Effect of measurement errors on the failure probability of quantum-aided Byzantine agreement

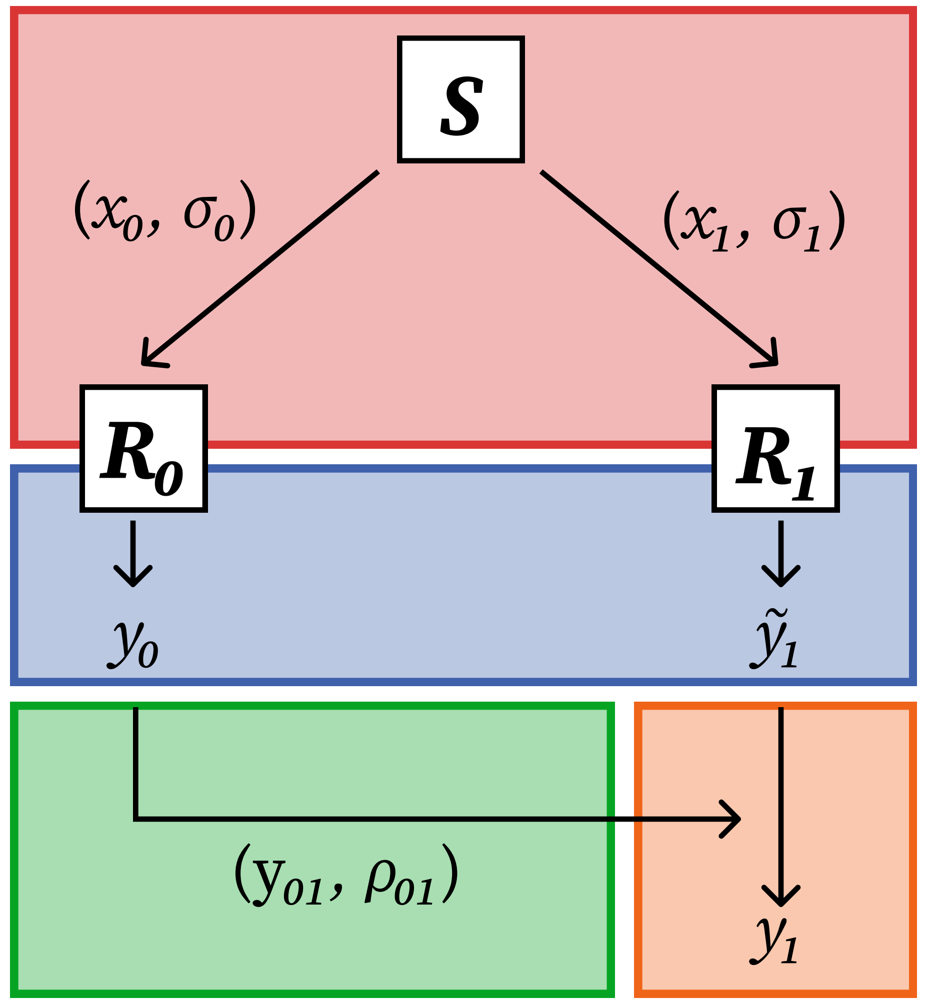
Author: Kimon Kyparos | *k.kyparos@student.tudelft.nl*
Supervisor: Tim Coopmans
EEMCS, Delft University of Technology

