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

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 (2004) [1]. 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 non-zero 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 non-zero conference key can be interpreted as a non-linear entanglement witness that detects a class of states which cannot be detected by usual linear entanglement witnesses.

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 [2,3] entanglement plays a crucial role in the security proofs [4,5]. Indeed, even prepare-and-measure protocols [2,6], which do not require any entanglement for their implementation, have an entanglement-based counterpart [2] which can be used for the protocol’s security analysis. In Ref. [1], 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 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. 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 principle 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, in order to obtain a non-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. [1] to the multipartite scenario.

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,..., BobN−1. Upon receiving the systems, the parties perform local measurements and record the classical outcome.

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 post-processing (parameter estimation, one-way information reconciliation and privacy amplification) as [13]

\[ r_\infty = \max \left[ 0, H(X|E) - \max_i H(X|Y_i) \right], \]

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 \( H(X|E) = H(X|E) - H(E) \) is the von Neumann entropy of Alice’s outcome in the key generation rounds, conditioned on Eve’s (possibly quantum) side information. \( H(X|Y_i) = H(X|Y_i) - H(Y_i) \) represents the amount of information Alice needs to communicate to Bob_i so that 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 \( \rho_X \) of a system X, the quantum von Neumann entropy is defined as \( H(X) = -\text{Tr}[\rho_X \log \rho_X] \).

The conditional von Neumann entropy satisfy 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 \( \rho_{AB} \) then \( H(A|BC) \leq H(A|B) \).

3. Conditioning on classical information [25 Proposition 5.4]: if \( \rho_{ABF} = \sum_j q_j \rho_{AB}^j \otimes \langle j|F \rangle \) 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 \( \rho_{AB}^j \).

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 [11]. In the multipartite scenario, however, different classes of entanglement can be defined, which have been extensively studied [27,31].

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

\[
\rho_{AB_1...B_{N-1}} = \sum_j q_j \rho_{S_{\alpha}}^j \otimes \rho_{\bar{S}_{\alpha}}^j, \tag{2}
\]

where \( \rho_{S_{\alpha}}^j \) and \( \rho_{\bar{S}_{\alpha}}^j \) are states shared by the parties in \( S_{\alpha} \) 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

\[
\rho_{bs} = \sum_{S_{\alpha}} \sum_j q_j \rho_{S_{\alpha}}^j \otimes \rho_{\bar{S}_{\alpha}}^j, \tag{3}
\]

where the first sum is performed over all proper subsets \( S_{\alpha} \) of the parties. Again, the coefficients must satisfy \( q_j \geq 0 \) \( \forall j \), \( \rho_{S_{\alpha}} \) and \( \sum_j q_j = 1 \). 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].

Entanglement is necessary for CKA – In the following we prove that entanglement across all partitions in the state shared by the parties is necessary in order to lead to a non-zero 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 \( H(X|Y_l) \geq H(X|E) \) for a specific Bob. Let us consider a state separable with respect to a partition \( S_{\alpha}|\bar{S}_{\alpha} \), in the form of Eq. (2), such that \( S_{\alpha} \) contains Alice. We consider a Bob contained in \( S_{\alpha} \), let us say Bob. Let Eve have a purification of the state of the form

\[
|\psi_{AB_1,...,B_{N-1},EFF}\rangle = \sum_j \sqrt{q_j} |\psi_{S_{\alpha},E\alpha}^j \rangle F |j\rangle F', \tag{4}
\]

where \( |\psi_{S_{\alpha},E\alpha}\rangle \) is a purification of \( \rho_{S_{\alpha}}^j \otimes \rho_{E\alpha}^j \) 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, will result in a state of the form

\[
\rho_{AB_1,F} = \sum_j q_j \rho_A^j \otimes \rho_{B_1}^j \otimes |j\rangle \langle j|F, \tag{5}
\]

which is a classical-quantum state consisting of a separable state for Alice and Bob \( B_1 \), 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:

\[
H(X|Y_l) \geq H(X|Y_l|F) \geq \sum_j q_j H(X|Y_l F = j) \geq \sum_j q_j H(X|F = j) = H(X|F) \geq H(X|EFF') = H(X|E_{tot})
\]

where \( E_{tot} \) indicates the global subsystem of Eve, which includes the classical registers. In the first, second and third line we used Property 1, Property 2 and Property 3 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 in order to establish a secret common key. It is worth noting that for \( N = 2 \) this proof simplifies the argumentation given in Ref. [11].

