Genuine multipartite entanglement is not a precondition for secure conference key agreement

Giacomo Carrara^{✉,*}, Hermann Kampermann, Dagmar Bruß, and Gláucia Murta^{✉,†}

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany

(Received 30 July 2020; accepted 16 February 2021; published 19 March 2021)

Entanglement plays a crucial role in the security of quantum key distribution. A secret key can only be obtained by two parties if there exists a corresponding entanglement-based description of the protocol in which entanglement is witnessed, as shown by Curty *et al.* [M. Curty, M. Lewenstein, and N. Lütkenhaus, *Phys. Rev. Lett.* **92**, 217903 (2004)]. Here we investigate the role of entanglement for the generalization of quantum key distribution to the multipartite scenario, namely, conference key agreement. In particular, we ask whether the strongest form of multipartite entanglement, namely, genuine multipartite entanglement, is necessary to establish a conference key. We show that, surprisingly, a nonzero conference key can be obtained even if the parties share biseparable states in each round of the protocol. Moreover, we relate conference key agreement with entanglement witnesses and show that a nonzero conference key can be interpreted as a nonlinear entanglement witness that detects a class of states which cannot be detected by usual linear entanglement witnesses.

DOI: [10.1103/PhysRevResearch.3.013264](https://doi.org/10.1103/PhysRevResearch.3.013264)

I. INTRODUCTION

Secure communication is a central demand for modern society. Security can be provided by quantum key distribution (QKD), which readily enters the industrial market. In QKD [1,2], entanglement plays a crucial role in the security proofs [3,4]. Indeed, even prepare-and-measure protocols [1,5], which do not require any entanglement for their implementation, have an entanglement-based counterpart [6] which can be used for the protocol's security analysis. In Ref. [7], the authors showed that entanglement is in fact a necessary condition to obtain a secure key in a QKD protocol and, moreover, the entanglement of the state shared by Alice and Bob can be witnessed using the measurements performed in the protocol.

We consider a generalization of QKD to the scenario where N parties wish to establish a common shared secret key. This task is called a conference key agreement (CKA) and allows for secure broadcast. CKA can be achieved using a concatenation of bipartite QKD [8–10], together with additional classical communication. However, the rich structure of multipartite correlations opens the possibility to design new protocols which can have clear advantages in certain network architectures [11]. Several protocols exploiting the correlations of multipartite entangled states have been proposed using qubit systems in the device-dependent [11–15] and device-independent scenario [16–18], as well as continuous-variable systems [19–21]. Even a proof of princi-

ple implementation of CKA with four nodes has been recently realized [22].

Here we ask the question of whether the strongest form of multipartite entanglement, namely, genuine multipartite entanglement, is a necessary ingredient for CKA based on multipartite quantum correlations. We will show that, counter-intuitively, this is not the case: N parties can establish a secret conference key even when the state distributed in each round of the protocol is biseparable. Moreover, we prove that, to obtain a no-zero conference key, the measurements used in the protocol need to be able to witness entanglement across any partition of the set of parties, extending the result of Ref. [7] to the multipartite scenario.

II. PRELIMINARIES

We focus on CKA protocols [23] consisting of several rounds where, in each round, a single copy of a multipartite state is distributed to the N parties, namely, Alice and Bob₁, ..., Bob _{$N-1$} . Upon receiving the systems, the parties perform local measurements and record the classical outcome. The scenario is sketched in Fig. 1.

In such protocols, an important figure of merit is the asymptotic secret key rate, i.e., the ratio between the number of extracted secret bits and the number of shared copies of the state, in the limit of an infinite number of rounds. Analogously to the bipartite case [24,25], the asymptotic secret key rate of the CKA protocols under consideration can be expressed, after the usual postprocessing (parameter estimation, one-way information reconciliation and privacy amplification) as [11]

$$r^\infty = \max [0, H(X|E) - \max_i H(X|Y_i)], \quad (1)$$

where X and Y_i denote the registers that store the outcomes of the measurements performed by Alice and Bob _{i} , respectively, in the key generation rounds. Here $H(X|E) = H(XE) - H(E)$ is the von Neumann entropy of Alice's outcome in the key generation rounds, conditioned on Eve's

*carrara@uni-duesseldorf.de

†glauca.murta@uni-duesseldorf.de

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

FIG. 1. Sketch of the considered CKA scenario: At each round of the protocol, a quantum resource is distributed to the parties (in our particular case, a multipartite quantum state). The parties perform local measurements and utilize the outcomes to extract a common secret key.

(possibly quantum) side information. $H(X|Y_i) = H(XY_i) - H(Y_i)$ represents the amount of information Alice needs to communicate to Bob_{*i*} so he can correct his raw key. The maximum over the Bobs in Eq. (1) illustrates the fact that Alice needs to communicate enough information to correct for the worst case of the Bobs. We recall that for a state ρ_X of a system X , the quantum von Neumann entropy is defined as $[H(X) = -\text{Tr}[\rho_X \log_2 \rho_X]]$.

The conditional von Neumann entropy satisfies the following properties [26]:

(1) Additivity for product states [[26], Corollary 5.9]: If $\rho_{AB} = \rho_A \otimes \rho_B$, then $H(A|B) = H(A)$.

(2) Data processing [[26], Corollary 5.5]: Considering ρ_{ABC} , then $H(A|BC) \leq H(A|B)$.

(3) Conditioning on classical information [[26], Proposition 5.4]: If $\rho_{ABF} = \sum_j q_j \rho_{AB}^j \otimes |j\rangle\langle j|_F$ is a classical-quantum state where the system F is a classical register, then $H(A|BF) = \sum_j q_j H(A|BF = j)$ where $H(A|BF = j)$ is evaluated on the state ρ_{AB}^j .

Our goal is to investigate the role of multipartite entanglement in the single copy of the state shared by the N parties in each round of the protocol. In the bipartite case, either the state is separable and no key can be extracted or the state is entangled and can potentially be used for QKD [7]. In the multipartite scenario, however, different classes of entanglement can be defined, which have been extensively studied [27–31].

