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

(arXiv:2007.11553)

Giacomo Carrara, Hermann Kampermann, Dagmar Bruß, and Gláucia Murta
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany

Entanglement is a crucial resource in quantum information processing. In particular, entanglement has been shown to be necessary [1] for the security of a bipartite Quantum Key Distribution (QKD) protocol [2–4]. Indeed, even prepare-and-measure protocols [2, 4], which do not require any entanglement for their implementation, have an entanglement-based counterpart [5] which can be used for the protocol's security analysis. Here we consider the generalization of QKD to the multipartite scenario, namely Conference Key Agreement (CKA) [6], where N parties wish to establish a common shared secret key, allowing for secure broadcast. We focus on CKA protocols in which, at each round, an N-partite state is distributed to the parties, Alice and $N-1$ Bobs, they perform local measurements and, at the end, classically post-process the outcomes of these measurements to extract a common secret key.

We ask the question whether Genuine Multipartite Entanglement (GME) [7, 8], the strongest form of multipartite correlations, is a necessary requirement to establish a secret conference key. As our main result we establish that, on the contrary, a conference key can be obtained even if the parties share biseparable states at each round of the protocol. Our results are summarized as following:

- Necessary condition for CKA: a non-zero asymptotic conference key rate can only be obtained if the state distributed at each round of the protocol is not separable with respect to any fixed partition of the parties.
- The following family of biseparable states can lead to a non-zero secret conference key:

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

  where $\mathcal{N}$ is a normalization factor, $\mathcal{S}^{(k)}$ is the set of subsets of k parties that contain Alice and $k-1$ Bobs, $|GHZ\rangle_{S_\alpha} = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes k} + |1\rangle^{\otimes k}\right)$ and $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$.
  We derived an analytical expression for the asymptotic conference key rate achievable by these states.

Figure 1 shows the behavior of the asymptotic key rate as a function of N for different values of k.

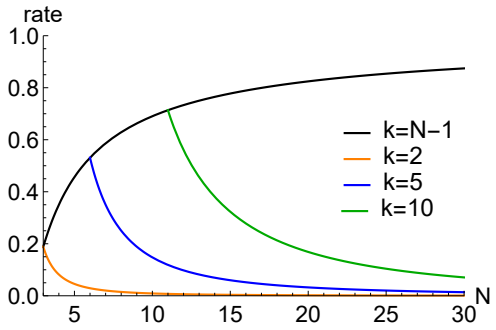

Figure 1. Asymptotic secret key rate for the state of Eq. (1) as a function of N for different values of k. We remark that since $k \leq N-1$, the curves start at different values of N.

- We showed that a non-zero key can be extracted with biseparable states in some well-known, simple protocols, namely the multipartite versions of the BB84 [9] and the six-state [10] protocols.
- We extended the result of Ref. [1] to the multipartite case: if a non-zero asymptotic conference key rate is obtained, then the parties must be able to witness entanglement in each bi-partition of the parties using the measurements performed in the CKA protocol. This result, together with the fact that the family of states (1) lead to non-zero key, provides us with a remarkable insight: a non-zero asymptotic conference key rate represents a new non-linear entanglement witness, which can detect a type of entanglement that cannot be detected by linear entanglement witnesses.

Our results have a significant interest on both theoretical and practical side. From a theoretical point of view, we shed light on the characterization of resources required to perform the task of CKA. So far, the proposed protocols aimed to explore the properties of GME states. We showed that weaker classes of entanglement can be exploited for cryptographic purposes as well. Moreover, from a practical point of view, the generation of biseparable states can be significantly less demanding than GME states.

[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] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[5] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[6] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review (2020), arXiv:2003.10186 [quant-ph].
[7] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[8] M. Walter, D. Gross, and J. Eisert, Multi-partite entanglement (2016), arXiv:1612.02437 [quant-ph].
[9] F. Grasselli, H. Kampermann, and D. Bruß, New Journal of Physics **20**, 113014 (2018).
[10] M. Epping, H. Kampermann, C. macchiavello, and D. Bruß, New Journal of Physics **19**, 093012 (2017).