Contribution ID: **63** Type: **Poster**

Robustness and security of a noisy multiparty quantum summation protocol

Connecting quantum computers to a quantum network opens a wide array of new applications, such as securely performing computations on distributed data sets. Near-term quantum networks will however remain noisy and hence correctness and security of protocols is not guaranteed.

Therefore, we consider noisy protocols with imperfect shared entangled states. This paper takes a first step in formally analyzing both the correctness and the security of these noisy distributed algorithms, by focusing on a multiparty summation protocol. We study the impact of depolarizing and dephasing noise on this protocol and extend the protocol to improve the security and eliminate the need for a trusted third party. Shamir' s secret sharing protocol underlies this extension and lets all parties learn the outcome without revealing individual inputs.

We conclude by proposing definitions of security, privacy and anonymity for quantum multiparty summation protocols, something which was previously only known with respect to specific types of attacks. The anonymity and privacy of these noisy protocols is guaranteed, in the honest-but-curious adversarial model.

Authors: RODRÍGUEZ OTERO, Antón (TNO, TU Delft master student); NEUMANN, Niels (TNO); WEZEMAN, Robert (TNO); VAN DER SCHOOT, Ward (TNO)

Presenter: RODRÍGUEZ OTERO, Antón (TNO, TU Delft master student)

Session Classification: Poster Session 1