

Formal Verification of Quantum Secret Sharing (QSS)

Huzaifa Khan., B.S, Maya Cutkosky., B.S, Rohit Chadha., PhD.



Quantum Innovation Center

University of Missouri

College of Engineering

University of Missouri

Introduction

Quantum Secret Sharing splits a secret among its participants using an entangled GHZ states, so it can only be recovered if all parties cooperate. Introduced by Hillery et al. in 1999, a complete cryptanalytic proof of its flaws didn't appear until nearly a decade after in Qin et al.

In the three-participant protocol, a dishonest insider may gain access to the secret without collaborating with the other participant and without triggering the security alarm, thus breaking the protocol security.

The flaw is caused by the ordering of the announcements in the security check. Measurement bases are announced before measured values, which gives the attacker the ability to calculate the whichever measured value will allow him to escape detection.

We look at formalizing this protocol, its flawed version, as well as its fixed version. We also looked at implementing the protocol on real hardware to study usability and scalability.

Objectives

1. **Formalize the original QSS Protocol as well as the fixed protocol in Quantum Relational Hoare Logic (QRHL)**
2. **Implement the protocol, and the attack in Qiskit and benchmark on real hardware; Also demonstrate the fixed protocol and scalability.**

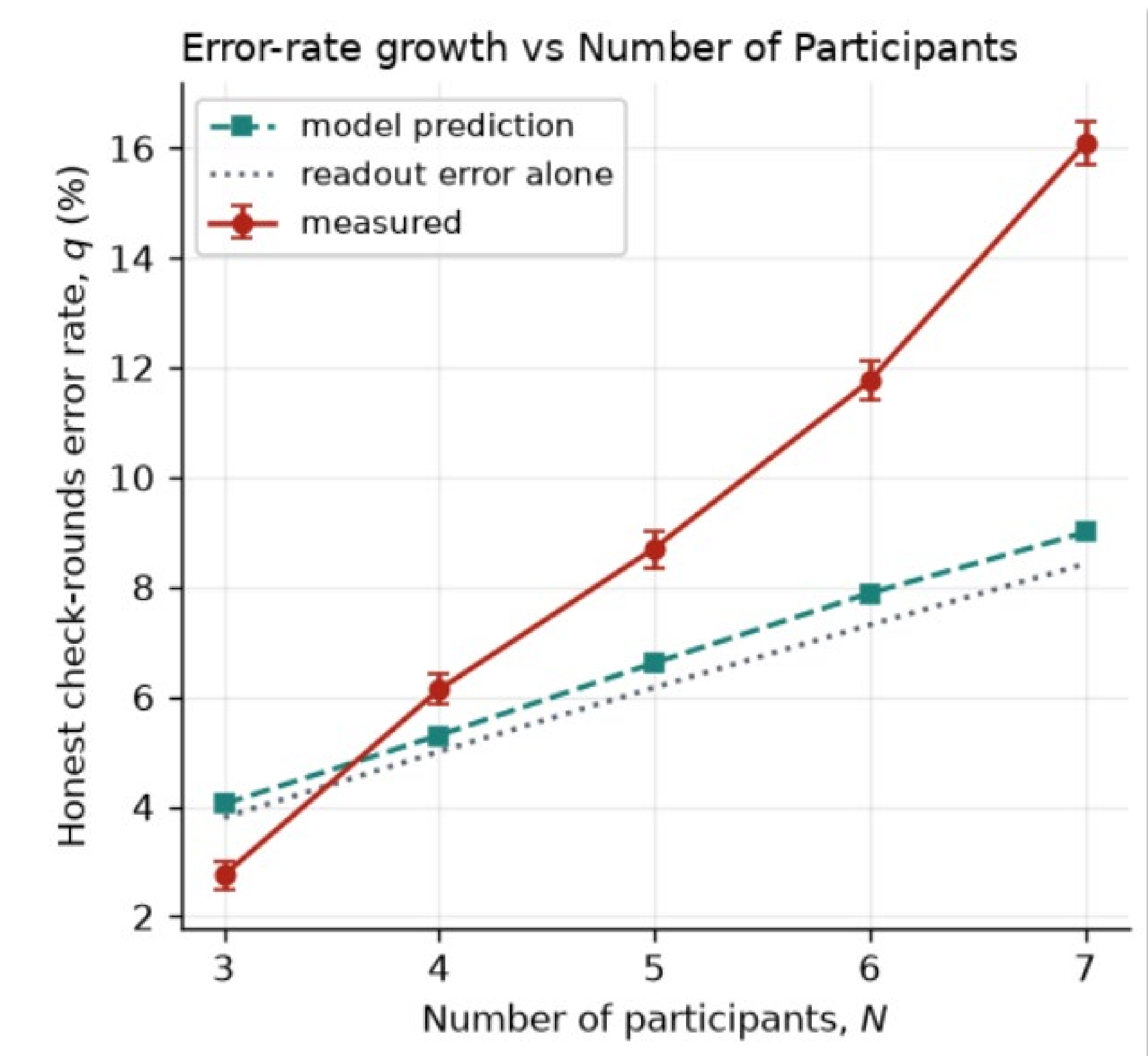
Methodology

Formal Verification: We used the QRHL-tool, a mechanization of the Quantum Relational Hoare Logic built on top of Isabelle/HOL. The logic relates two quantum programs using preconditions and postconditions, and the tool verifies that starting at a precondition, the post condition is always reached after running the program.