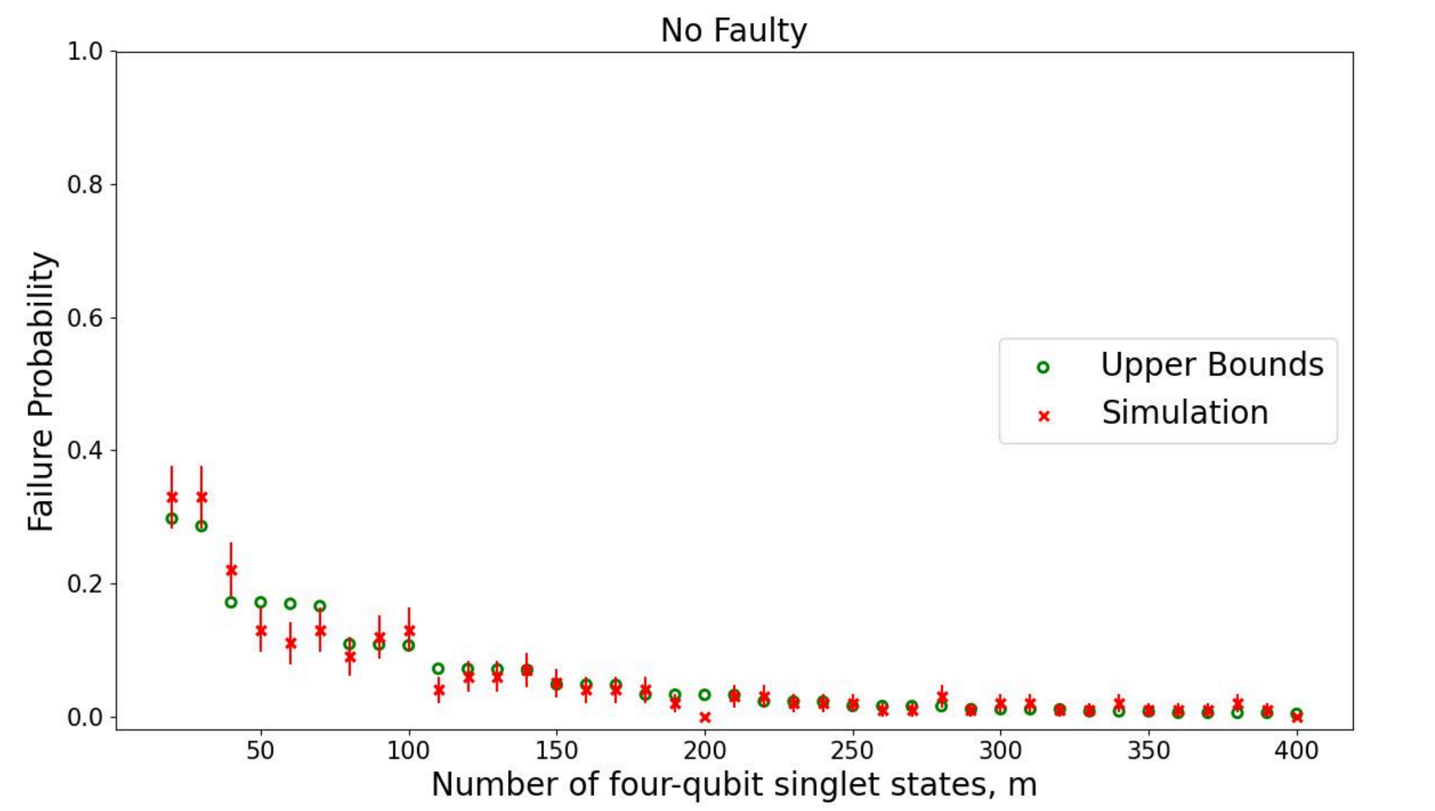
Introduction

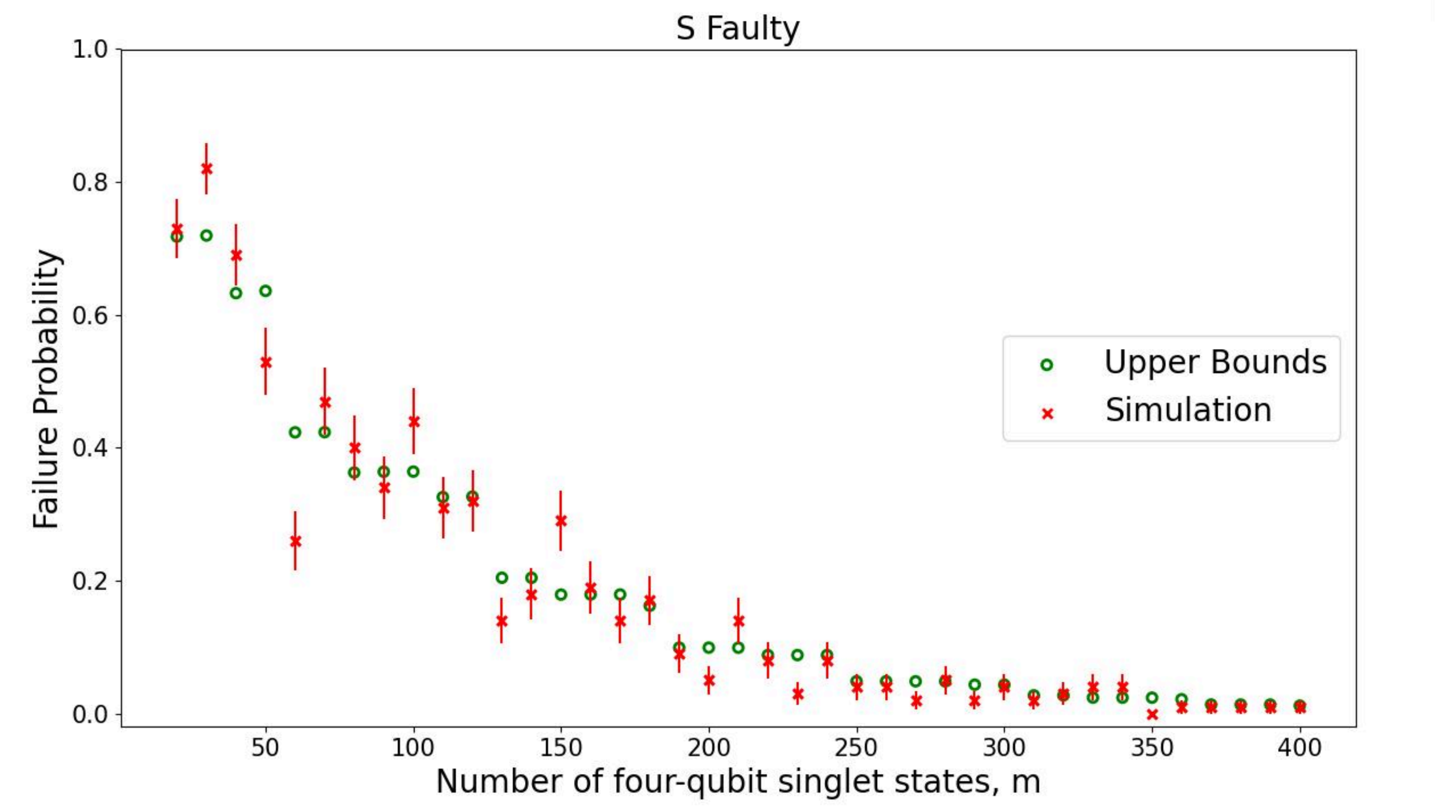
- From blockchain to distributed databases, distributed and multi-agent systems need the participating nodes to reach consensus on a certain value.
- **Byzantine agreement** allows this
- Byzantine **fault tolerance**: in a network of n nodes, the protocol can reach consensus even if there are up to t faulty nodes
- Classical implementation offers tolerance $t < n/3$
- Quantum implementations exist that offers tolerance up to $t < n/2$

