QCRYPT 2020

COMPOSABLE SECURITY FOR MULTIPARTITE ENTANGLEMENT VERIFICATION

Raja Yehia, Eleni Diamanti, Iordanis Kerenidis

Sorbonne Université - LIP6

Contact: raja.yehia@lip6.fr, arXiv: 2004.07679

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.

Setup

- n parties with **limited quantum hardware**: Ability to receive and measure one qubit at a time.
- One source of multipartite entanglement.
- n Quantum channels linking the source and each party.
- Underlying **authenticated** Classical Internet architecture.
- 2 Common random oracles.

Protocol

Protocol 1 Multipartite Entanglement Verification protocol [1]

1. The source creates an n-qubit GHZ state and sends each qubit i to party i using a state generation resource and n one-way quantum channels.
2. All parties receive a random bit C. If $C = 0$ they keep the qubit for computation and stop the protocol. if $C = 1$ they randomly choose one party to be the Verifier.
3. The Verifier (chosen randomly among the parties) selects for each $i \in [n]$ a random input $x_i \in \{0, 1\}$ such that $\sum_{i=1}^{n} x_i \equiv 0 \pmod 2$ and sends it to the corresponding party via an authenticated classical channel resource. She keeps one to herself.
4. if $x_i = 0$, party i performs a Hadamard gate on their qubit. If $x_i = 1$, party i performs a $\sqrt{X}$ gate.
5. Each party i measures their qubit in the $\{|0\rangle, |1\rangle\}$ basis and sends its outcome y_i to the Verifier via the classical channel.
6. The Verifier accepts and broadcasts $b_{out} = 0$ if and only if

$$\sum_{i=1}^{n} y_i \equiv \frac{1}{2} \sum_{i=1}^{n} x_i (\text{mod } 2)$$

Result

Using the Abstract Cryptography framework [2; 3], we prove that $\pi_{[n]}\mathcal{R}\pi_S \approx \mathcal{MEV}_C\perp$ and that $\exists\sigma_S$ s.t. $\pi_{[n]}\mathcal{R} \approx \mathcal{MEV}_C\sigma_S$. This means that the multipartite entanglement verification protocol presented is composable when all parties are honest but with a possibly dishonest source. The protocol can thus be thought of as a black box and equivalently replaced by the $\mathcal{MEV}_C$ resource when designing protocols using this one as a subroutine.

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," *In Innovations In Computer Science*, 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.

Protocol in Abstract Cryptography

Ideal Resource

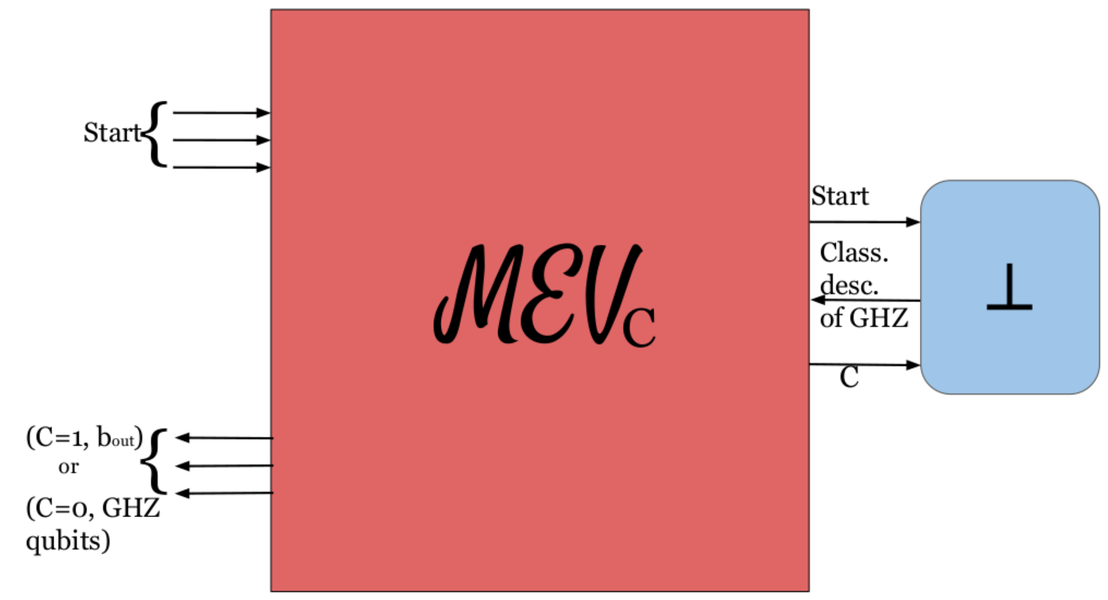

Figure 1: Ideal filtered Multipartite entanglement verification Resource $\mathcal{MEV}_C\perp$ for $n = 3$ parties wishing to test a source. $\perp$ represents honest use of the resource.