**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 non-zero conference key:

\[
\rho^{(N,k)}_{AB_1,...,B_{N-1}} = \sum_{\alpha \in S^{(k)}_\alpha} \frac{1}{N} \Phi^{GHZ,k}_{S_{\alpha}} \otimes |+\rangle \langle +|B_m, \tag{7}
\]

where \( S^{(k)} \) is the set of subsets of \( k \) parties that contain Alice and \( k - 1 \) Bobs, \( \Phi^{GHZ,k}_{S_{\alpha}} = |GHZ\rangle_{GHZ} \langle GHZ|_{S_{\alpha}} \) is the
projector of the GHZ state shared by the \( k \) parties of the subset \( S_{\alpha} \), defined as \( |GHZ\rangle_{S_{\alpha}} = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes k} + |1\rangle^{\otimes k}) \) and \( |+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \). The normalization factor is equal to \( N = \binom{N-1}{k-1} \) 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.

If the parties perform measurements in the \( Z \) basis for key generation, we can show that this class of states always leads to \( H(X|E) = 1 \). The reason is that the reduced density matrix, describing Alice and Eve’s state after the measurement, has the form \( \rho_{XE} = \frac{1}{2} \rho_A \otimes \rho_E \), where \( \rho_E \) is Eve’s reduced state. Thus, using Property 1 of the conditional entropy we have \( H(X|E) = H(X) = 1 \). The detailed proof can be found in the Supplemental Material.

We calculate the asymptotic conference key rate for the family of states \( \rho_{(N,k)}^{(N,k)} \), Eq. (7), as a function of the total number of parties \( N \) and the number of parties that are entangled \( k \) (for details, see the Supplemental Material):

\[
r_{\infty}(N, k) = \frac{1}{2} \log_2 \left( \frac{N - k}{N - 1} \right) + \frac{1}{2} \log_2 \left( \frac{N + k - 2}{N - 1} \right).
\] (8)

We remark that we have assumed a full characterization of the state, which can be achieved, e.g., if the parties perform measurements in all the Pauli bases during the test rounds of the CKA protocol. In Figure 1, we show the secret key rate as a function of the number of parties \( N \) for different values of the number of entangled parties \( k \). We conclude that it is indeed possible to obtain a non-zero asymptotic secret key rate from a biseparable state.

Figure 2 illustrates the behavior of the asymptotic key rate for the family of states \( \rho_{(N,k)}^{(N,k)} \), Eq. (7), for different functions \( k(N) \). The plots show that if \( k \) is a linear function of \( N \), the asymptotic key rate reaches a finite value, whereas for \( k = \sqrt{N} \) the key rate drops asymptotically to zero as \( N \) increases.

We have also analyzed the previously introduced protocols that generalize the six-state [33] and the BB84 [14] protocols to the multipartite scenario. Using the criterion introduced in Ref. [34], we can exhibit a family of biseparable states that yield a non-zero key rate in these simple protocols. The full analysis can be found in the Supplemental Material.

Our results show that CKA without GME states is possible. We remark that in Ref. [35] the authors have established that GME is a necessary condition for non-zero key in a one-shot conference key agreement protocol. This result, at first, seems in contradiction to our findings, however Ref. [35] refers to the global input state, that for the class of protocols we consider would be \( \rho_{AB_{1},...,B_{N-1}} \), 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 analysing 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.

