Noisy Byzantine Agreement in a Small Quantum Network

How is the failure probability of the protocol affected by "leakage" errors?

Ayşe İdil Evci
A.I.Evci@student.tudelft.nl

Supervisor & Responsible Professor: Tim Coopmans
Delft University of Technology

1. Motivation & Problem

- Quantum networks enable applications like secure communication and distributed computing [5].
- **Byzantine Agreement Protocols** (BAP) ensure consensus despite faulty/malicious parties [4].
- Quantum BAPs can tolerate up to $t < n/2$ faulty nodes, outperforming classical $t < n/3$ where n is the number of participating parties [3].
- We investigate the impact of leakage errors on the **Weak Broadcast (WBC)** protocol [2, 3].

2. Quantum Computing

- **Qubits**:
  - superposition of classical states 0 and 1.
  - $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- **Entanglement**:
  - 2+ qubits become correlated in a way that the state of one determines the state of the others.
  - Non-separable, it cannot be written as combination of different states.
  - Enables quantum communication.
- **Quantum Gates**:
  - Operations to manipulate qubits.
  - We can build circuits and use them to generate entangled multi-qubit states.

3. WBC(3, 1) Protocol Overview

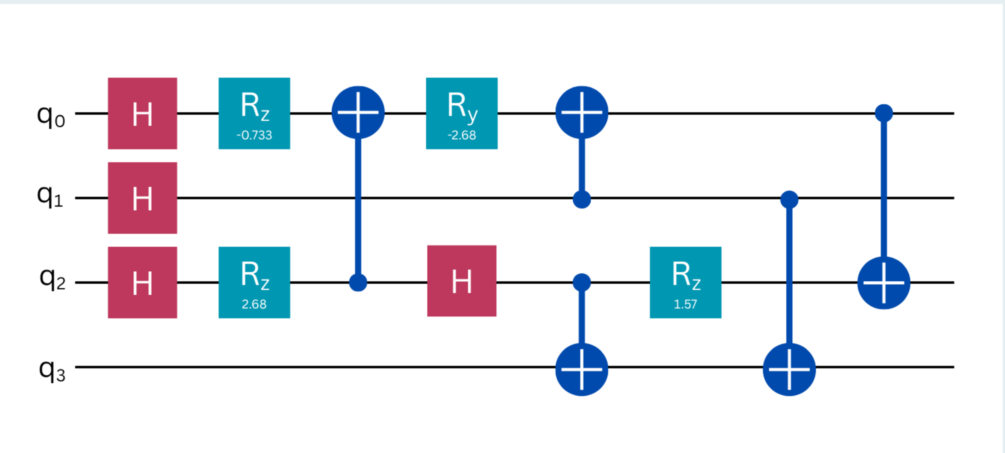

Figure 1: Preparation circuit for the four-qubit state used in WBC(3,1) based on the Loop Circuit from Guba et al. [3]

- The sender prepares a 4-qubit entangled state and chooses a bit value (0 or 1).
- The sender measures the first 2 qubits. If both match the chosen bit, the round is added to the check set.

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

Figure 2: The four-qubit entangled state used in WBC(3,1).

3. WBC(3, 1) Protocol Overview

1) Invocation Phase: After m rounds, the sender sends the bit value and check set to both receivers.
2) Check Phase: Each receiver checks if the check set has elements above a threshold T and that all their measurements differ from the sender's bit.
3) Cross-Calling Phase: Receiver R_0 sends its decision and check set to R_1.
4) Cross-Check Phase: R_1 accepts R_0's decision only if:
- R_1's own result is different from R_0's result,
- R_0's check set has size ≥ T,
- R_1's measurements contradict R_0's bit in most of the check set.

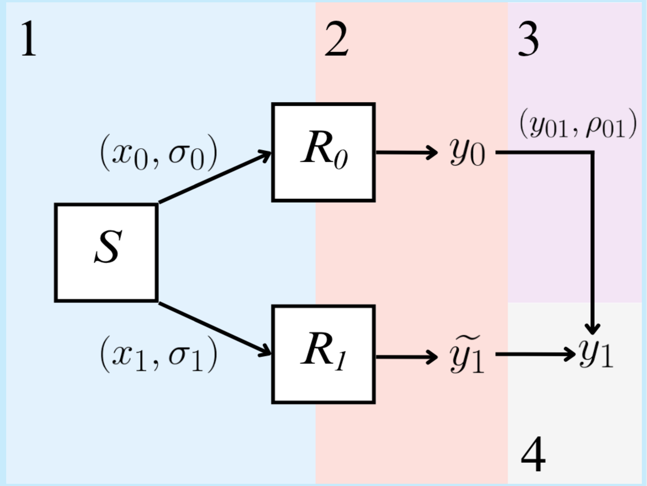

Figure 3: Illustration of the three parties involved in the WBC(3,1) protocol: Sender S, Receiver R0, and Receiver R1.