Let S_α be a proper subset of the parties and $\bar{S}_\alpha$ be the complement. Then a state $\rho_{AB_1 \dots B_{N-1}}$ is *separable with respect to the partition* $S_\alpha | \bar{S}_\alpha$ if it is of the form

$$\rho_{AB_1 \dots B_{N-1}} = \sum_j q_j \rho_{S_\alpha}^j \otimes \rho_{\bar{S}_\alpha}^j, \quad (2)$$

where $\rho_{S_\alpha}^j$ and $\rho_{\bar{S}_\alpha}^j$ are states shared by the parties in S_α and $\bar{S}_\alpha$, respectively, and where $q_j \geq 0$ and $\sum_j q_j = 1$.

A state is called *biseparable* [27] if it is a convex combination of states that are separable with respect to different partitions, that is,

$$\rho_{bs} = \sum_{S_\alpha} \sum_j q_{S_\alpha}^j \rho_{S_\alpha}^j \otimes \rho_{\bar{S}_\alpha}^j, \quad (3)$$

where the first sum is performed over all proper subsets S_α of the parties. Again, the coefficients must satisfy $q_{S_\alpha}^j \geq 0 \forall j, S_\alpha$ and $\sum_\alpha \sum_j q_{S_\alpha}^j = 1$. It is worth noting that a state can be biseparable, yet not separable with respect to any partition.

Finally, if a state cannot be written in the form of Eq. (3) we call it *genuine multipartite entangled (GME)*. All CKA protocols based on multipartite entanglement proposed so far [11–17, 19–21] explore the correlations of GME states, such as the Greenberger-Horne-Zeilinger (GHZ) state [32] or the W state [33].

III. ENTANGLEMENT IS NECESSARY FOR CKA

In the following, we prove that entanglement across all partitions in the state shared by the parties is necessary to lead to a nonzero asymptotic conference key rate.

Theorem 1. Given a CKA protocol, if the state shared by the N parties is separable with respect to some partition $S_\alpha | \bar{S}_\alpha$, then $r^\infty = 0$.

Proof of Theorem 1 To prove the statement, since the asymptotic key rate in Eq. (1) includes an optimization over all the Bobs, it suffices to prove that $H(X|Y_i) \geq H(X|E)$ for a specific Bob_{*i*}. Let us consider a state separable with respect to a partition $S_\alpha | \bar{S}_\alpha$, in the form of Eq. (2), such that S_α contains Alice. We consider a Bob contained in $\bar{S}_\alpha$, let us say Bob_{*i*}. Let Eve have a purification of the state of the form

$$|\psi_{AB_1, \dots, B_{N-1} E F F'}\rangle = \sum_j \sqrt{q_j} |\psi_{S_\alpha \bar{S}_\alpha E}^j\rangle |j\rangle_F |j\rangle_{F'}, \quad (4)$$

where $|\psi_{S_\alpha \bar{S}_\alpha E}^j\rangle$ is a purification of $\rho_{S_\alpha}^j \otimes \rho_{\bar{S}_\alpha}^j$ and the systems F and F' are classical registers held by Eve. The additional classical register F' is necessary to exploit the properties of the von Neumann entropy of classical-quantum states. In fact, tracing out the system F' , Eve's system E and all the Bobs except Bob_{*i*} will result in a state of the form

$$\rho_{AB_i F} = \sum_j q_j \rho_A^j \otimes \rho_{B_i}^j \otimes |j\rangle\langle j|_F, \quad (5)$$

which is a classical-quantum state consisting of a separable state for Alice and Bob_{*i*}, paired with the classical register F held by Eve. We remark that performing local measurements on a separable state will result in a separable state. Thus, after the measurements of the CKA protocol, the state will still be in the form of Eq. (5). Moreover, we can write the following chain of inequalities:

$$\begin{aligned} H(X|Y_i) &\geq H(X|Y_i F) \\ &= \sum_j q_j H(X|Y_i F = j) \\ &= \sum_j q_j H(X|F = j) \\ &= H(X|F) \geq H(X|E F F') = H(X|E_{\text{tot}}), \end{aligned} \quad (6)$$

where E_{tot} indicates the global subsystem of Eve, which includes the classical registers. In the first, second, and third line we used Property 2, Property 3, and Property 1 of the conditional Von Neumann entropy, respectively. Finally, in the

fourth line we used again Properties 2 and 3. This concludes the proof.

It follows that there must be some entanglement shared between Alice and all the Bobs to establish a secret common key. It is worth noting that for $N = 2$ this proof simplifies the argumentation given in Ref. [7].

IV. CKA WITHOUT GME

We will now focus on the main question, that is, whether a positive conference key can be established without GME. We answer this question in the affirmative by exhibiting a family of biseparable states that can lead to a nonzero conference key,

$$\rho_{AB_1, \dots, B_{N-1}}^{(N,k)} = \sum_{\substack{\alpha \\ S_\alpha \in \mathcal{S}^{(k)}}} \frac{1}{\mathcal{N}} \Phi_{S_\alpha}^{\text{GHZ},k} \bigotimes_{\substack{m \\ B_m \in \bar{S}_\alpha}} |+\rangle\langle+|_{B_m}, \quad (7)$$

where $\mathcal{S}^{(k)}$ is the set of subsets of k parties that contain Alice and $k-1$ Bobs, $\Phi_{S_\alpha}^{\text{GHZ},k} = |\text{GHZ}\rangle\langle\text{GHZ}|_{S_\alpha}$ is the projector of the GHZ state shared by the k parties of the subset S_α , defined as $|\text{GHZ}\rangle_{S_\alpha} = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes k} + |1\rangle^{\otimes k})$ and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The normalization factor is equal to $\mathcal{N} = \binom{N-1}{k-1}$ since the number of terms in the convex combination is equal to the number of subsets of cardinality $k-1$ within the $N-1$ Bobs.

We show that this family of states can be used to generate a nonzero key in a simple CKA protocol, namely, the N-BB84 protocol [14]. The N-BB84 protocol consists of X -basis measurements for the parameter estimation rounds and Z -basis measurements for the key generation rounds.

