_{AB}. 7. Alice sets $\mathsf{K}_{\mathrm{CKA}} = \mathsf{K}_{AB}$ and computes $\mathsf{K}_{\mathrm{XOR}} \coloneqq \mathsf{K}_{AC} \oplus \mathsf{K}_{AB}$, which she announces. Carole computes $\mathsf{K}_{\mathrm{CKA}} = \mathsf{K}_{\mathrm{XOR}} \oplus \mathsf{K}_{AC}$, meanwhile Bob sets $\mathsf{K}_{\mathrm{CKA}} = \mathsf{K}_{AB}$.

In this protocol, all classical communication takes place using authenticated public channels (i.e., an eavesdropper can overhear, but not modify these messages) and the quantum communication uses insecure quantum channels (i.e., an eavesdropper can do anything allowed by quantum physics to these signals). It is important that during the protocol untrusted devices do not learn anything other than what they need to perform the protocol; see Supplemental Material [30] for details.

We now consider an ideal honest implementation using a biseparable state. In this implementation, the state shared between the honest parties is

$$\rho = \frac{1}{2}|\Phi_0\rangle\langle\Phi_0|_{Q_AQ_B} \otimes |+\rangle\langle+|_{Q_C} \otimes |000\rangle\langle000|_{T_AT_BT_C} + \frac{1}{2}|\Phi_0\rangle\langle\Phi_0|_{Q_AQ_C} \otimes |+\rangle\langle+|_{Q_B} \otimes |111\rangle\langle111|_{T_AT_BT_C}, \quad (1)$$

where $Q_{A/B/C}$ are qubit systems, $|\Phi_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and T_A, T_B, and T_C are binary registers. Each party then performs the following ideal, four outcome measurements. On registers T_A, T_B, and T_C, each party measures in the computational basis (for every input). On registers Q_A, Q_B, and Q_C, the parties perform qubit measurements according to their input, described by the observables

$$A_0 = \sigma_Z,\ A_1 = \sigma_X,$$
$$B_{0/1} = C_{0/1} = (\sigma_Z \pm \sigma_X)/\sqrt{2},\ B_2 = C_2 = \sigma_Z, \quad (2)$$

where σ_Z and σ_X are the Pauli operators. Note that the classical nature of the $T_{A/B/C}$ registers makes it easy not to abort in step 4 ($|0\rangle\langle 0|_{T_A}$ etc. can be macroscopic).

Security proof—In the asymptotic regime, there are typically two quantities of interest for a DICKA protocol. The first is the conditional von Neumann entropy of Alice's key generation measurement, stored in the classical system A, conditioned on Eve's quantum side information E. This captures the amount of extractable randomness per round in Alice's raw string. The second captures the worst case cost of error reconciliation between Alice and every other party. That is, it captures the maximum information Alice needs to release so that every party can correct their raw key to Alice's. The conference key rate is the difference between these two terms and captures the amount of distillable key, per round, in the asymptotic limit. If one entangled state is consumed in each round of the protocol, as in the case of GHZ-based protocols [10–12], this can be reinterpreted as the rate per entangled state. The suitability of this definition is debatable, which we elaborate on in the Discussion and Supplemental Material [30].

For our protocol, we define the bipartite rate between Alice and Bob, conditioned on a particular value of the flag T [58], by

$$r^{\infty}_{T=0} = \inf\ H(A|X=0, T=0, E) - H(A|B, X=0, Y=2, T=0), \quad (3)$$

where $H(A|E)_\rho = H(\rho_{AE}) - H(\rho_E)$, $H(\rho) = -\mathrm{Tr}[\rho\log(\rho)]$, and the infimum is taken over all quantum states and measurements compatible with some observations, such as the violation of a Bell inequality. A similar quantity, $r^{\infty}_{T=1}$, can be defined between Alice and Carole. Following Alice's XOR reconciliation procedure, the final conference key rate is given by

$$r^{\infty}_{\mathrm{CKA}} = \min\{p_T(0)r^{\infty}_{T=0}, p_T(1)r^{\infty}_{T=1}\}, \quad (4)$$

where $p_T(t)$ is the probability the parties record $T = t$. Since in each round a single multipartite state is distributed, $r^{\infty}_{\mathrm{CKA}}$ captures the asymptotic rate per state consumed by the protocol. Proving security then becomes the task of bounding $\inf H(A|X=0, T=t, E)$ for $t \in \{0,1\}$.

