

Quantum leader election

An important task in distributed systems is that of leader election. This amounts to deciding for example which of a set of threads, processes or nodes gets to modify certain data, assign work to the other members of the system and so on. Another example of leader election is in blockchain, where the task of electing a leader is equivalent to deciding who gets to create the new block [1].

In some scenarios, the parties attempting to elect a leader might not trust each other and want to agree on a leader in a fair way. That is, without an individual, or group of individuals, being able to bias the outcome of the election. While this is impossible to do using just classical information processing, there exists quantum protocols for this task [2].

Quantum leader election is based on a protocol called weak coin flipping [3]. In this scenario, two parties Alice and Bob want to agree on a random outcome, 0 or 1, without trusting each other. It can be thought of as if the coin is 0 then Alice is elected, and if the coin is 1 Bob is elected. The protocol is said to be unbiased if a player attempting to cheat still cannot be elected with a probability more than $\frac{1}{2} + \epsilon$, where ϵ is some number that can be made arbitrarily small.

For this challenge, however, you will implement a simpler version of a coin flipping protocol, that does have a finite bias but is nevertheless better than any classical protocol [4]. For details on this protocol, please consult Section 2 of Ref. [5], where it is described in a detailed step by step manner.

Note that the protocol requires Alice to prepare a qutrit state – that is, a quantum state of dimension three (that can take on values $\{0,1,2\}$ instead of just $\{0,1\}$ in the case of a qubit).

The steps of the challenge are the following:

1. Find a way to encode a qutrit using qubits in SquidASM (for example using the symmetric subspace of two-qubit states).
2. Implement a circuit for Alice to prepare the state $|\psi_a\rangle$ as defined in Ref. [5].
3. Send the qutrit part of the state to Bob using quantum teleportation.
4. Implement the classical rounds of communication, simulate the protocol and check that it is fair (gives an equal winning probability) when neither player cheats.
5. Try to think of a way for Alice or Bob to cheat, implement this strategy and simulate the winning probability they can achieve (see Ref. [5] for an example of a cheating strategy).

[1] <https://eprint.iacr.org/2022/993.pdf>

[2] [0910.4952.pdf \(arxiv.org\)](https://arxiv.org/abs/0910.4952)

[3] [Coin Flipping - Quantum Protocol Zoo \(veriqcloud.fr\)](https://veriqcloud.fr/Coin_Flipping_-_Quantum_Protocol_Zoo/)

[4] [1811.02984.pdf \(arxiv.org\)](https://arxiv.org/abs/1811.02984)

[5] [arXiv:quant-ph/0206121v2 12 Jul 2002](https://arxiv.org/abs/quant-ph/0206121)