**CKA and entanglement witnesses** – Theorem 1 provides us with a necessary condition to obtain a non-zero key rate in a CKA protocol. We now want to extend to the multipartite scenario the bipartite result presented in Ref. 11: 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, 36, 37] is a Hermitian operator \( W \) such that \( \text{Tr}(W\sigma) \geq 0 \) for all

---

**Figure 1.** Asymptotic secret key rate for the state of Eq. (7) as a function of \( N \) for different values of \( k \). We remark that since \( k \leq N - 1 \), the curves start at different values of \( N \).

**Figure 2.** Asymptotic secret key rate for the state of Eq. (7) as a function of \( N \), with \( k \) depending differently on \( N \).
separable states \( \sigma \) and \( \text{Tr}(W \rho) < 0 \) for at least one entangled state \( \rho \). 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 \([36,38]\). 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. \([1, Theorem 1]\): 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 2.** 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 \( \{G^a_2\}, \{G^b_1\}, \ldots, \{G^{b_{N-1}}_{y_{N-1}}\} \), where \( a, b_1, \ldots, b_{N-1} \) indicate the outputs of the measurements labeled by \( x, y_1, \ldots, y_{N-1} \), then one can obtain a non-zero 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 bi-partition can be verified through a set of entanglement witnesses of the form

\[
W_\alpha = \sum_{x, y_1, \ldots, y_{N-1}, a, b_1, \ldots, b_{N-1}} c^{(\alpha)}_{x, y_1, \ldots, y_{N-1}} G^a_2 \otimes G^{b_1}_{y_1} \otimes \cdots \otimes G^{b_{N-1}}_{y_{N-1}}
\]

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

The proof is given in the Supplemental Material. Theorem 2 implies that entanglement across any bi-partition can be witnessed using the statistics of results of the measurements specified by the protocol, since the witness operators \( W_\alpha \) are constructed from the POVM elements of these measurements. Theorem 2 combined with the results of the previous Section, leads to the following Corollary.

**Corollary 2.1.** The figure of merit \( r_\infty > 0 \) is a non-linear entanglement witness, detecting the presence of entanglement across any bi-partition of the parties.

This corollary is due to the result of Theorem 2 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 \([36]\) (see Figure 3). Moreover, if a CKA protocol is performed and a non-zero 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 non-zero 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 non-zero conference key, thus allowing us to conclude that the witness cannot be linear, hence the corollary.

**Conclusions** – We addressed the question of whether GME is a necessary resource for a conference key agreement 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. Moreover, we proved that no conference key can be extracted if the state is separable with respect to any partition of the parties. We remark that our results can have direct implications to experimental implementations, as we have shown an explicit way to obtain a conference key using biseparable states, which are much less costly to produce. Further investigation is required to determine the noise tolerance of implementations that aim to produce these states.

Finally, we related our results to the concept of entanglement witness, showing that a non-zero 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. \([1]\) for bipartite QKD to the multipartite scenario. As a consequence, we can infer that a non-zero asymptotic conference key rate represents a non-linear 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 \([31]\). More-

\[\text{GME} \text{ A|BC B|AC \ Fully separable C|AB}\]

Figure 3. (Color online) Schematic representation of the set of tripartite states, adapted from Ref. \([39]\). In blue is represented the set of GME states. In red is highlighted the set of biseparable states that are not separable with respect to any fixed partition, whereas in yellow are represented the sets of states that are separable with respect to a fixed partition. In green is represented the set of fully separable states. A linear witness defines a hyperplane in the space of states. A non-zero conference key rate can be seen as a non-linear entanglement witness, as it can detect states in the red area, i.e. outside a non-convex set.
over, 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. Such a result can lead to converse bounds on the key rates achievable by different classes of multipartite entangled states in the considered CKA protocols.

**Acknowledgements**

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. [35]. This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany’s Excellence Strategy - Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 - 390534769.