For the security proof, we assume each party holds an arbitrary quantum system $\tilde{Q}_{A/B/C}$. We denote Alice's positive operator-valued measure elements $\tilde{M}_{(a,t)|x}$, Bob's $\tilde{N}_{(b,t)|y}$, and Carole's $\tilde{O}_{(c,t)|z}$. We denote the underlying state, including Eve's purification, by $|\Psi\rangle_{\tilde{Q}_A\tilde{Q}_B\tilde{Q}_C E}$. The outcome t can have no dependence on the parties' input choices, otherwise the no-signaling assumption would be violated. Therefore, we can consider the parties observing a joint distribution (suppressing the tensor product)

$$p(abct|xyz) = \langle\Psi|\tilde{M}_{(a,t)|x}\tilde{N}_{(b,t)|y}\tilde{O}_{(c,t)|z}|\Psi\rangle, \qquad (5)$$

from which the Bell value $\langle I\rangle := \langle I_{\mathrm{CHSH}}^{AB,T=0}\rangle + \langle I_{\mathrm{CHSH}}^{AC,T=1}\rangle$ can be calculated, where $I_{\mathrm{CHSH}}^{AB,T=t} := \tilde{A}_{0,t}(\tilde{B}_{0,t} + \tilde{B}_{1,t}) + \tilde{A}_{1,t}(\tilde{B}_{0,t} - \tilde{B}_{1,t})$ and similarly for $I_{\mathrm{CHSH}}^{AC,T=t}$. In the above, $\tilde{A}_{x,t} := \tilde{M}_{(0,t)|x} - \tilde{M}_{(1,t)|x}$ (note that $\tilde{A}_{x,t}$ is not an observable) and similarly for $\tilde{B}_{y,t}, \tilde{C}_{z,t}$, and for any operator O, $\langle O\rangle = \langle\Psi|O|\Psi\rangle$. The local bound of $\langle I\rangle$ is at most 2, whereas the quantum bound of $2\sqrt{2}$ is achieved by the honest strategy.

The following proposition underpins the security of our construction at maximum violation, i.e., when $\langle I\rangle = 2\sqrt{2}$, and under the assumption of asymptotically many independent and identically distributed rounds (this can be used as a basis for finite rates using tools such as the entropy accumulation theorem [59,60]).

Proposition 1—Let the Bell expression I be defined above. Then we have the following for $t \in \{0,1\}$:

$$\inf H(A|X=0, T=t, E) = 1, \qquad (6)$$

where the infimum is taken over all quantum states and measurements that achieve $\langle I\rangle = 2\sqrt{2}$ and for which it is impossible to abort in step 4, and the von Neumann entropy is evaluated on the postmeasurement state

$$\rho_{AE|X=0,T=t} = \frac{1}{p_{T|X=0}(t)} \sum_{a\in\{0,1\}} |a\rangle\langle a|_A \otimes \mathrm{Tr}_{\tilde{Q}_A\tilde{Q}_B\tilde{Q}_C}\left[(\tilde{M}_{(a,t)|0} \otimes \mathbb{1}_{\tilde{Q}_B\tilde{Q}_C E})|\Psi\rangle\langle\Psi|\right], \qquad (7)$$

where $p_{T|X=0}(t) := \sum_{a\in\{0,1\}} \langle\Psi|(\tilde{M}_{(a,t)|0} \otimes \mathbb{1}_{\tilde{Q}_B\tilde{Q}_C E})|\Psi\rangle$.

The precise proposition and proof can be found in Supplemental Material [30]. Note that, in the honest strategy, Alice and Bob (Carole) will observe perfect correlations when $X=0$, $Y=2$, and $T=0$ ($X=0$, $Z=2$, and $T=1$), hence we find $r_{T=0}^{\infty} = r_{T=1}^{\infty} = 1$. The honest strategy also has $p_T(0) = p_T(1) = 1/2$ and as a result we find $r_{\mathrm{CKA}}^{\infty} = 1/2$. We also show our construction is robust to noise in Supplemental Material [30].

Our protocol is similar in structure to the device-dependent result of Ref. [29]. Moreover, it leaves open the possibility for modification. For example, one could equivalently use an honest implementation without source randomness or substitute the CHSH inequality for another Bell inequality with different properties. We elaborate on these points in Supplemental Material [30].