The asymptotic conference key rate of the N-BB84 protocol for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, Eq. (7), as a function of the total number of parties N and the number of parties k that are entangled is given by

$$r_{\text{N-BB84}}^\infty(N, k) = \frac{1}{2} \frac{N-k}{N-1} \log_2 \left(\frac{N-k}{N-1} \right) + \frac{1}{2} \frac{N+k-2}{N-1} \log_2 \left(\frac{N+k-2}{N-1} \right). \quad (8)$$

A strictly positive rate $r_{\text{N-BB84}}^\infty(N, k)$ is obtained for all possible values of N and k even though the family of states Eq. (7) is biseparable for $k < N$. Therefore, we have proven our main result:

Theorem 2. Genuine multipartite entanglement is not necessary for CKA, and a nonzero secret conference key rate r^∞ can be established in a CKA protocol that uses biseparable states at each round.

A detailed derivation of $r_{\text{N-BB84}}^\infty(N, k)$ is presented in Appendix A. Moreover, in Appendix B, we show that the key rate given in Eq. (8) is optimal for the family of states Eq. (7), when the key is generated with measurements in the Z basis.

In Fig. 2 we plot the secret key rate, $r_{\text{N-BB84}}^\infty(N, k)$, as a function of the number of parties N for different values of the number of entangled parties k . For comparison, we also plot the key rate of a CKA protocol based on the concatenation of multiple bipartite QKD protocols, in the noiseless scenario, for a network with bottleneck [11]. In this case, Alice runs $N-1$ bipartite QKD protocols to establish a secret key with each of the Bobs.

FIG. 2. Asymptotic secret key rate, $r_{\text{N-BB84}}^\infty(N, k)$, for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, Eq. (7), for the N-BB84 CKA protocol. The curves (straight lines) represent different values of k (light grey: from left to right, $k = 2$, $k = 5$, $k = 10$; dark grey: top, $k = N-1$, bottom, $k = \frac{N}{2}$). We also plot the key rate of CKA based on multiple noiseless bipartite QKD protocols (dashed line), both as a function of N . We remark that since $k \leq N-1$, the curves for fixed k start at different values of N .

Figure 2 shows that $r_{\text{N-BB84}}^\infty$ approaches 1 as N increases, if k equals $N-1$. Moreover, even in the case when only two parties, Alice and one of the Bobs, are entangled in each term of the mixture, a nonzero secret key can be obtained. However, for a fixed value of k , $r_{\text{N-BB84}}^\infty \rightarrow 0$ as N increases. The comparison with the key rate of a concatenation of multiple bipartite QKD protocols yields interesting results: while, on one hand, no advantage can be obtained for $k = 2$, on the other hand an advantage can be obtained in the regime of a k close to N , with a marked advantage for high k .

To further analyze the advantage obtainable with the presented protocol compared to the concatenation of bipartite QKD protocols, we evaluate the performance of the family of states Eq. (7) in the presence of noise. We consider the case where the qubit of each Bob undergoes a *local depolarizing channel* $\mathcal{D}$, where $\mathcal{D}[\rho] = (1-p)\rho + p\frac{\mathbb{I}}{2}$. We compare this with a concatenation of bipartite QKD protocols that undergo the same type of noise. Details of this analysis can be found in Appendix C. Figure 3 illustrates the result for $N=6$. Even in the noisy scenario, an advantage can be obtained in the low noise regime and for k close to N .

Our results show that CKA without GME states is possible. We remark that in Ref. [34] the authors have established that GME is a necessary condition for a nonzero key in a one-shot CKA protocol. This result, at first, seems in contradiction to our findings, however, Ref. [34] refers to the *global* input state, that for the class of protocols we consider would be $\rho_{AB_1, \dots, B_{N-1}}^{\otimes n}$, where n is the number of rounds. Since the set of biseparable states is not closed under tensor product, the global input state can be GME even if the single copy of the state is biseparable. Here we focus on analyzing the entanglement properties of the single copy of the states. This is because we consider a class of protocols in which the states are distributed and measured at each round, therefore, no storage or quantum global operation on all the copies is required.

FIG. 3. Plot of the asymptotic key rate of the N-BB84 protocol for the state of Eq. (7) undergoing local depolarizing noise (solid lines), as a function of the depolarizing channel parameter p , for fixed $N = 6$ and different k : $k = 4$ (blue, left) and $k = 5$ (green, right). The results are compared with the key rate of a concatenation of noisy bipartite BB84 QKD protocols (red dashed line).

V. CKA AND ENTANGLEMENT WITNESSES

Theorem 1 provides us with a necessary condition to obtain a nonzero key rate in a CKA protocol. We now want to extend to the multipartite scenario the bipartite result presented in Ref. [7]: no secret key can be extracted in a QKD protocol unless Alice and Bob are able to witness entanglement in the shared state using the measurements performed in the protocol. An entanglement witness [31,35,36] is a Hermitian operator W such that $\text{Tr}(W\sigma) \geq 0$ for all separable states σ and $\text{Tr}(W\rho) < 0$ for at least one entangled state ρ . This definition of an entanglement witness is based on the fact that the set of separable states is closed and convex, and can thus be separated with a hyperplane from its complement [35,37]. In the multipartite scenario, given the more intricate structure of possible correlations, witnesses can be defined to distinguish different classes of states [31]. We thus consider the same approach of Ref. [7], Theorem 1: Starting from the measurements performed by the parties, we analyze the entanglement witnesses that can be constructed with them. We obtain the following theorem.

Theorem 3. Given a CKA protocol in which the parties use a set of local measurements, for the test and key generation rounds, which are represented by the Positive Operator-Valued Measures (POVMs) $\{G_x^a\}, \{G_{y_1}^{b_1}\}, \dots, \{G_{y_{N-1}}^{b_{N-1}}\}$, where $a, b_1, \dots, b_{N-1}$ indicate the outputs of the measurements labeled by $x, y_1, \dots, y_{N-1}$, then one can obtain a nonzero asymptotic conference key rate $r^{\infty} > 0$ only if the presence of entanglement can be proved across any partition of the parties into two subsets.

