Quantum-ensured comparative voting and anonymous broadcast channels

Ho Trung Dung
Institute of Physics, Academy of Sciences and Technology
1 Mac Dinh Chi Street, District 1, Ho Chi Minh City, Vietnam

Mark Hillery
Department of Physics and Astronomy, Hunter College of CUNY
695 Park Avenue, New York, NY 10065, USA

Abstract

We want to explore methods for quantum communication that protect privacy. These arose initially out of a study of quantum voting. In quantum voting, one has an authority, who prepares ballots and counts the votes, and voters, who cast votes. We suggest schemes that allow the authority to determine how many ``yes" and ``no" votes there are, but not how any individual voter voted. Cases of two, four, and an arbitrary number of voters are considered. Possible realization with linear optics is discussed and the vulnerability of these schemes to eavesdropping is examined. Comparative voting schemes are closely related to cryptographic constructs called anonymous broadcast channels. This is a multi-party channel in which anyone can send a message to everyone else, but the source of the message will not be known. In order to create a quantum anonymous broadcast channel, we need a multi-particle quantum state in which users can, by local operations, create the same global quantum state. The simplest example is given by an n-qubit Greenberger-Horne-Zeilinger state where the information to be conveyed anonymously to participants in the network is encoded in the phase differences between the component states. A quantum anonymous broadcast channel with the information encoded in the weights of the component states can be set up as well, via rotations of an n-qubit symmetric state. Finally we consider a scheme based on a two-mode squeezed vacuum.