Secure Position Verification

Description

Users may need to prove they are not inside a prohibited area, or equivalently that they are inside a permitted area, in a sensitive scenario where revealing the actual position is not a viable or secure option.

Given that users may be on moving vehicles/aircrafts, it is likely that they will not have direct access to any kind of quantum device connected to the Quantum Internet. Let us also assume that users have access to a precise, reliable and trusted system to acquire their position. In this setting, the users could send fragments of their position information, through secure classical communication channels, to different nodes of a quantum network that are able to perform quantum secure multi-party computation. Through QSMPC, the quantum nodes will check whether the position meets the limitations and requirements of a specific scenario and communicate the result to the users and, eventually, to some interested third parties. Meanwhile, no complete information on the users' precise position will be revealed to the quantum nodes or other third parties.

Translating the problem of checking whether a position or point is inside or outside a specified area into a quantum algorithm, to be performed via QSMPC, may not be trivial. Reducing the problem to simple comparison operations, if possible, may be a feasible approach.

Quantum advantage

The protocol is secure against a dishonest majority, up to n-1 malicious clients, whereas the state-of-the-art classical counterparts can cope with at most n/2-1 adversaries.