Moreover, the presence of entanglement across each bipartition can be verified through a set of entanglement witnesses of the form

$$W_{\alpha} = \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{(\alpha)} G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}}, \quad (9)$$

FIG. 4. Schematic representation of the set of tripartite states, adapted from Ref. [38]. In light blue (outer set) is represented the set of GME states. In red (dark grey area) is highlighted the set of biseparable states that are not separable with respect to any fixed partition, whereas in yellow (light grey) are represented the sets of states that are separable with respect to a fixed partition. In the middle, in green, is represented the set of fully separable states. A linear witness defines a hyperplane in the space of states. A nonzero conference key rate can be seen as a nonlinear entanglement witness, as it can detect states in the red area, i.e., outside a nonconvex set.

where α labels the partition $S_{\alpha}|\bar{S}_{\alpha}$ with S_{α} being a proper subset of the parties and $\bar{S}_{\alpha}$ is its complement, and where $c_{x, y_1, \dots, y_{N-1}}^{(\alpha)}$ are real coefficients.

The proof is given in Appendix D. Theorem 3 implies that entanglement across any bipartition can be witnessed using the statistics of results of the measurements specified by the protocol, since the witness operators W_{α} are constructed from the POVM elements of these measurements. Theorem 3, combined with the results of the previous section, leads to the following Corollary.

Corollary 3.1. The figure of merit $r^{\infty} > 0$ is a nonlinear entanglement witness, detecting the presence of entanglement across any bipartition of the parties.

This corollary is due to the result of Theorem 3 in combination with the examples presented in the previous section: In fact, the union of all the sets of states that are separable with respect to a specific partition is not a convex set and thus cannot be separated by linear witnesses from its complement [35] (see Fig. 4). Moreover, if a CKA protocol is performed and a nonzero key rate is obtained, it is a necessary condition that the state shared by the parties is not separable across any partition of the parties. Therefore, a nonzero key rate reveals that the state utilized in the protocol is outside of the union of the sets of states that are separable with respect to a fixed partition. Finally, the results of the previous section tell us that non-GME states can also lead to a nonzero conference key, thus allowing us to conclude that the witness cannot be linear, hence the corollary.

VI. CONCLUSIONS

We addressed the question of whether GME is a necessary resource for a CKA protocol. We proved that, surprisingly, the parties can establish a conference key by sharing biseparable

states in each round of the protocol. To show this, we exhibited a family of suitable biseparable states, which lead to nonzero key rates in the simple N-BB84 CKA protocol. We showed that, in a network with bottleneck, the key rates achieved by our family of states outperform protocols based on a concatenation of bipartite QKD, especially for high numbers of entangled parties.

Furthermore, we related our results to the concept of entanglement witnesses, showing that a nonzero asymptotic conference key rate can only be obtained if one is able to detect entanglement, across any partition, in the state shared by the parties in each round of the CKA protocol. This extends the result of Ref. [7] for bipartite QKD to the multipartite scenario. As a consequence, we can infer that a nonzero asymptotic conference key rate represents a nonlinear entanglement witness, which can detect a type of entanglement that cannot be detected by the traditional linear entanglement witnesses.

Given our results, several lines of research can follow. For example, it is known that distillation of GHZ states starting from biseparable states is possible [31]. Moreover, the GHZ state can be used to generate a perfect conference key. It is an open question whether the considered class of CKA protocols is equivalent to the distillation of a GHZ state from biseparable states. Another open point is to establish converse bounds on the key rates achievable by different classes of multipartite entangled states for such simple CKA protocols. Finally, an interesting topic for further investigation is the consequence of our results for experimental implementations. An analysis tailored to particular setups and noise models could determine the payoff of using biseparable states to establish a conference key.

ACKNOWLEDGMENTS

We thank F. Grasselli for helpful discussions, and S. Das, S. Bäuml, M. Winczewski, and K. Horodecki for clarifying discussions about of the apparent contradiction of our results with Ref. [34]. We also thank an anonymous referee for valuable comments that inspired us to strengthen our results. This work was funded by the Deutsche Forschungsgemeinschaft (DFG) (the German Research Foundation) under Germany's Excellence Strategy–Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1–390534769.

APPENDIX A: CONFERENCE KEY RATE OF THE N-BB84 PROTOCOL WITH THE FAMILY OF STATES $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$

As a first step, we briefly sketch the N-BB84 protocol introduced in Ref. [14]. The protocol consists of the following steps:

- (1) A source distributes a state to the N parties.
- (2) The parties perform two type of measurements: For the parameter estimation rounds, they make measurements in the X basis. For the key generation rounds, they make measurements in the Z basis.
- (3) The parties compute the following parameters:

- (a) Using the outcomes of the parameter estimation rounds the parties compute

$$Q_X = \frac{1 - \langle X^{\otimes N} \rangle}{2}, \quad (A1)$$

where $\langle X^{\otimes N} \rangle$ is the expectation value of the operator X for each party. Q_X represents the probability that the parties obtain an unexpected result from the parameter estimation rounds.

- (b) Using some of the outcomes of the key generation estimation rounds, the parties compute

$$Q_{AB_i} = \frac{1 - \langle Z_{AB_i} \rangle}{2}, \quad (A2)$$

where $\langle Z_{AB_i} \rangle$ is the expectation value of the operator Z for Alice and Bob B_i . This parameter is computed for each Bob and represents the probability that Alice and Bob B_i get a discordant outcome in the key generation rounds.

- (4) The asymptotic key rate is given by

$$r_{N\text{-BB84}}^\infty = 1 - h(Q_X) - \max_i h(Q_{AB_i}), \quad (A3)$$

where $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy.

To evaluate the performance of the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, Eq. (7), we need to evaluate the two parameters Q_X and Q_{AB_i} . It can be straightforwardly seen that $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, for all N and k is invariant under the application of the X operator on all parties. This implies $\langle X^{\otimes N} \rangle = 1$ and thus $Q_X = 0$ for any N and k .