[1] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. 92, 217903 (2004).
[2] C. H. Bennett and G. Brassard, Theoretical Computer Science 560, 7 (2014).
[3] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[5] H.-K. Lo, Quantum Inf. Comput. 1, 81 (2001).
[6] D. Bruß, Phys. Rev. Lett. 81, 3018 (1998).
[7] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. 68, 557 (1992).
[8] C. Elliott, New Journal of Physics 4, 46 (2002).
[9] M. Gellm, O. Nikiforov, D. Demirel, A. Sauer, D. Butin, F. Günther, G. Alber, T. Walther, and J. Buchmann, The status of quantum-based long-term secure communication over the internet (2017), arXiv:1711.09793 [cs.CR].
[10] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yinen, L. Zhang, D. Krauch, 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, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, Phys. Rev. Lett. 120, 030501 (2018).
[11] A. Cabello, Multiparty key distribution and secret sharing based on entanglement swapping (2000), arXiv:quant-ph/0009025 [quant-ph].
[12] K. Chen and H.-K. Lo, Multi-party quantum cryptograph protocls with noisy ghz states (2004), arXiv:quant-ph/0404133 [quant-ph].
[13] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, New Journal of Physics 19, 093012 (2017).
[14] F. Grasselli, H. Kampermann, and D. Bruß, New Journal of Physics 20, 113014 (2018).
[15] F. Grasselli, H. Kampermann, and D. Bruß, New Journal of Physics 21, 123002 (2019).
[16] J. Ribeiro, G. Murta, and S. Wehner, Phys. Rev. A 97, 022307 (2018).
[17] J. Ribeiro, G. Murta, and S. Wehner, Phys. Rev. A 100, 062302 (2019).
[18] T. Holz, D. Miller, H. Kampermann, and D. Bruß, Phys. Rev. A 100, 026301 (2019).
[19] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, Phys. Rev. A 93, 022325 (2016).
[20] Z. Zhang, R. Shi, and Y. Guo, Appl. Sci. 8, 1312 (2018).
[21] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, Commun. Phys. 2, 10.1038/s42005-019-0209-6 (2019).
[22] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement (2020), arXiv:2002.01491, arXiv:2002.01491 [quant-ph].
[23] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review (2020), arXiv:2003.10186 [quant-ph].
[24] R. Renner, Security of quantum key distribution (2005), arXiv:quant-ph/0512258 [quant-ph].
[25] I. Devetak and A. Winter, Proc. R. Soc. A. 461, 10.1098/rspa.2004.1372 (2005).
[26] M. Tomamichel, Quantum Information Processing with Finite Resources (Springer, Cham, 2016).
[27] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. 81, 865 (2009).
[28] M. Walter, D. Gross, and J. Eisert, Multi-partite entanglement (2016), arXiv:1612.02437 [quant-ph].
[29] R. Horodecki, M. Horodecki, P. Horodecki, and K. Horodecki, Quantum Conference Key Agreement: A Review (2020), arXiv:2002.01491 [quant-ph].
[30] N. Friis, G. Vitagliano, M. Malik, and M. Huber, Nat Rev Phys 1, 72 (2019).
[31] O. Gühne and G. Tóth, Physics Reports 474, 1 (2009).
[32] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Going beyond bell’s theorem (2007), arXiv:0712.0921 [quant-ph].
[33] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A 62, 062314 (2000).
[34] O. Gühne and M. Seevinck, New Journal of Physics 12, 053002 (2010).
[35] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal limitations on quantum key distribution over a network (2019), arXiv:1912.03646 [quant-ph].
[36] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Letters A 223, 1 (1996).
[37] B. M. Terhal, Theoretical Computer Science 287, 313 (2002) natural Computing.
[38] R. E. Edwards, Functional Analysis, Theory and Application (Holt, Rinehart and Win-ston, New York, 1965).
[39] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. 87, 040401 (2001).
Supplemental Material: Genuine multipartite entanglement is not a precondition for secure conference key agreement