Different Faulty Configurations of the Protocol:

- **No-Faulty**: All parties are honest.
  - If S, R_0, and R_1 agree on either 0 or 1 → Success ✅
  - Otherwise → Failure ❌
- **S-Faulty**: Sender sends different bits to R_0 and R_1.
  - If R_0 and R_1 agree → Failure ❌
  - Otherwise → Success ✅
- **R_0-Faulty**: R_0 accepts the wrong bit and sends a forged check set to R_1.
  - If S and R_1 agree on the bit → Success ✅
  - Otherwise → Failure ❌

4. Leakage Errors & Bit-Flip Noise Model

- **Leakage Errors:**
  - Out of 16 possible basis states, only 6 are useful in the protocol.
  - Leakage occurs when the outcome deviates to one of the 10 unintended basis states.
- **Modeling:**
  - Two approaches considered:
    - Bit-flip Model (applies bit flips after measurement).
    - Kraus Operator Model (applies noise before measurement).
  - We chose the Bit-flip Model because:
    - It is more transparent.
    - It allows better control over the error probabilities.
- **Bit-flip probability definitions:**
  - p0 → probability of incorrectly measuring a qubit in state $|0\rangle$ as $|1\rangle$.
  - p1 → probability of incorrectly measuring a qubit in state $|1\rangle$ to $|0\rangle$.

5. Analytical Analysis of the Bit-flip Model

$$p_f^{0011} = l_T^{0011} + (1 - l_T^{0011}) \cdot \left[1 - (1 - q^{0011}(p_0, p_1)^m)\right]$$

Figure 4: The overall theoretical failure probability under asymmetric measurement noise when the sender's bit is 0.

- We derived a formula for the failure probability under bit-flip noise for the no-faulty configuration.
- **Failure occurs due to:**
  - Check set being too small (violates the length condition).
  - Harmful inconsistencies in the check set (violates the consistency condition).

6. Results & Discussion

- Simulator: **SquidASM** (built on NetSquid)
- Our noise-free results match the results from Figure 4 from Guba et al. [3]
- Simulation details:
  - Number of entangled states: **m** ∈ [20, 400]
  - Monte Carlo trials per m: **N** = 100
  - Bit-flip probabilities derived from the fidelity values reported by the NetSquid paper [1]:
    - $\mathbf{p_0} = 0.05$
    - $\mathbf{p_1} = 0.005$

Error bars show the standard error of Bernoulli trials: **SE** = $\sqrt{p \times (1 - p) / N}$

No-Faulty Configuration:
- Failure probability increases with m.
- Bit-flip model results are less pessimistic than Guba et al.'s assumptions [3].

S-Faulty Configuration:
- Slight decrease in failure under leakage noise.
- Aborts are counted as successful outcomes.
- Leakage disrupts sender's ability to deceive both receivers.

R_0-Faulty Configuration:
- Failure probability increases with m.
- Bit-flips act similarly to the no-faulty case and bit-flips in R_1 measurements help R_0 deceive.
- Our setup always sets sender's bit to 0, which slightly reduces failures due to asymmetry in readout fidelity.