To calculate $\langle Z_{AB_i} \rangle$, we remark that $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$ is a mixture of $\mathcal{N} = \binom{N-1}{k-1}$ terms, where each of these terms is a projector onto the GHZ state shared by Alice and $k-1$ Bobs, and a projector onto the $|+\rangle$ -state for the remaining Bobs. It is straightforward to see that $\langle Z_{AB_i} \rangle = 0$ for the terms in which Bob B_i is not entangled with Alice. On the other hand, the terms in which Bob B_i shares part of the GHZ state with Alice are invariant under the application of the Z operator on Alice and Bob B_i , so we obtain $\langle Z_{AB_i} \rangle = 1$ for these terms. Overall, the expectation value $\langle Z_{AB_i} \rangle$ reads

$$\langle Z_{AB_i} \rangle = \frac{f}{\mathcal{N}} = \frac{k-1}{N-1}, \quad (A4)$$

where $f = \binom{N-2}{k-2}$ is the number of terms in which Bob B_i shares part of a GHZ state with Alice. We remark that, due to the symmetry of the state, this result holds for any Bob. Thus, dropping the index i we obtain

$$Q_{AB}(N, k) = \frac{N-k}{2(N-1)}. \quad (A5)$$

With further, straightforward calculations, we obtain

$$\begin{aligned} r_{N\text{-BB84}}^\infty(N, k) &= 1 - h(Q_{AB}) = \frac{1}{2} \frac{N-k}{N-1} \log_2 \left(\frac{N-k}{N-1} \right) \\ &\quad + \frac{1}{2} \frac{N+k-2}{N-1} \log_2 \left(\frac{N+k-2}{N-1} \right). \end{aligned} \quad (A6)$$

APPENDIX B: THE N-BB84 PROTOCOL IS OPTIMAL FOR Z MEASUREMENTS

In this Appendix, we prove that the N-BB84 protocol is the optimal protocol for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, when the parties use the Z basis for key generation. We prove this by analyzing the general class of protocol presented in the Introduction of the paper, thus assuming full state characterization. We show that the key rate of the N-BB84 protocol is identical to the one obtained assuming full tomography of the states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, thus proving that the N-BB84 protocol is optimal for this family of states.

1. Conditional entropy $H(X|E)$ for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$

Here we will calculate the conditional entropy $H(X|E)$ for a generalization of the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, as we consider states of the form

$$\rho_{AB_1, \dots, B_{N-1}} = \sum_{\alpha \in \mathcal{S}^{(k)}} q_{\alpha} \Phi_{S_{\alpha}}^{\text{GHZ},k} \bigotimes_{B_m \in S_{\alpha}} |+\rangle_{B_m} \langle +|, \quad (\text{B1})$$

$$\begin{aligned} \rho_{XB_1, \dots, B_{N-1}E} = \sum_{\substack{\alpha, \beta \\ S_{\alpha}, S_{\beta} \in \mathcal{S}^{(k)}}} \frac{1}{2} \sqrt{q_{\alpha} q_{\beta}} & \left(|0\rangle_X \langle 0| \bigotimes_{B_m \in I_{\alpha, \beta}} |0\rangle_{B_m} \langle 0| \bigotimes_{B_r \in \bar{U}_{\alpha, \beta}} |+\rangle_{B_r} \langle +| \bigotimes_{B_t \in S_{\alpha} \setminus I_{\alpha, \beta}} |0\rangle_{B_t} \langle +| \bigotimes_{B_l \in S_{\beta} \setminus I_{\alpha, \beta}} |+\rangle_{B_l} \langle 0| \otimes |e_{\alpha}\rangle \langle e_{\beta}| \right. \\ & \left. + |1\rangle_X \langle 1| \bigotimes_{B_m \in I_{\alpha, \beta}} |1\rangle_{B_m} \langle 1| \bigotimes_{B_r \in \bar{U}_{\alpha, \beta}} |+\rangle_{B_r} \langle +| \bigotimes_{B_t \in S_{\alpha} \setminus I_{\alpha, \beta}} |1\rangle_{B_t} \langle +| \bigotimes_{B_l \in S_{\beta} \setminus I_{\alpha, \beta}} |+\rangle_{B_l} \langle 1| \otimes |e_{\alpha}\rangle \langle e_{\beta}| \right), \quad (\text{B3}) \end{aligned}$$

where $I_{\alpha, \beta} = (S_{\alpha} \cap S_{\beta})$ is the intersection and $U_{\alpha, \beta} = S_{\alpha} \cup S_{\beta}$ the union between the subsets of the Bobs in S_{α} and S_{β} , $\bar{U}_{\alpha, \beta}$ is the complement of $U_{\alpha, \beta}$, and $\rho_{XB_1, \dots, B_{N-1}E}$ indicates the state after Alice's measurement. We can then trace out all the Bobs, which leaves us with Alice and Eve's reduced state in the form

$$\begin{aligned} \rho_{XE} &= \sum_{\alpha, \beta} \frac{1}{2} \frac{\sqrt{q_{\alpha} q_{\beta}}}{2^{k-s_{\alpha, \beta}}} |0\rangle_X \langle 0| \otimes |e_{\alpha}\rangle \langle e_{\beta}| + \sum_{\alpha, \beta} \frac{1}{2} \frac{\sqrt{q_{\alpha} q_{\beta}}}{2^{k-s_{\alpha, \beta}}} |1\rangle_X \langle 1| \otimes |e_{\alpha}\rangle \langle e_{\beta}| \\ &= \sum_{\alpha, \beta} E_{\alpha, \beta} \frac{1}{2} (|0\rangle_X \langle 0| + |1\rangle_X \langle 1|) \otimes |e_{\alpha}\rangle \langle e_{\beta}| \\ &= \frac{\mathbb{1}_X}{2} \otimes \rho_E, \quad (\text{B4}) \end{aligned}$$

where $s_{\alpha, \beta}$ is the cardinality of $I_{\alpha, \beta}$, where we defined $E_{\alpha, \beta} = \frac{\sqrt{q_{\alpha} q_{\beta}}}{2^{k-s_{\alpha, \beta}}}$ in the second line of the equation and where $\rho_E = \sum_{\alpha, \beta} E_{\alpha, \beta} |e_{\alpha}\rangle \langle e_{\beta}|$ is Eve's reduced state. Finally, since ρ_{XE} is a product state, we can use Property 1 of the conditional entropy to write $H(X|E) = H(X) = 1$, thus concluding the proof.

