Composable Security for Multipartite Entanglement Verification

Raja YEHIA[1], **Eleni DIAMANTI**[1], **Iordanis KERENIDIS**[2]
[1] *LIP6, CNRS, Sorbonne Université, 75005 Paris, France*
[2] *IRIF, CNRS, Université de Paris, 75013 Paris, France*

Abstract. We present a multipartite entanglement verification protocol for n parties consisting only in local quantum operations and authenticated classical communication once a state is shared among them and providing composable security against a malicious source. It can be used as a secure subroutine in the Quantum Internet to test if a source is sharing quantum states that are at least ϵ-close to the GHZ state before performing a communication or computation protocol. Using the Abstract Cryptography framework, we can readily compose our basic protocol in order to create a composably secure multi-round protocol enabling honest parties to obtain a state close to a GHZ state or an abort signal, even in the presence of a noisy or malicious source.
Keywords: Entanglement verification, Composable Security, Quantum Internet, Abstract Cryptography.
Link to ArXiv paper: The full paper can be found on https://arxiv.org/abs/2004.07679.

Extended Abstract: Our work extends the work from [1], where the authors develop and analyze a n-party entanglement verification protocol consisting only of classical communication and local quantum operations. One of the parties, called the *Verifier*, has a central role in the protocol: she sends instructions to all parties and broadcasts the output of the verification. The identity of the Verifier as well as the event that the verification actually takes place is randomized to allow for repetition of the protocol in a possibly dishonest setting. We assume that the parties have access to trusted common random sources. We use the Abstract Cryptography framework, where one defines an ideal resource and a concrete resource and the goal is to prove that they are indistinguishable in the presence of malicious parties.

Ideal resource. Our ideal resource, called $\mathcal{MEV}_C$, is meant to be used repetitively by n parties to know if a source is sharing states that are close to the GHZ state. They collectively send a start signal to $\mathcal{MEV}_C$ while the source sends a classical description of a n qubit state ρ. $\mathcal{MEV}_C$ then produces either a bit $C = 0$ and the state ρ shared among the parties or a bit $C = 1$ and a verification bit b_{out} that depends on how close ρ is from the GHZ state. See Fig. 1 for 3 parties.

Concrete resource. We call $\mathcal{R}$ the resource constructed by a state generator resource composed in series to a collection of n quantum channel resources and in parallel to n classical channel resources, and two multiparty trusted common random oracles $\mathcal{O}_C$ and $\mathcal{O}_v$. Moreover we call $\pi_{[n]} = \{\pi_i\}_{i=1}^n$ the protocols of each party and π_S the protocol of an honest source. Together they form our concrete resource $\pi_{[n]}\mathcal{R}\pi_S$. See Fig. 2 for a 3-party example and the paper for formal definitions.

Results and Contribution for QTurn: We prove indistinguishability between $\mathcal{MEV}_C$ and $\pi_{[n]}\mathcal{R}\pi_S$ in the Abstract Cryptography framework [2, 3] resulting in the composable security of the multipartite entanglement verification protocol in a distributed setting with faulty devices. Our work first provides a practical introduction to composable frameworks, which are increasingly used in modern cryptography, and then proves rigorously the composability of the protocol. As a consequence, multipartite entanglement verification can be thought as a secure resource in the distributed setting and can be readily used as a subroutine of more complex protocols in a near-term Quantum Internet. In our work, we show an example of such construction by presenting a multi-round resource that has practical use for many Quantum Internet near-term protocols. A photonic implementation of the protocol has already been realized that shows the feasibility of the protocol with current state-of-the-art experimental capabilities [4].

References

[1] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, "Multipartite entanglement verification resistant against dishonest parties," *Physical Review Letters*, vol. 108, 12 2011.

[2] U. Maurer and R. Renner, "Abstract cryptography," 2011.

[3] U. Maurer and R. Renner, "From indifferentiability to constructive cryptography (and back)," in *Theory of Cryptography*, (Berlin, Heidelberg), pp. 3–24, Springer Berlin Heidelberg, 2016.