I. CONDITIONAL ENTROPY $H(X|E)$ FOR THE FAMILY OF STATES $\rho_{AB_1,...,B_{N-1}}^{(N,k)}$

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

$$\rho_{AB_1,...,B_{N-1}} = \sum_{\alpha, \beta} q_{\alpha, \beta} \Phi_{S_{\alpha}, S_{\beta}}^{GHZ,k} |+\rangle\langle+|_{B_m}$$  \hspace{1cm} (S1)

where $\Phi_{S_{\alpha}, S_{\beta}}^{GHZ,k}$ is the projector of the GHZ state shared by the parties of the subset $S_{\alpha}$, defined as $\Phi_{S_{\alpha}, S_{\beta}}^{GHZ,k} = \frac{1}{\sqrt{2}} (|0\rangle^\otimes k + |1\rangle^\otimes k)$ and $|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$. We substituted $\frac{1}{X}$ with some general real coefficients $q_{\alpha}$ such that $q_{\alpha} \geq 0$ for all $\alpha$ 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. (S1). An explicit valid purification of the state is given by

$$|\psi_{AB_1,...,B_{N-1}}\rangle = \sum_{\alpha, \beta} \sqrt{q_{\alpha}} |GHZ\rangle_{S_{\alpha}} \otimes |+\rangle_{B_m} |e_{\alpha}\rangle$$  \hspace{1cm} (S2)

where $\{|e_{\alpha}\rangle\}$ 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

$$\rho_{X_{B_1,...,B_{N-1}}E} = \sum_{\alpha, \beta} \frac{1}{2} \sqrt{q_{\alpha}q_{\beta}} |0\rangle_{X} \otimes |0\rangle_{B_m} \otimes |0\rangle_{B_r} \otimes |+\rangle_{B_{r}} \otimes |0\rangle_{B_t} \otimes |+\rangle_{B_{t}} \otimes |+\rangle_{B_{r}} \otimes |e_{\alpha}\rangle \langle e_{\beta}|$$

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 $S_{\alpha}$ and $S_{\beta}$, $U_{\alpha, \beta}$ is the complement of $U_{\alpha, \beta}$ and $\rho_{X_{B_1,...,B_{N-1}}E}$ 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

$$\rho_{XE} = \sum_{\alpha, \beta} \frac{1}{2} \sqrt{q_{\alpha}q_{\beta}} |0\rangle_{X} \otimes |0\rangle_{e_{\alpha}} \otimes |e_{\beta}| = \sum_{\alpha, \beta} \frac{1}{2} \sqrt{q_{\alpha}q_{\beta}} |0\rangle_{X} \otimes |0\rangle_{e_{\alpha}} \otimes |e_{\beta}|$$

where $s_{\alpha, \beta}$ is the cardinality of $I_{\alpha, \beta}$, where we defined $E_{\alpha, \beta} = \frac{1}{2^{s_{\alpha, \beta}}}$ 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 $\rho_{XE}$ 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.

II. CONFERENCE KEY RATES FOR THE FAMILY OF STATES $\rho_{AB_1,...,B_{N-1}}^{(N,k)}$

We now evaluate the analytical expression for the asymptotic key rate for the family of biseparable states $\rho_{AB_1,...,B_{N-1}}^{(N,k)}$, 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 $N = \binom{N-1}{k-1}$, and that we consider all the coefficients to be equal to $q_k = \frac{1}{N}$.

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

$$\rho_{XY_i} = \frac{1}{2N} \left[ \begin{array}{cccc}
\frac{1}{4} & 0 & \frac{1}{4} & 0 \\
0 & C_{N,k} & 0 & 0 \\
0 & 0 & \frac{1}{4}(1 - C_{N,k}) & 0 \\
0 & 0 & 0 & \frac{1}{4}(1 + C_{N,k}) 
\end{array} \right], \quad (S5)$$

where $f$ is the number of terms in which Bob 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

$$\rho_{XY_i} = \frac{1}{2N} \left[ \begin{array}{cccc}
\frac{1}{4} & 0 & \frac{1}{4} & 0 \\
0 & C_{N,k} & 0 & 0 \\
0 & 0 & \frac{1}{4}(1 - C_{N,k}) & 0 \\
0 & 0 & 0 & \frac{1}{4}(1 + C_{N,k}) 
\end{array} \right], \quad (S6)$$