2. Conference key rates for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$

We now evaluate the analytical expression for the asymptotic key rate for the family of biseparable states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, given by Eq. (7) in the main text. We recall that the number of terms in the convex combination is equal to the number of subsets of cardinality $k-1$ within the $N-1$ Bobs, which is equal to $\mathcal{N} = \binom{N-1}{k-1}$, and that we consider all the coefficients to be equal to $q_{\alpha} = \frac{1}{\mathcal{N}}$.

To calculate the asymptotic key rate, since $H(X|E) = 1$, as proven in Sec. B 1, we need to evaluate the leakage $H(X|Y_i) \forall \text{ Bob}_i$ which, with our choice of coefficients, will be equal for all the Bobs. We thus calculate the reduced density matrix of Alice and Bob_{*i*} after they perform the key generation measurements, ρ_{XY_i} , to estimate the leakage term. Tracing out all the Bobs except one and performing the measurements both on Bob_{*i*} and Alice's side gives us the state

$$\rho_{XY_i} = \frac{1}{2} \frac{f}{\mathcal{N}} (|0\rangle_X \langle 0| \otimes |0\rangle_{Y_i} \langle 0| + |1\rangle_X \langle 1| \otimes |1\rangle_{Y_i} \langle 1|) + \left(1 - \frac{f}{\mathcal{N}}\right) \frac{\mathbb{1}_{XY_i}}{4}, \quad (\text{B5})$$

where $\Phi_{S_{\alpha}}^{\text{GHZ},k} = |\text{GHZ}\rangle \langle \text{GHZ}|_{S_{\alpha}}$ is the projector of the GHZ state shared by the parties of the subset S_{α} , defined as $|\text{GHZ}\rangle_{S_{\alpha}} = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes k} + |1\rangle^{\otimes k})$ and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We substituted $\frac{1}{\mathcal{N}}$ with some general real coefficients q_{α} such that $q_{\alpha} \geq 0 \forall \alpha$ and $\sum_{\alpha} q_{\alpha} = 1$.

We start the explicit calculation of the conditional entropy $H(X|E)$ by writing a purification of the state in Eq. (B1). An explicit valid purification of the state is given by

$$|\psi_{AB_1, \dots, B_{N-1}E}\rangle = \sum_{\alpha \in \mathcal{S}^{(k)}} \sqrt{q_{\alpha}} |\text{GHZ}\rangle_{S_{\alpha}} \bigotimes_{B_m \in S_{\alpha}} |+\rangle_{B_m} |e_{\alpha}\rangle, \quad (\text{B2})$$

where $\{|e_{\alpha}\rangle\}_{\alpha}$ is an orthonormal basis of Eve's subsystem of proper dimension. We thus look at the state after Alice performs her measurements on the Pauli Z basis. We obtain the following explicit expression of the state:

where f is the number of terms in which Bob_i is entangled with Alice in the original state. The number f can be expressed in term of k and N as $f = \binom{N-2}{k-2}$. Thus the reduced density matrix in the computational basis has the form

$$\rho_{XY_i} = \begin{bmatrix} \frac{1}{4}(1 + C_{N,k}) & 0 & 0 & 0 \\ 0 & \frac{1}{4}(1 - C_{N,k}) & 0 & 0 \\ 0 & 0 & \frac{1}{4}(1 - C_{N,k}) & 0 \\ 0 & 0 & 0 & \frac{1}{4}(1 + C_{N,k}) \end{bmatrix}, \quad (\text{B6})$$

where $C_{N,k} = \frac{f}{N} = \frac{k-1}{N-1}$. Note that the reduced density matrix of Bob_i after the measurement is $\rho_{Y_i} = \frac{\mathbb{I}_{Y_i}}{2}$. We therefore obtain

$$\begin{aligned} r^\infty(N, k) &= 1 - H(XY_i) + H(Y_i) \\ &= \frac{1}{2} \frac{N-k}{N-1} \log_2 \left(\frac{N-k}{N-1} \right) + \frac{1}{2} \frac{N+k-2}{N-1} \log_2 \left(\frac{N+k-2}{N-1} \right). \end{aligned} \quad (\text{B7})$$

The key rate obtained with this method is equivalent to Eq. (A6), thus proving that the N-BB84 protocol is optimal for Z -basis measurements for the key generation rounds.

APPENDIX C: NOISE ANALYSIS FOR THE N-BB84 PROTOCOL

In this Appendix, we consider a noise model for the N-BB84 protocol with the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$ and compare its performance with a concatenation of bipartite QKD protocols between Alice and $N-1$ Bobs, where all the channels between Alice and the Bobs are noisy. For a fair comparison, we thus consider local depolarizing noise. This corresponds to applying the map

$$\mathcal{D}[\rho] = (1-p)\rho + p\frac{\mathbb{I}}{2} \quad (\text{C1})$$

to each of the Bobs. The state we will consider will thus be

$$\rho_{AB_1, \dots, B_{N-1}}^{\text{noise}} = \mathcal{D}^{\otimes(N-1)}[\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}]. \quad (\text{C2})$$