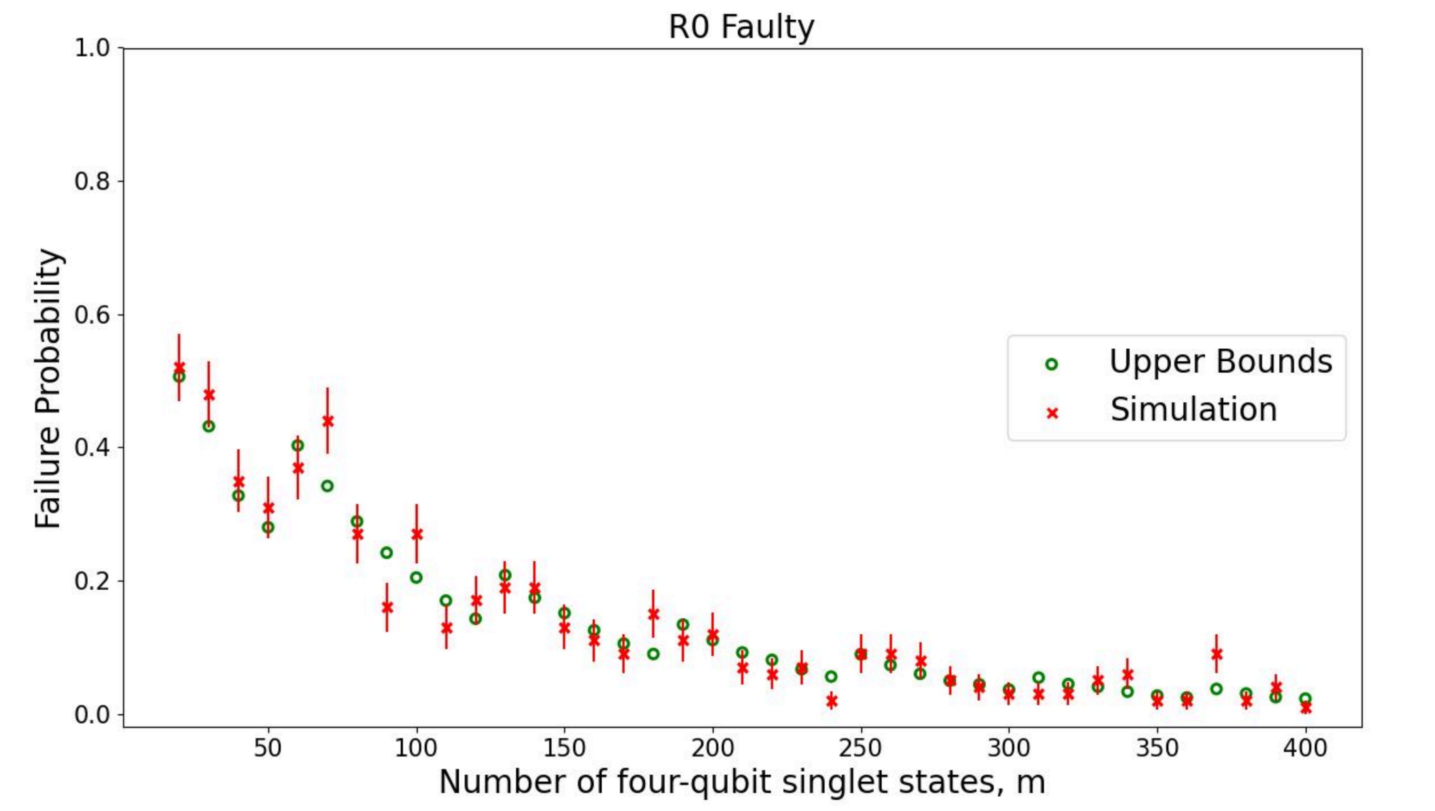
- **BUT:** Quantum networks are noisy
- Noise can cause the protocol to fail
- Multiple possible sources of noise, we focus on **measurement errors**
- A question arises: *How is the failure probability of the quantum variant of the protocol affected by measurement errors?*

Weak Broadcast Protocol[1]









Quantum Background

- **Qubits:** superpositions of $|0\rangle$ and $|1\rangle$
- Quantum **gates**: operations on the qubits
- Protocol is based on the four-qubit singlet state:

$$|\psi\rangle = \frac{1}{2\sqrt{3}}(2|0011\rangle - |0101\rangle - |0110\rangle - |1010\rangle - |1001\rangle + 2|1100\rangle)$$

- Qubits distributed through **teleportation**

Methodology

- The protocol was simulated on a **three-node network** using SquidASM
- **POVM** measurement using the Kraus operators:

$$M_0 = \begin{bmatrix} \sqrt{f_0} & 0 \\ 0 & \sqrt{1-f_1} \end{bmatrix}, M_1 = \begin{bmatrix} \sqrt{1-f_0} & 0 \\ 0 & \sqrt{f_1} \end{bmatrix}$$

- This gives $1 - f_0$ probability of a 0 flipping to a 1 and $1 - f_1$ probability of a 1 flipping to a 0:

$$\Pr(0) = \mathrm{Tr}(M_0|\psi\rangle\langle\psi|M_0^\dagger) = \alpha^2 f_0 + \beta^2(1-f_1)$$
$$\Pr(1) = \mathrm{Tr}(M_1|\psi\rangle\langle\psi|M_1^\dagger) = \alpha^2(1-f_0) + \beta^2 f_1$$

Experiments and Results

- Weak Broadcast Protocol (WBC) was run **without noise** and the failure probability was compared to the upper bounds calculated by Guba et al.[1]
  - Network simulation follows upper bounds
- WBC was subsequently simulated using near-term, *3x* and *10x* improved **noise** values (f_0, f_1)
  - Simulation results show that measurement error noise has a **significant effect** on the failure probability. High failure probability was observed, even with the improved parameters

Conclusions and Future Work

- Measurement error noise **greatly affects** the failure probability. Even with improved parameters, failure probability is exceedingly high for practical applications
- More research needed into extending to more nodes, using different protocols or improving the existing one

References
[1] Zoltán Guba et al. "Resource analysis for quantum-aided Byzantine agreement with the four-qubit singlet state". In: Quantum 8 (2024). doi: https://doi.org/10.22331/q-2024-04-30-1324