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

$$r_\infty(N, k) = 1 - H(X|Y_i) + H(Y_i) = \frac{1}{2} N - k \log_2 \left( \frac{N - k}{N - 1} \right) + \frac{1}{2} \frac{N + k - 2}{N - 1} \log_2 \left( \frac{N + k - 2}{N - 1} \right). \quad (S7)$$

III. KNOWN CKA PROTOCOLS: MULTIPARTY BB84 [14] AND SIX-STATE [13]

We now consider two well known CKA protocols, namely the generalizations to the multipartite scenario of the BB84 [14] and the six-state [13] protocols. Our aim is to show that, even for these protocols, a secure conference key can also be established using biseparable states.

For that we consider the following $N$-partite state $\frac{3}{4} |\psi_0^+(N)\rangle\langle\psi_0^+(N)| + \frac{1}{4} |\psi_0^-(N)\rangle\langle\psi_0^-(N)|$, where $|\psi_0^\pm(N)\rangle = 1/\sqrt{2} (|0\rangle^\otimes N \pm |1\rangle^\otimes N)$, undergoing a depolarizing noise:

$$\rho_{dep}(p) = (1 - p) \left( \frac{3}{4} |\psi_0^+(N)\rangle\langle\psi_0^+(N)| + \frac{1}{4} |\psi_0^-(N)\rangle\langle\psi_0^-(N)| \right) + \frac{p}{2N} I_N, \quad (S8)$$

where $p \in [0, 1]$.

![Figure S1. Plot of the asymptotic key rate for the state of Eq. (S8) as a function of $p$, for different values of $N$. In solid lines are represented the results for the multipartite 6-state protocol, whereas in dashed lines are represented the results for the multipartite BB84 protocol.](image-url)
A criterion introduced in Ref. [34] provides a necessary and sufficient condition for biseparability of states diagonal in the GHZ basis. Using this criterion, we can establish that the state $\rho_{dep}^{(N)}(p)$, given in Eq. (S8), is biseparable for all $N$ and the whole range of $p$.

In Figure S1 we plot the asymptotic conference key rates achieved by the state $\rho_{dep}^{(N)}(p)$ in the multiparty BB84 [14] and six-state [13] protocols for $N = 3$ and $N = 10$.

The plots show that for both simple protocols a non-zero key rate is achievable with the biseparable state $\rho_{dep}^{(N)}(p)$ for some range of $p$. The asymptotic key rate, however, rapidly drops to zero as the white noise fraction increases.

IV. PROOF OF THEOREM 2

We give here the full proof of Theorem 2. For completeness we repeat the statement of the theorem.

**Theorem 2.** 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 $\{G^a_x\}, \{G^b_y\} \ldots \{G^{b_{N-1}}_{y_{N-1}}\}$, where $a, b_1, \ldots, b_{N-1}$ indicate the outputs of the measurements labelled by $x, y_1, \ldots, y_{N-1}$, then one can obtain a non-zero 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

$$W_{\alpha} = \sum_{x,y_1,\ldots,y_{N-1}} c^{(\alpha)}_{x,y_1,\ldots,y_{N-1}} G^a_x \otimes G^b_{y_1} \otimes \cdots \otimes G^{b_{N-1}}_{y_{N-1}}$$

(S9)

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

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

$$P(a, b_1, \ldots, b_{N-1}| x, y_1, \ldots, y_{N-1}) = \text{Tr}(G^a_x \otimes G^b_{y_1} \otimes \cdots \otimes G^{b_{N-1}}_{y_{N-1}} \rho_{AB_1\ldots B_{N-1}}),$$

