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

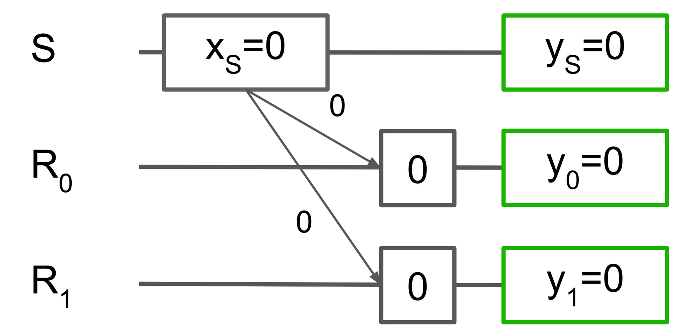
(3) Óbuda University

(4) Wigner Research Centre for Physics

(5) BME-MTA Quantum Information Theory "Momentum" Research Group

The task:

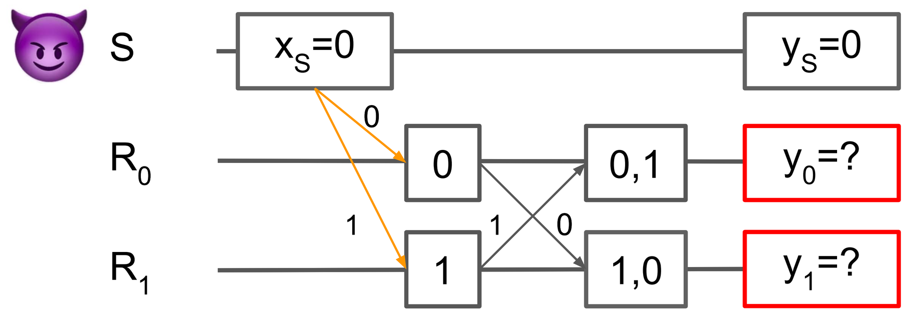
to achieve consensus among three components.



Ideal scenario

$n = 3$

$t = 0$



$n = 3$

$t = 1$

One faulty component can confuse the receivers

Lamport ACM 1982

Protocols are usually resilient against t adversaries if $t < n/4$.

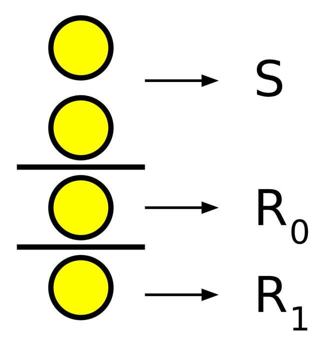
There are ideas for protocols resilient against t < n/3 :

use quantum physics to achieve consensus.

four-qubit singlet state

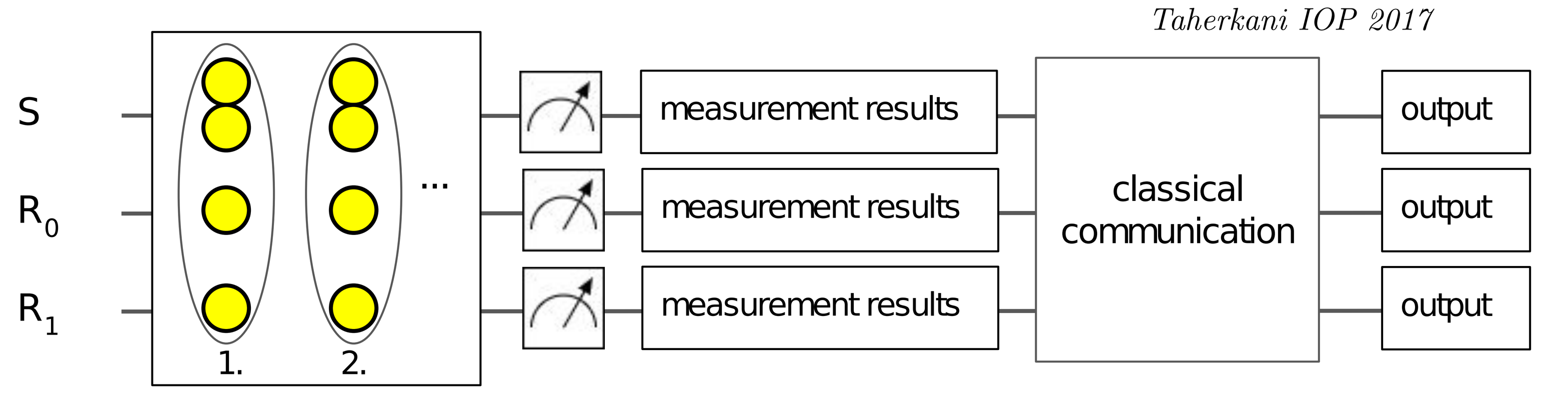
$$|\psi\rangle = \frac{1}{2\sqrt{3}}(2\,|0011\rangle - |0101\rangle - |0110\rangle - |1010\rangle - |1001\rangle + 2\,|1100\rangle)$$