Concrete resource

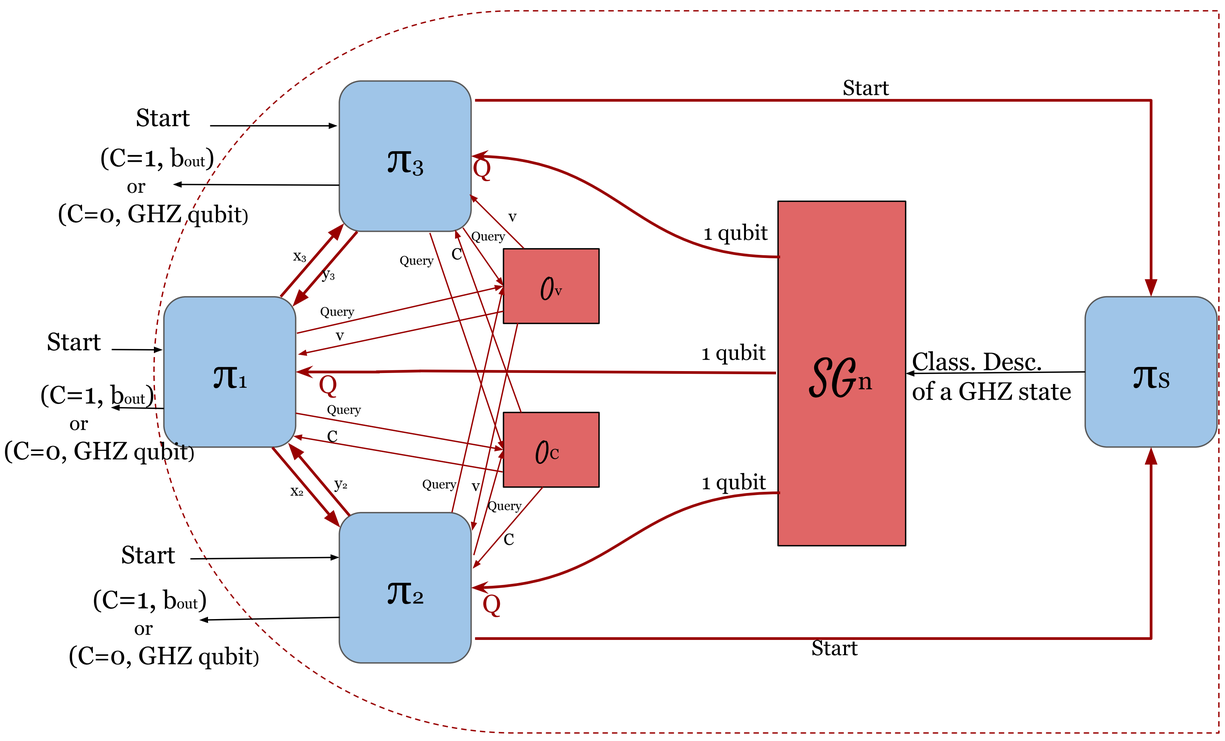

Figure 2: Concrete Multipartite entanglement verification Resource $\pi_{[n]}\mathcal{R}\pi_S$ within the dotted red line for $n = 3$ parties wishing to test a source, when party 1 is chosen to be the Verifier. Resources are depicted in red and converters in blue.

Consequence: Composably secure resource for sharing GHZ states

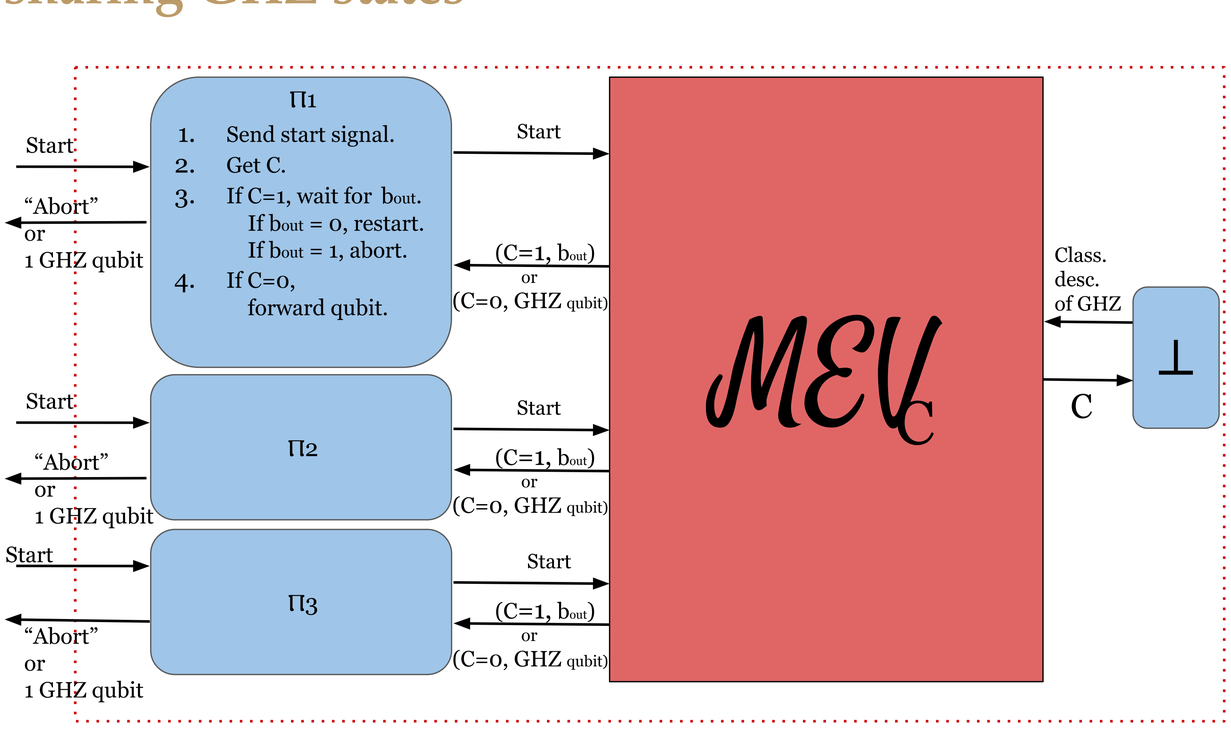

Figure 3: Multi-round verification resource $\Pi_{[n]}\mathcal{MEV}_C\perp$ for 3 parties (in the red dotted square). It takes start signals as input and outputs either a shared quantum state ϵ-close to the GHZ state or an abort signal.

QUANTUM INTERNET ALLIANCE

QUANTUM FLAGSHIP