Small-scale referendum

Description

Voting is a fundamental process on which democracy is based. Depending on the individual setting, there are distinct security levels that are required to be achieved.

When examining the quantum setting, even though there exist several proposals for quantum electronic voting, none is fulfilling the desired security properties, namely privacy and verifiability [1]. However, if we consider some assumptions on the capabilities of the dishonest parties, we could imagine a simplified quantum voting scheme that satisfies some conditions.

There exist four main categories of quantum voting protocols:

- Based on dual-basis measurements
- Travelling ballot
- Distributed ballot
- Based on conjugate coding

These suffer from different vulnerabilities and therefore could be implemented under different assumptions. In a small-scale election, e.g., in the European parliament, one could assume that the election authorities are trusted, or that the hardware that the voters have access to, is correctly manufactured and not susceptible to change. Finally, even though general elections allow for a voter to vote for many different options, it is simpler to consider a 'yes' or 'no' vote as a starting point.

Quantum advantage

Classical electronic voting schemes are based on computational assumptions to achieve the security properties, in this case, the security stems from encoding in the unitaries applied to a shared entangled quantum state