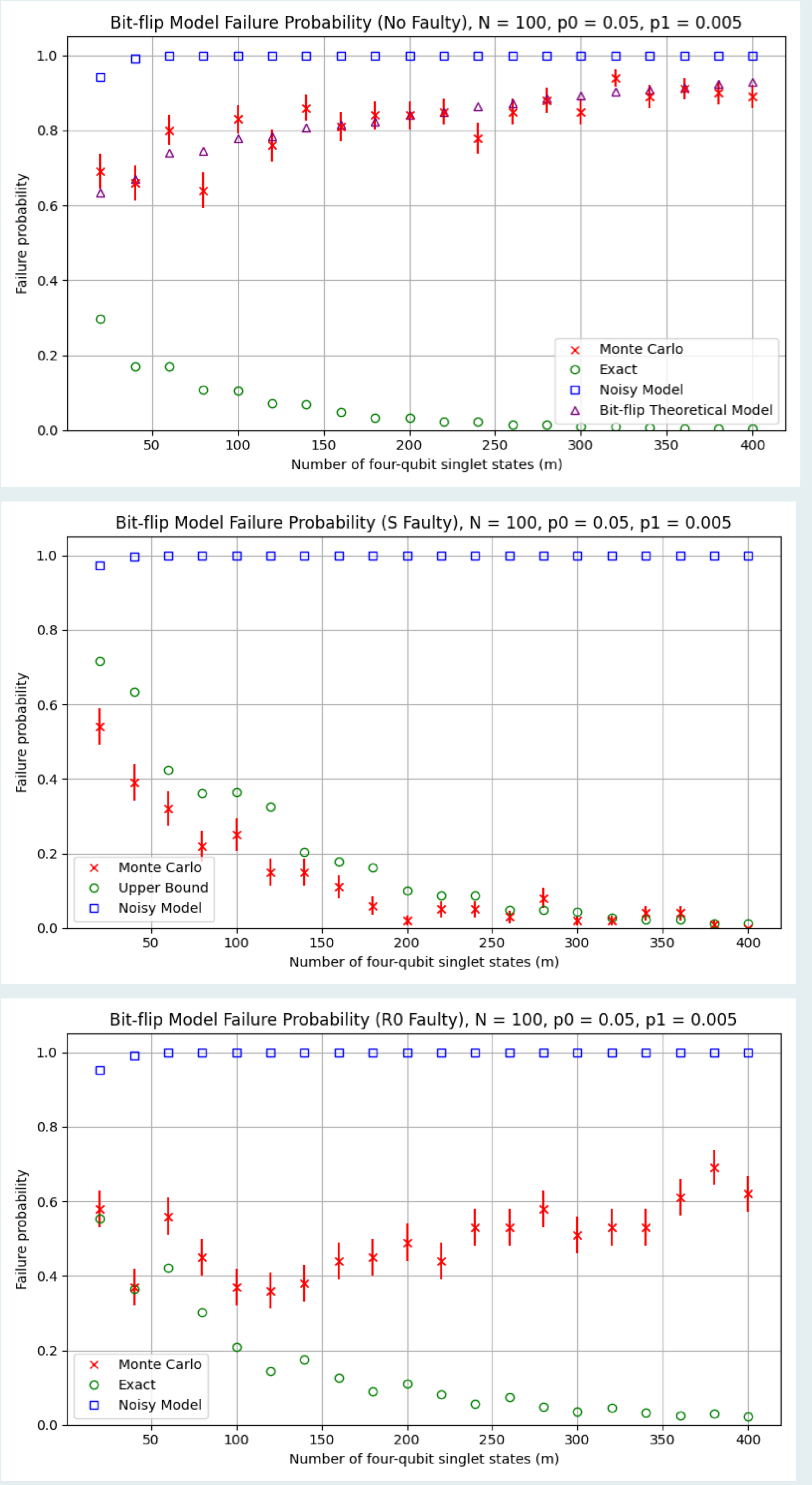

Figure 5: Simulation results under bit-flip model: no-faulty, S-faulty, and R0-faulty configurations.

7. Conclusion

- Our custom bit-flip model shows less pessimistic outcomes than Guba et al. [3].
- WBC(3,1) is not resilient to realistic measurement noise.

8. Future Work

- Why does the Kraus Operator Model produce different trends compared to the Bit-flip model?
- Can we redesign WBC(3,1) to be more robust to hardware noise?

References

[1] Tim Coopmans, Robert Knegjens, Axel Dahlberg, David Maier, Loek Nijsten, Julio de Oliveira Filho, Martijn Papendrecht, Julian Rabbie, Filip Rozpadek, Matthew Skrzypczyk, Leon Wubben, Walter de Jong, Damian Podareanu, Ariana Torres-Knoop, David Elkouss, and Stephanie Wehner. Netsquid, a network simulator for quantum inormation using discrete events. Communications Physics, 4(1):164, 2021.
[2] Matthias Fitzi. Generalized Communication and Security Models in Byzantine Agreement. PhD thesis, ETH Zurich, 2003. Reprint as vol. 4 of ETH Series in Information Security and Cryptography, Hartung-Gorre Verlag.
[3] Zoltán Guba, István Finta, Ákos Budai, Lőránt Farkas, Zoltán Zimborás, and András Pályi. Resource analysis for quantum-aided byzantine agreement with the four-qubit singlet state. Quantum, 8:1324, April 2024.
[4] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3):382–401, 1982.
[5] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. Science, 362(6412):eaam9288, 2018.