distribution of qubits:



protocol:

Fitzi et al EUROCRYPT 2002
Cabello PRA 2003
Taherkani IOP 2017



goal: achieve **Weak Broadcast**

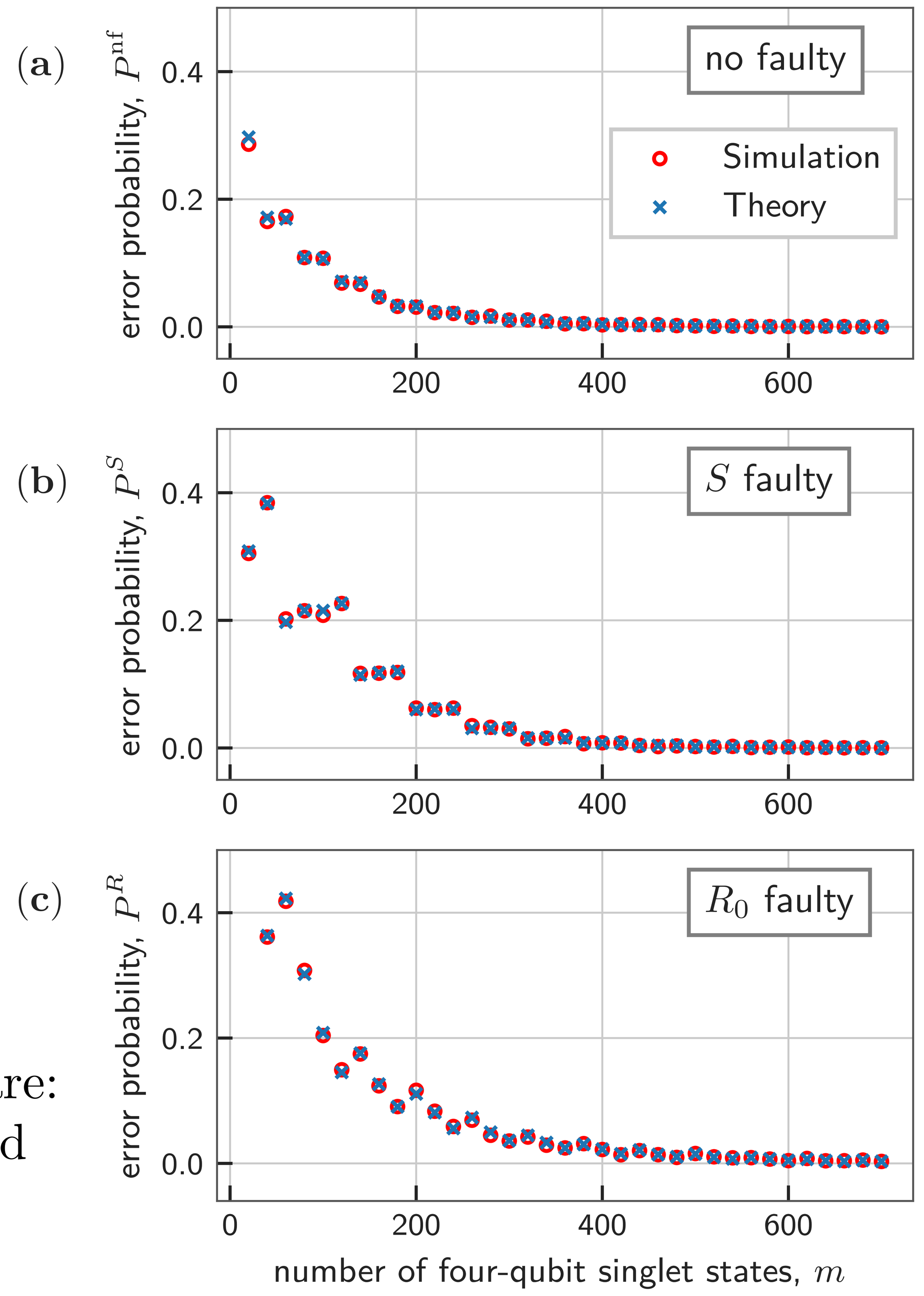
New family of Weak Broadcast protocols:

based on previous ideas we define a new protocol.

Resource analysis for the protocol

(1) Define smart adversary strategies.
(2) Compute error probabilities.

error probability: probability that the protocol ends with failure.



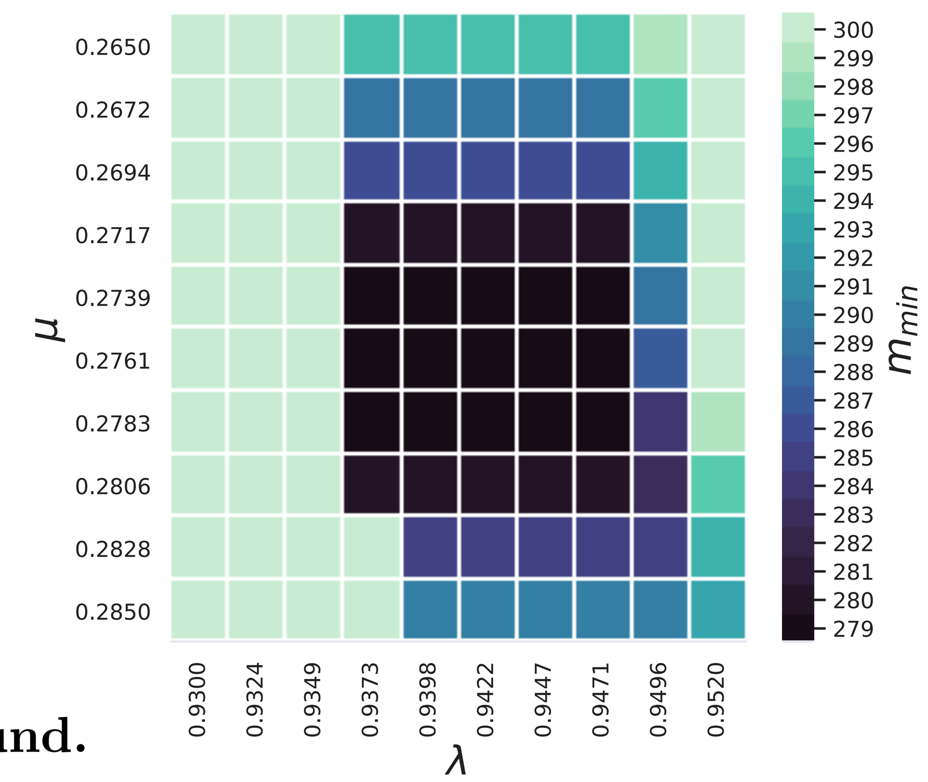
here the parameters are: $\mu = 0.272$ and $\lambda = 0.94$

Optimization in the parameter space

parameters: λ, μ

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

minimal m: 279



This is only a lower bound.

Measurements on IBM Quantum

What is the precision of the state preparation for the singlet state?

