Resource analysis for quantum-aided Byzantine agreement

Z. Guba (1), I. Finta (2,3), Á. Budai (1,2,4), L. Farkas (2), Z. Zimborás (4,5), A. Pályi (1)

(1) Department of Theoretical Physics, Budapest University of Technology and Economics
(2) Nokia Bell Labs
(3) Óbuda University
(4) Wigner Research Centre for Physics
(5) BME-MTA Quantum Information Theory "Momentum" Research Group

Acknowledgments:
This research was supported by the Ministry of Innovation and Technology and the National Research, Development and Innovation Office (NKFIH) within the Quantum Information National Laboratory of Hungary and the Quantum Technology National Excellence Program (Project No. 2017-1.2.1-NKP-2017-00001), and by the NKFIH fund TKP2020 BES (Grant No. BMSE-IE-NAI) under the auspices of the Ministry for Innovation and Technology. The research has been supported by the National Research, Development and Innovation Office (NKFIH) through the OTKA Grant FK 132146 and FK 135220.

The task:
to achieve consensus among three components.

New family of Weak Broadcast protocols:
based on previous ideas we define a new protocol.

Ideal scenario
One faulty component can confuse the receivers

Classical
communication
output

One faulty component can confuse the receivers

Resource analysis for the protocol
(1) Define smart adversary strategies.
(2) Compute error probabilities.

Error probability: probability that the protocol ends with failure.

There are ideas for protocols resilient against \( t < n/3 \) : use quantum physics to achieve consensus.

New family of Weak Broadcast protocols:
based on previous ideas we define a new protocol.

Measurements on IBM Quantum
What is the precision of the state preparation for the singlet state?

(1) compare measured distribution

Classical fidelity

best classical fidelity: \( F_c = 0.9021 \)

(2) quantum state tomography

Quantum state fidelity

best quantum fidelity: \( F_q = 0.8116 \)

Significant errors in state preparation.

Hardware improvements & more efficient circuit needed.

Optimization in the parameter space
parameters: \( \lambda, \mu \)

Task: find minimal number of singlet states needed to push the error probability under 5%.

minimal \( m = 279 \)

This is only a lower bound.

Conclusion:
- New family of parameter-dependent Weak Broadcast protocols.
- Resource analysis of the protocol.
- Optimization in the parameter space.
- Experimental characterization of the state preparation on real qubits.

Future work:
- Security proof.
- Resistance against physical errors.
- Generalization for \( n \)-component systems.
- Implementation on real hardware

Acknowledgments:
This research was supported by the Ministry of Innovation and Technology and the National Research, Development and Innovation Office (NKFIH) within the Quantum Information National Laboratory of Hungary and the Quantum Technology National Excellence Program (Project No. 2017-1.2.1-NKP-2017-00001), and by the NKFIH fund TKP2020 BES (Grant No. BMSE-IE-NAI) under the auspices of the Ministry for Innovation and Technology. The research has been supported by the National Research, Development and Innovation Office (NKFIH) through the OTKA Grant FK 132146 and FK 135220.