In this scenario, the parameters of the N-BB84 protocol can be analytically evaluated and read

$$Q_x = \frac{1 - (1-p)^{N-1}}{2}, \quad (\text{C3})$$

$$Q_{AB} = \frac{N-1 - (1-p)(k-1)}{2(N-1)}, \quad (\text{C4})$$

where, again, we dropped the index i since, due to the symmetry of the state, all Q_{AB_i} are equal. We thus can evaluate analytically the key rate for the N-BB84 protocol, which reads

$$\begin{aligned} r_{N\text{-BB84}}^\infty(N, k, p) &= \frac{1}{2} (1 - (1-p)^{N-1}) \log_2 (1 - (1-p)^{N-1}) \\ &+ \frac{1}{2} (1 + (1-p)^{N-1}) \log_2 (1 + (1-p)^{N-1}) \\ &+ \frac{N-1 - (1-p)(k-1)}{2(N-1)} \\ &\times \log_2 \left(\frac{N-1 - (1-p)(k-1)}{2(N-1)} \right) \\ &+ \frac{N-1 + (1-p)(k-1)}{2(N-1)} \log_2 \left(\frac{N-1 + (1-p)(k-1)}{2(N-1)} \right). \end{aligned} \quad (\text{C5})$$

We compare it with the scenario where Alice performs a bipartite BB84 protocol with each of the Bobs, sharing a maximally entangled state mixed with white noise, as in Eq. (C1). The resulting key rate of a concatenation of bipartite BB84 protocols reads [3,11]

$$r_{\text{QKD}}^\infty(N) = \frac{1 - 2h(\frac{p}{2})}{N-1}, \quad (\text{C6})$$

where we divide the key rate of the bipartite BB84 protocol in the presence of white noise by the number of times Alice must perform the bipartite protocol to establish a secure key with each of the $N-1$ Bobs. The results are shown in Fig. 5. We can see that for some regimes, the N-BB84 protocol outperforms a concatenation of bipartite QKD protocols: For a low number of parties, we can obtain a marked advantage for k close to N in the low noise regime. Moreover, increasing the number of parties increases the advantage obtained and the range of k for which we can obtain it. However, we note that the N-BB84 protocol has a lower noise tolerance than the concatenation of bipartite QKD protocols, and thus for high noise regimes the latter is always preferred.

APPENDIX D: PROOF OF THEOREM 3

We give here the full proof of Theorem 3. For completeness, we repeat the statement of the theorem.

Theorem 3. Given a CKA protocol in which the parties use a set of local measurements, for the test and key generation rounds, which are represented by the POVMs $\{G_x^a\}, \{G_{y_1}^{b_1}\}, \dots, \{G_{y_{N-1}}^{b_{N-1}}\}$, where $a, b_1, \dots, b_{N-1}$ indicate the outputs of the measurements labeled by $x, y_1, \dots, y_{N-1}$, then one can obtain a nonzero asymptotic conference key rate $r^\infty > 0$ only if the presence of entanglement can be proved across any partition of the parties.

Moreover, the presence of entanglement across each partition can be verified through a set of entanglement witnesses of the form

$$W_\alpha = \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{(\alpha)} G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}}, \quad (\text{D1})$$

where α labels the partition $S_\alpha | \bar{S}_\alpha$ with S_α being a proper subset of the parties and $\bar{S}_\alpha$ is its complement, and where $c_{x, y_1, \dots, y_{N-1}}^{(\alpha)}$ are real coefficients.

FIG. 5. Left panel: Plot of the asymptotic key rate of the N-BB84 protocol for the state of Eq. (C2) (solid lines) as a function of p , for fixed $N = 6$ and different k : $k = 4$ (blue, left) and $k = 5$ (green, right). The results are compared with the key rate of a concatenation of BB84 QKD protocols, given in Eq. (C6) (red dashed line), for $N = 6$, as a function of p . Right panel: Plot of the asymptotic key rate of the N-BB84 protocol for the state of Eq. (C2) (solid lines) as a function of p , for a fixed value of $N = 13$ and different values of k : $k = 7$ (blue, left), $k = 9$ (green, middle) and $k = 11$ (black, right). The results are compared with the key rate of a concatenation of BB84 QKD protocols, given in Eq. (C6) (red dashed line), for $N = 13$, as a function of p .

proof. We start by focusing on the probability distribution of the outcomes $a, b_1, \dots, b_{N-1}$ given the inputs $x, y_1, \dots, y_{N-1}$ of the measurements that can be performed in the test and key generation rounds of the CKA protocol, namely, $P(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1})$. The probability distributions are obtained as

$$P(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1}) = \text{Tr}(G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}} \rho_{AB_1 \dots B_{N-1}}), \quad (\text{D2})$$

where G_x^a , $G_{y_i}^{b_i}$ are the POVM elements of the measurements performed by Alice and Bob _{i} , respectively.

We analyze the map that maps each state into the corresponding probability distribution, given the measurements of the protocol, that is,

$$\Pi_{\text{CKA}} : \rho_{AB_1 \dots B_{N-1}} \mapsto \{P(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1})\}. \quad (\text{D3})$$

Considering a subset of the Hilbert space, namely, Σ , we call Σ^Π the projection of the subset Σ through the map Π_{CKA} , defined as in Eq. (D2). We now denote the set of states separable across the partition $S_\alpha | \bar{S}_\alpha$ as Σ_α . We note that Σ_α is a closed and convex set. Furthermore, the projection

of the set Σ_α through the linear map Π_{CKA} , namely, Σ_α^Π is still a closed and convex set. The elements of the projected set represent the probability distributions that come from states that are separable across the partition $S_\alpha | \bar{S}_\alpha$. Due to Theorem 1, a necessary condition to obtain a nonzero key rate is that the state is not separable with respect to any partition. This implies that, given a state $\rho_{A, B_1, \dots, B_{N-1}}^*$ that leads to a nonzero key rate in a specific protocol, the corresponding probability distribution $P^*(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1})$ is such that $P^*(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1}) \notin \Sigma_\alpha^\Pi \forall \alpha$. Moreover, since each Σ_α^Π is a convex and compact set, it is a well-known fact that each element of its complement $\bar{\Sigma}_\alpha^\Pi$ can be separated from Σ_α^Π with a proper hyperplane [35,37]. In the probability space, any hyperplane can be defined as

$$\sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}} P(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1}) = 0, \quad (\text{D4})$$

where $c_{x, y_1, \dots, y_{N-1}}^{a, b_1, \dots, b_{N-1}}$ are real coefficients. Furthermore, for each probability distribution $P^*(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1}) \notin \Sigma_\alpha^\Pi \forall \alpha$, we can find, for each partition $S_\alpha | \bar{S}_\alpha$, coefficients $c_{x, y_1, \dots, y_{N-1}}^{(\alpha), a, b_1, \dots, b_{N-1}}$, defining hyperplanes such that

$$\forall P_\alpha(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1}) \in \Sigma_\alpha^\Pi \quad \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{(\alpha)} P_\alpha(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1}) \geq 0 \quad \text{and}$$

$$\text{for } P^*(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1}) \notin \Sigma_\alpha^\Pi \forall \alpha, \quad \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{(\alpha)} P^*(a, b_1, \dots, b_{N-1} | x, y_1, \dots, y_{N-1}) < 0. \quad (\text{D5})$$