(1) compare measured distribution

Classical fidelity

$$F_c = \left(\sum_{s=(0000)}^{(1111)} \sqrt{P_{\text{exp}}(s)P_{\text{id}}(s)}\right)^2$$

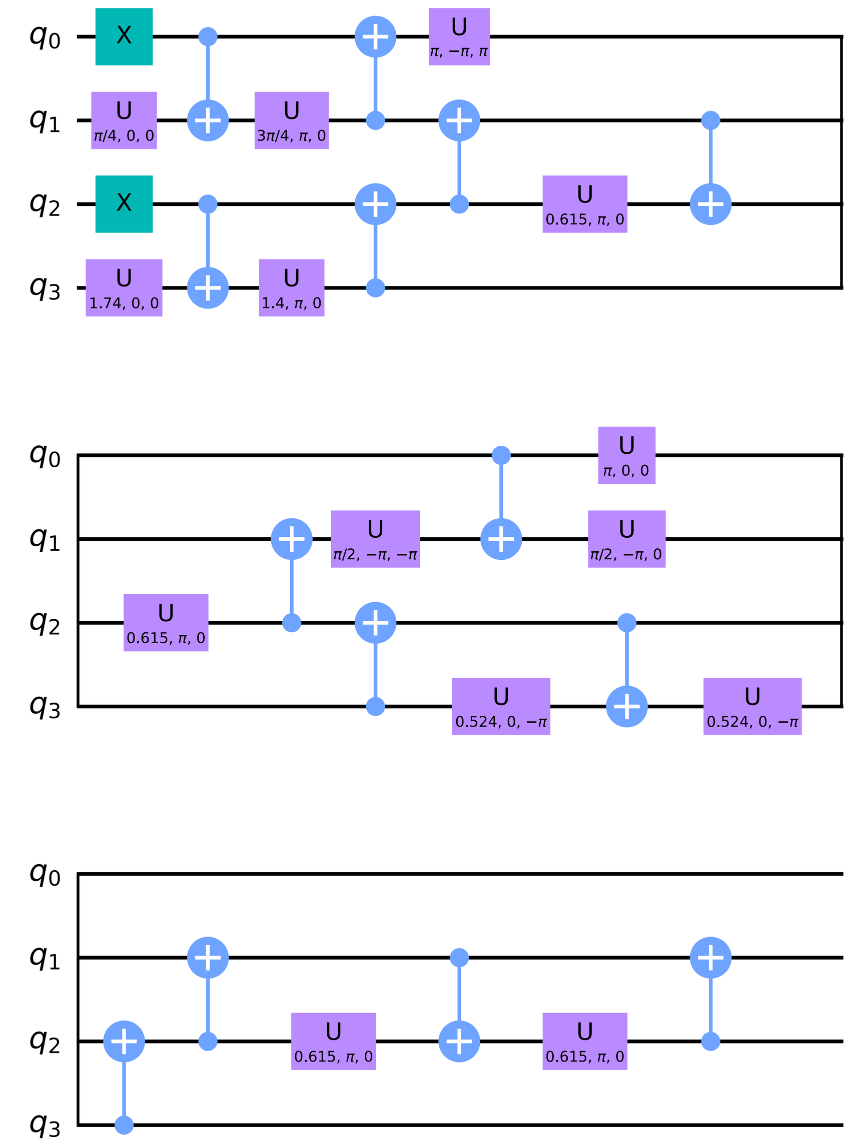
best classical fidelity: $F_c = 0.9021$

(2) quantum state tomography

Quantum state fidelity

$$F_q = \left(\mathrm{Tr}\sqrt{\rho_{\text{id}}^{1/2}\,\rho_{\text{exp}}\,\rho_{\text{id}}^{1/2}}\right)^2$$

best quantum fidelity: $F_q = 0.8116$



Gard npj Quantum Inf. 2020
B. T. Gard (private communication)

Significant errors in state preparation.
Hardware improvements & more efficient circuit needed.

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 IES (Grant No. BME-IE-NAT), under the auspices of the Ministry for Innovation and Technology. This research has been supported by the National Research, Development and Innovation Office (NKFIH) through the OTKA Grant FK 132146 and FK 135220.