Multiparty Entanglement for Secure, Distributed Function Estimation

Description

Several different tasks can be described mathematically as the distributed calculation of a linear functions (such as a mean), including clock synchronisation, which is essential for a wide variety of applications, or the sharing of medical or other information. For clock synchronisation in particular, a secure implementation is fundamental for some applications involving sensitive information, such as the case of global navigation.

However, revealing the exact parameter values corresponding to particular users may pose a security risk within a larger network, as it may reveal unintended information about the user. Therefore, in a synchronisation scheme it is advantageous to be able to contribute a value to a function (such as calculating the mean) without any additional information being revealed to other members of the network. In classical clock synchronisation, this is analogous to the more recently developed 'network time security' update to the widely used 'network time protocol'. Additionally, the confidentiality of data managed in networks of sensors is a concern more generally (e.g. temperature), to which this protocol can be easily generalised.

The primary advantage of this is from the privacy of the parameter, however we also benefit from increased precision from quantum advantage, reaching the super-classical 'Heisenberg limit'. The proposed scheme involves analysing correlations from GHZ states distributed across the network, which is the source of both the precision and the assurance that no information about individual parameters can be leaked to other participants. Comparison to the expected outcomes of randomly chosen 'verification' rounds provides the opportunity to identify potential attacks from dishonest users of the network. This also aligns with ongoing experimental work within QIA to generate GHZ states.

Quantum advantage

Quantum advantage arises firstly from the quadratic reduction in variance due to the quantum Cramer-Rao bound. On the security side, using a fully entangled state makes it possible to compute linear combinations without requiring knowledge of individual parameters. The inherent randomness of measurement outcomes gives perfect privacy to an external observer, whereas correlation between measurement outcomes only reveals the linear function.

Due to continuity of the quantum Fisher information, these properties are implied from verifying that the provided GHZ state is close in fidelity to the optimal GHZ state.