Discussion—In this Letter, we presented a secure DICKA protocol that can be performed (even optimally) without GME states, resolving the open question posed in Ref. [23]. Our protocol is operationally equivalent to concatenating bipartite DIQKD protocols based on CHSH tests. This prompts another question: how do protocols with bipartite entanglement compare to those with GME? Frequently, the figure of merit chosen for this comparison is the key rate per "network resource" or, rather, per entangled state [6,23,29]. As acknowledged by the authors of Ref. [23], this can be misleading, since it implies that every entangled state has the same experimental cost. In many experimental setups, it is easier to generate bipartite entanglement than entanglement shared by three or more systems; hence it would not make sense to define the same cost to both (as done in Ref. [23]). Theoretically, a more suitable measure could consist of an entanglement monotone [61], such as the amount of distillable entanglement [62], which is likely complicated in the multipartite scenario [63]. In practice, the best approach will be architecture dependent, with factors such as cost, complexity, and performance playing a role.

For example, Ref. [3] discussed different network topologies in which (device-dependent) protocols using GHZ states are argued to have an advantage over the bipartite case below certain noise thresholds. Here, the key rate is measured per unit time. This depends on the network structure, something that is missed when counting per entangled state [23]. In Ref. [9], a different network topology was used that allows multiple Bell pairs to be distilled in a single network use, referred to as "multicast." Under these conditions, the experiment in Ref. [9] maintains a key rate improvement from the use of GHZ states. Whether such improvements can be observed in DICKA is an interesting question, since the stringent noise requirements of DI protocols may be limiting.

Additional arguments against concatenating bipartite DIQKD protocols include [3] (i) the additional qubit consumption of $N-1$ Einstein-Podolsky-Rosen pairs versus one GHZ state, (ii) the additional classical communication cost to perform efficient XOR based reconciliation, and (iii) the issue of memory effects [23], requiring Alice to use a separate device to establish a key with each party. Points (i) and (ii) depend on the capabilities of an experimental setup. For example, it may take multiple attempts to successfully distribute a GHZ state, and a greater classical overhead may be acceptable in return for more noise-resilient quantum resources. Moreover, a significant bottleneck for QKD implementations is the computational efficiency of privacy amplification [64]. Efficient algorithms impose requirements on the min-entropy rate (the min-entropy accumulated as a fraction of the total block length) and the seed length. Whether bipartite protocols or multipartite protocols are more beneficial in this regard is a further open question.

For point (iii), we have introduced a DICKA protocol based on bipartite entanglement that inherently requires one device per party. In essence, the conditional entropy of Alice's key when entanglement is shared with Bob is certified by the same Bell test as when shared with Carole, so Alice can use the same device. If the device was to leak information about an Alice-Bob key bit in the announced data for the Alice-Carole key, this would decrease the Bell violation, as Alice and Carole would no longer maximally violate CHSH. We also acknowledge that concatenating bipartite DIQKD in the standard way with a single device per party can still be made secure against memory attacks. Though penalizing as the number of parties increase, provided *all* information leaked over the classical channel is accounted for in the min-entropy estimate of each bipartite key, the final conference key remains secure.

Finally, we emphasize that this discussion is relevant to DI protocols that use GHZ states. This excludes, for example, protocols based on interfering single photons or weak coherent pulses [5,8,65,66]. Similar remarks could also be made for DI randomness generation protocols based on GHZ states [23–25,67] versus, e.g., parallel bipartite protocols. It would be interesting to see if the protocol presented here could be adapted to this task, allowing randomness generation from N devices using bipartite entanglement. Unlike key distribution, however, randomness expansion experiments do not require the physical separation of devices. Rather, the no-signaling assumption can be satisfied by shielding the devices from each other, while remaining in the same laboratory. This reduces the effect of transmission loss when distributing entanglement, boosting the noise tolerance. This could make protocols that rely on GHZ states more realistic.

Acknowledgments—The authors thank Gláucia Murta for useful discussions about CKA protocols and feedback on a preliminary version of the manuscript. This work was supported by EPSRC via the Quantum Communications Hub (Grant No. EP/T001011/1), the Integrated Quantum Networks Hub (Grant No. EP/Z533208/1), Grant No. EP/SO23607/1, and the European Union's Horizon Europe research and innovation program under the project "Quantum Secure Networks Partnership" (QSNP, Grant Agreement No. 101114043).

Data availability—The data that support the findings of this article are openly available [31].

[1] A. Cabello, Multiparty key distribution and secret sharing based on entanglement swapping, arXiv:quant-ph/0009025.

[2] K. Chen and H. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states, Quantum Inf. Comput. **7**, 689 (2007).

[3] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, New J. Phys. **19**, 093012 (2017).