(S10)

where $G^a_x, G^b_{y_i}$ 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

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

(S11)

Considering a subset of the Hilbert space, namely $\Sigma$, we call $\Sigma_{\Pi}$ the projection of the subset $\Sigma$ through the map $\Pi_{\text{CKA}}$, defined as in Eq. (S11). We denote the set of states separable across the partition $S_\alpha | S_\alpha$ as $\Sigma_{\alpha}$. We note that $\Sigma_{\alpha}$ is a closed and convex set. Furthermore, the projection of the set $\Sigma_{\alpha}$ through the linear map $\Pi_{\text{CKA}}$, namely $\Sigma_{\Pi(\alpha)}$ 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 $S_\alpha | S_\alpha$. Due to Theorem 1 a necessary condition to obtain a non-zero key rate is that the state is not separable with respect to any partition. This implies that, given a state $\rho_{A_1B_1\ldots B_{N-1}}$ that leads to a non-zero key rate in a specific protocol, the corresponding probability distribution $P^*(a, b_1, \ldots, b_{N-1}| x, y_1, \ldots, y_{N-1})$ is such that $P^*(a, b_1, \ldots, b_{N-1}| x, y_1, \ldots, y_{N-1}) \notin \Sigma_{\Pi(\alpha)} \forall \alpha$. Moreover, since each $\Sigma_{\Pi(\alpha)}$ is a convex and compact set, it is a well known fact that each element of its complement $\Sigma_{\Pi(\alpha)}^\alpha$ can be separated from $\Sigma_{\Pi(\alpha)}$ with a proper hyperplane [36,38]. In the probability space any hyperplane can be defined as

$$\sum_{x,y_1,\ldots,y_{N-1}} c^{x,y_1,\ldots,y_{N-1}}_{a,b_1,\ldots,b_{N-1}} P(a, b_1, \ldots, b_{N-1}| x, y_1, \ldots, y_{N-1}) = 0$$

(S12)

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

$$\forall P_\alpha(a, b_1, \ldots, b_{N-1} | x, y_1, \ldots, y_{N-1}) \in \Sigma^H, \sum_{x, y_1 \ldots y_{N-1}, a, b_1 \ldots b_{N-1}} c^{(\alpha)}_{x, y_1 \ldots y_{N-1}, a, b_1 \ldots b_{N-1}} P_\alpha(a, b_1, \ldots, b_{N-1} | x, y_1, \ldots, y_{N-1}) \geq 0$$

and

$$\text{for } P^* (a, b_1, \ldots, b_{N-1} | x, y_1, \ldots, y_{N-1}) \notin \Sigma^H \forall \alpha, \sum_{x, y_1 \ldots y_{N-1}, a, b_1 \ldots b_{N-1}} c^{(\alpha)}_{x, y_1 \ldots y_{N-1}, a, b_1 \ldots b_{N-1}} P^*(a, b_1, \ldots, b_{N-1} | x, y_1, \ldots, y_{N-1}) < 0$$

(S13)

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

$$W_\alpha = \sum_{x, y_1 \ldots y_{N-1}, a, b_1 \ldots b_{N-1}} c^{(\alpha)}_{x, y_1 \ldots y_{N-1}, a, b_1 \ldots b_{N-1}} G^{a_x} \otimes G^{b_{y_1}} \otimes \cdots \otimes G^{b_{y_{N-1}}}$$

(S14)

such that, due to Eq. (S13), for each $\alpha$

$$\text{Tr}(W_\alpha \sigma_{\alpha}) \geq 0, \forall \sigma_{\alpha} \in \Sigma_{\alpha}$$

$$\text{Tr}(W_\alpha \rho^*_{A, B_1, \ldots, B_{N-1}}) < 0.$$ 

(S15)

As a matter of fact, Eq. (S15) tells us that the operator $W_\alpha$ is an entanglement witness that detect entanglement across partition $S_\alpha | S_\alpha$. This concludes the proof of the Theorem.