Finally, the coefficients define a set of entanglement witnesses in the form

$$W_\alpha = \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{(\alpha), a, b_1, \dots, b_{N-1}} G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}}, \quad (\text{D6})$$

such that, due to Eq. (D5), for each α :

$$\begin{aligned} \text{Tr}(W_\alpha \sigma_\alpha) &\geq 0, \quad \forall \sigma_\alpha \in \Sigma_\alpha \\ \text{Tr}(W_\alpha \rho_{A, B_1, \dots, B_{N-1}}^*) &< 0. \end{aligned} \quad (\text{D7})$$

As a matter of fact, Eq. (D7) tells us that the operator W_α is an entanglement witness [31,35] that detects entangle-

ment across partition $S_\alpha|\bar{S}_\alpha$. This concludes the proof of the theorem.

-
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
 - [2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
 - [4] H.-K. Lo, Proof of unconditional security of six-state quantum key distribution scheme, *Quantum Info. Comput.* **1**, 81 (2001).
 - [5] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, *Phys. Rev. Lett.* **81**, 3018 (1998).
 - [6] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography Without Bell's Theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
 - [7] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, *Phys. Rev. Lett.* **92**, 217903 (2004).
 - [8] C. Elliott, Building the quantum network, *New J. Phys.* **4**, 46 (2002).
 - [9] M. Geihs, O. Nikiforov, D. Demirel, A. Sauer, D. Butin, F. Günther, G. Alber, T. Walther, and J. Buchmann, The status of quantum-key-distribution-based long-term secure internet communication, *IEEE Trans. Sustain. Comput.*, 19 (2019).
 - [10] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, *et al.*, Satellite-Relayed Intercontinental Quantum Network, *Phys. Rev. Lett.* **120**, 030501 (2018).
 - [11] 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).
 - [12] A. Cabello, Multiparty key distribution and secret sharing based on entanglement swapping, *arXiv:quant-ph/0009025*.
 - [13] K. Chen and H.-K. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states, *Quantum Info. Comput.* **7**, 689 (2007).
 - [14] F. Grasselli, H. Kampermann, and D. Bruß, Finite-key effects in multipartite quantum key distribution protocols, *New J. Phys.* **20**, 113014 (2018).
 - [15] F. Grasselli, H. Kampermann, and D. Bruß, Conference key agreement with single-photon interference, *New J. Phys.* **21**, 123002 (2019).
 - [16] J. Ribeiro, G. Murta, and S. Wehner, Fully device-independent conference key agreement, *Phys. Rev. A* **97**, 022307 (2018).
 - [17] J. Ribeiro, G. Murta, and S. Wehner, Reply to 'Comment on 'fully device-independent conference key agreement'', *Phys. Rev. A* **100**, 026302 (2019).
 - [18] T. Holz, D. Miller, H. Kampermann, and D. Bruß, Comment on 'Fully device-independent conference key agreement,' *Phys. Rev. A* **100**, 026301 (2019).
 - [19] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, Continuous-variable measurement-device-independent multipartite quantum communication, *Phys. Rev. A* **93**, 022325 (2016).
 - [20] Z. Zhang, R. Shi, and Y. Guo, Multipartite continuous variable quantum conferencing network with entanglement in the middle, *Appl. Sci.* **8**, 1312 (2018).
 - [21] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, Modular network for high-rate quantum conferencing, *Commun. Phys.* **2** (2019).
 - [22] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement, *arXiv:2002.01491*.
 - [23] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, *Adv. Quantum Technol.* **3**, 2000025 (2020).
 - [24] R. Renner, Security of quantum key distribution, *arXiv:quant-ph/0512258*.
 - [25] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. A* **461** (2005).
 - [26] M. Tomamichel, *Quantum Information Processing with Finite Resources* (Springer, Cham, 2016).
 - [27] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, *Rev. Mod. Phys.* **81**, 865 (2009).
 - [28] M. Walter, D. Gross, and J. Eisert, Multi-partite entanglement *arXiv:1612.02437*.
 - [29] F. Clivaz, M. Huber, L. Lami, and G. Murta, Genuine-multipartite entanglement criteria based on positive maps, *J. Math. Phys.* **58**, 082201 (2017).
 - [30] N. Friis, G. Vitagliano, M. Malik, and M. Huber, Entanglement certification from theory to experiment, *Nat. Rev. Phys.* **1**, 72 (2019).
 - [31] O. Gühne and G. Tóth, Entanglement detection, *Phys. Rep.* **474**, 1 (2009).
 - [32] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Going beyond Bell's theorem *arXiv:0712.0921*.
 - [33] W. Dür, G. Vidal, and J. I. Cirac, Three qubits can be entangled in two inequivalent ways, *Phys. Rev. A* **62**, 062314 (2000).
 - [34] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal limitations on quantum key distribution over a network *arXiv:1912.03646*.
 - [35] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: Necessary and sufficient conditions, *Phys. Lett. A* **223**, 1 (1996).
 - [36] B. M. Terhal, Detecting quantum entanglement, *Theor. Comput. Sci.* **287**, 313 (2002), natural Computing.
 - [37] R. E. Edwards, *Functional Analysis, Theory and Application* (Holt, Rinehart and Winston, New York, 1965).
 - [38] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Classification of Mixed Three-Qubit States, *Phys. Rev. Lett.* **87**, 040401 (2001).