[4] W. McCutcheon, A. Pappa, B. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. Rarity, and M. Tame, "Experimental verification of multipartite entanglement in quantum networks," *Nature Communications*, vol. 7, p. 13251, 11 2016.

Figures

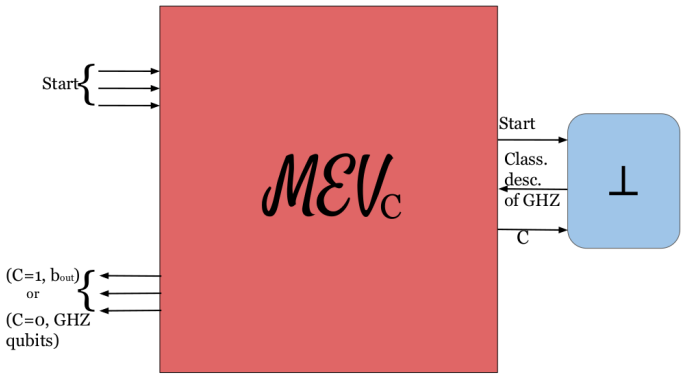

Figure 1: The ideal filtered $\mathcal{MEV}_C\perp$ resource for $n = 3$ parties. On the left are the parties interfaces that are used by the parties to collectively send the start signal and receive the output. On the right is the source interface, filtered by $\perp$ in the honest case that blocks any input and sends specific messages to the resource.

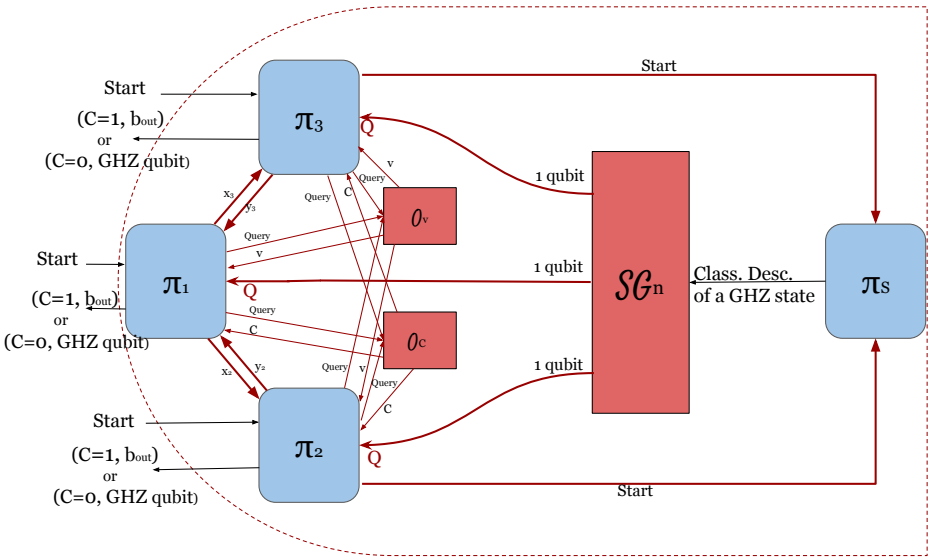

Figure 2: The $\pi_{[n]}\mathcal{R}\pi_S$ resource included within the dotted red line for $n = 3$ parties wishing to test a source, when party 1 is chosen to be the Verifier. We represent resources in red and converters in blue. We recall the timeline of the protocol: (1) all the π_i send a start signal to π_S that sends a classical description of a GHZ state to the $\mathcal{SG}_n$ resource. (2) Upon reception of the qubit, they send a query to $\mathcal{O}_C$ and get C. (3) If $C = 0$ output a GHZ qubit and if $C = 1$ the parties query $\mathcal{O}_v$ and get v (here party 1). (4) The Verifier sends instructions $X = \{x_i\}_{i=1}^n$ (here $\{x_2, x_3\}$) to others parties, get outcomes $Y = \{y_i\}_{i=1}^n$ (here $\{y_2, y_3\}$) and computes and broadcasts b_{out}.