[4] F. Grasselli, H. Kampermann, and D. Bruß, Finite-key effects in multipartite quantum key distribution protocols, New J. Phys. **20**, 113014 (2018).

[5] F. Grasselli, H. Kampermann, and D. Bruß, Conference key agreement with single-photon interference, New J. Phys. **21**, 123002 (2019).

[6] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, Adv. Quantum Technol. **3**, 2000025 (2020).

[7] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement, Sci. Adv. **7**, eabe0395 (2021).

[8] G. Carrara, G. Murta, and F. Grasselli, Overcoming fundamental bounds on quantum conference key agreement, Phys. Rev. Appl. **19**, 064017 (2023).

[9] A. Pickston, J. Ho, A. Ulibarrena, F. Grasselli, M. Proietti, C. L. Morrison, P. Barrow, F. Graffitti, and A. Fedrizzi, Conference key agreement in a quantum network, npj Quantum Inf. **9**, 82 (2023).

[10] J. Ribeiro, G. Murta, and S. Wehner, Fully device-independent conference key agreement, Phys. Rev. A **97**, 022307 (2018).

[11] T. Holz, D. Miller, H. Kampermann, and D. Bruß, Comment on "fully device-independent conference key agreement," Phys. Rev. A **100**, 026301 (2019).

[12] J. Ribeiro, G. Murta, and S. Wehner, Reply to "comment on 'fully device-independent conference key agreement'," Phys. Rev. A **100**, 026302 (2019).

[13] T. Holz, H. Kampermann, and D. Bruß, Genuine multipartite Bell inequality for device-independent conference key agreement, Phys. Rev. Res. **2**, 023251 (2020).

[14] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, Phys. Rev. **47**, 777 (1935).

[15] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, England, 1987).

[16] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Nonlocal correlations as an information-theoretic resource, Phys. Rev. A **71**, 022101 (2005).

[17] J. Barrett, L. Hardy, and A. Kent, No signalling and quantum key distribution, Phys. Rev. Lett. **95**, 010503 (2005).

[18] 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).

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

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

[21] U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[22] A multipartite state is biseparable if it can be written as a convex combination of states, where each state in the combination is separable across some bipartition.

[23] F. Grasselli, G. Murta, H. Kampermann, and D. Bruß, Boosting device-independent cryptography with tripartite nonlocality, Quantum **7**, 980 (2023).

[24] F. Grasselli, G. Murta, H. Kampermann, and D. Bruß, Entropy bounds for multiparty device-independent cryptography, PRX Quantum **2**, 010308 (2021).

[25] E. Woodhead, B. Bourdoncle, and A. Acín, Randomness versus nonlocality in the Mermin-Bell experiment with three parties, Quantum **2**, 82 (2018).

[26] K. Horodecki, M. Winczewski, and S. Das, Fundamental limitations on the device-independent quantum conference key agreement, Phys. Rev. A **105**, 022604 (2022).

[27] A. Philip, E. Kaur, P. Bierhorst, and M. M. Wilde, Multipartite intrinsic non-locality and device-independent conference key agreement, Quantum **7**, 898 (2023).

[28] J. Barrett, R. Colbeck, and A. Kent, Memory attacks on device-independent quantum cryptography, Phys. Rev. Lett. **106**, 010503 (2013).

[29] G. Carrara, H. Kampermann, D. Bruß, and G. Murta, Genuine multipartite entanglement is not a precondition for secure conference key agreement, Phys. Rev. Res. **3**, 013264 (2021).

[30] See Supplemental Material at http://link.aps.org/supplemental/10.1103/v4s8-3zl5 for proof of Proposition 1 and additional discussions, which includes Refs. [29–48].

[31] L. Wooltorton, P. Brown, and R. Colbeck, Dataset for Fig. 1 of the Supplemental Material, 10.5281/zenodo.17235290 (2025).

[32] A. Aspect, J. Dalibard, and G. Roger, Experimental test of Bell's inequalities using time-varying analyzers, Phys. Rev. Lett. **49**, 1804 (1982).

[33] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature (London) **526**, 682 (2015).

[34] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, Experimental quantum key distribution certified by Bell's theorem, Nature (London) **607**, 682 (2022).

[35] R. Bhavsar, S. Ragy, and R. Colbeck, Improved device-independent randomness expansion rates using two sided randomness, New J. Phys. **25**, 093035 (2023).

[36] V. Paulsen, *Completely Bounded Maps and Operator Algebras*, Cambridge Studies in Advanced Mathematics (Cambridge University Press, Cambridge, England, 2003).