- Security properties are expressed as follows: one program may be the real protocol, while the other is an idealized protocol, and the two should be indistinguishable based against the post condition.

- Similarly, an attack on the protocol is expressed using the post-condition and proven that the post-condition is reachable from the precondition after running the programs.

Qiskit Implementation: We implemented the protocol as quantum circuits in Qiskit, running the GHZ preparation and simulated sending the qubits among the participants on IBM hardware, verifying the resulting measurements against the theoretical predictions. The attack was demonstrated and studied, then the protocol was fixed and shown to now detect the attack. Some attacker strategies were studied, and the generalized protocol was tested with arbitrary group sizes, from N=3 to N=7, comparing growth of error in the simulator vs noisy hardware.



Results: Formal Verif.

We formalized correctness and security property of QSS and mechanized the attack against the original protocol; this allows us to easily see the flaw of the protocol and how it was fixed. We also studied the tool itself, which is still a work in progress, and see what its limitations are.

Correctness – the recipients reconstruct the secret on all usable rounds:

qrhl {Cla[True]} call qss_run; ~ skip;

{Cla[(a_basis1 + b_basis1 + c_basis1 = 0) --> (guess = secret)]}.

Lemma1 – the attacker evades and steals secret with probability = 1:

Pr[(check=1 -> detected=0) && (check=0 -> guess=secret) : attack(rho)] = 1.

Lemma2 – under fixed protocol, guessing correct basis restores attack:

Pr[(gA=bA && gB=bB) -> ((check=1 -> detected=0) && (check=0 -> guess=m_A)) : qin_attack(rho)] = 1.

Lemma3 - guessing the sender's basis correctly is sufficient for recovering secret :

Pr[(gA=bA) -> guess=m_A : qin_key(rho)] = 1.

Lemma4 – guessing third party's basis is sufficient to evade detection:

Pr[(gB=bB) -> detected=0 : qin_check(rho)] = 1. [not proven]

Results: Qiskit

We implemented the broken and fixed protocol in qiskit and simulated the attacks. **Table 1** compares the statistics from the attack on the original protocol vs the fixed protocol. The original protocol is secure by detection against an outside attacker but is insecure against an insider attack.

The fixed protocol can be shown to detect even the insider attack.

Table 1: Probabilites for detection of adversary and of stealing the secret%.

Scenario	Detected per check round	Secret stolen
Outside eavesdropper	25.6%	50.5%
Charlie, measures immediately	0.0%	74.7%
Charlie, with entangled ancilla	0.0%	100.0%
Fixed ordering, simple forgery	51.3%	74.4%
Fixed ordering, entangled forgery	26.7%	75.4%

Generalizing the protocol to arbitrary sizes, **Figure 1** shows the error rates for sizes of N=3 to N=7, comparing the simulated noise models to the actual hardware. The error rate on hardware grows much faster than expected, making the protocol limited only to a few participants for now.

Conclusion

To conclude, we have done formal analysis of the original protocol, the flaw, as well as the fixed protocol; the analysis remains incomplete due to the nascent nature of the QRHL tool. We also found that QSS does not necessarily scale well with the current hardware as it is due to excess noise.

Next steps: proving the fixed protocol in a genralized way requires features of qrhl not yet implemented, but other simpler insightful lemmas might be provable. On hardware side, the error is likely reducible using conventional techniques, but its effect on adversary detection could be studied

•[1] M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing,” Phys. Rev. A 59, 1829 (1999).

•[2] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, “Cryptanalysis of the Hillery–Bužek–Berthiaume quantum secret-sharing protocol,” Phys. Rev. A 76, 062324 (2007).

•[3] D. Unruh, “Quantum relational Hoare logic,” Proc. ACM Program. Lang. 3 (POPL), 33 (2019).

•[4] A. Karlsson, M. Koashi, and N. Imoto, “Quantum entanglement for secret sharing and secret splitting,” Phys. Rev. A, vol.59, no. 1, pp. 162–168, Jan. 1999.

•This work was supported by the Mizzou Quantum Innovation Center through the summer internship program.