[37] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, Phys. Rev. A **91**, 052111 (2015).

[38] D. Cui, A. Mehta, H. Mousavi, and S. S. Nezhadi, A generalization of CHSH and the algebraic structure of optimal strategies, Quantum **4**, 346 (2020).

[39] T. Franz, F. Furrer, and R. F. Werner, Extremal quantum correlations and cryptographic security, Phys. Rev. Lett. **106**, 250502 (2011).

[40] E. Kreyszig, *Introductory Functional Analysis with Applications* (John Wiley & Sons, New York, 1991), Vol. 17.

[41] V. B. Scholz and R. F. Werner, Tsirelson's problem, arXiv:0812.4305.

[42] M. Navascués, T. Cooney, D. Pérez-García, and N. Villanueva, A physical approach to Tsirelson's problem, Found. Phys. **42**, 985 (2012).

[43] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, Quantum **8**, 1445 (2024).

[44] M. Navascués, S. Pironio, and A. Acín, Bounding the set of quantum correlations, Phys. Rev. Lett. **98**, 010401 (2007).

[45] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).

[46] T. P. Le, C. Meroni, B. Sturmfels, R. F. Werner, and T. Ziegler, Quantum correlations in the minimal scenario, Quantum **7**, 947 (2023).

[47] V. Barizien, P. Sekatski, and J.-D. Bancal, Custom Bell inequalities from formal sums of squares, Quantum **8**, 1333 (2024).

[48] L. Wooltorton, P. Brown, and R. Colbeck, Device-independent quantum key distribution with arbitrarily small nonlocality, Phys. Rev. Lett. **132**, 210802 (2024).

[49] M. Farkas, Unbounded device-independent quantum key rates from arbitrarily small nonlocality, Phys. Rev. Lett. **132**, 210803 (2024).

[50] G. Pereira Alves and J. Kaniewski, Optimality of any pair of incompatible rank-one projective measurements for some nontrivial Bell inequality, Phys. Rev. A **106**, 032219 (2022).

[51] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. **23**, 880 (1969).

[52] We use upper case for random variables and lower case for particular instances.

[53] As is standard in cryptography, we use the following assumptions: 1. Each party works within an isolated laboratory within which they can control information flow to the outside world as well as to individual devices within their laboratory. 2. Each party has their own private random number generator. 3. The eavesdropper is limited by the laws of physics and is computationally unbounded. 4. The parties can communicate classically through authenticated public channels.

[54] Each device only learns its own input and not whether it is a test or generation round. See Supplemental Material [30] for details.

[55] For the purposes of this proof-of-principle demonstration, this threshold is set to the maximum Bell violation (cf. Proposition 1).

[56] Additionally, all parties need to release a fraction of their generation data to perform an alignment test with Alice. If the fraction of matched outcomes is below a threshold, they will also abort.

[57] In the event of maximum Bell violation, the key distillation process is trivial, since all raw key bits are secure.

[58] Recall, given that the protocol did not abort, all parties agree on their classical variable $T_{A/B/C} \equiv T$.

[59] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, Commun. Math. Phys. **379**, 867 (2020).

[60] 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).

[61] M. B. Plenio and S. S. Virmani, An introduction to entanglement theory, Quantum Inf. Comput. **7**, 001 (2007).

[62] R. Arnon-Friedman and J.-D. Bancal, Device-independent certification of one-shot distillable entanglement, New J. Phys. **21**, 033010 (2019).

[63] A. Philip and M. M. Wilde, Device-independent certification of multipartite distillable entanglement, Phys. Rev. A **111**, 012436 (2025).

[64] M. Hayashi and T. Tsurumaru, More efficient privacy amplification with less random seeds via dual universal hash function, IEEE Trans. Inf. Theory **62**, 2213 (2016).

[65] X.-Y. Cao, Y.-S. Lu, Z. Li, J. Gu, H.-L. Yin, and Z.-B. Chen, High key rate quantum conference key agreement with unconditional security, IEEE Access **9**, 128870 (2021).

[66] X.-Y. Cao, J. Gu, Y.-S. Lu, H.-L. Yin, and Z.-B. Chen, Coherent one-way quantum conference key agreement based on twin field, New J. Phys. **23**, 043002 (2021).

[67] L. Wooltorton, P. Brown, and R. Colbeck, Expanding bipartite Bell inequalities for maximum multi-partite randomness, arXiv:2308.07030.