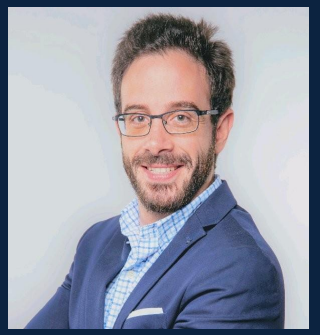
UTSA The University of Texas at San Antonio™

A Live Digital Forensics Approach for Quantum Mechanical Computers

Dayton Closser



Elias Bou-Harb

Cyber Center for Security and Analytics
The University of Texas at San Antonio

UTSA
The University of Texas at San Antonio™
The Cyber Center for Security and Analytics

9th Annual DFRWS EU 2022 Conference – March 29th - 1st, 2022

Motivation:

- **Never done before in the domain of digital forensics**
  - **Prior works only abstractions and not empirical in nature on real quantum systems**

- **Fast approaching forensic challenges for the 21st and 22nd centuries:**
  - Quantum computers are already a reality
  - No tested methodologies for handling quantum forensics

- **Digital Forensics has an enormous focus on classical computers, but enormous deficit with quantum computers**

- **Richard Overall [1] proposed that digital forensics is impossible on quantum computers:**
  - Limitations due to quantum phenomena and behavior
  - Work strictly an abstraction of concepts and theory, not empirical components

[1] Overill, Richard E. "Digital quantum forensics: future challenges and prospects." International Journal of Information Technology, Communications and Convergence 5 2.3 (2012): 205-211.

Related Work:

- **Richard E. Overill**
  - **"**Digital quantum forensics: future challenges and prospects**"**
- **Sandeep Kumar Sharma and Kamaljit I. Lakhtaria**
  - "The Role of Quantum Computing in Software Forensics and Digital Evidence: Issues and Challenges"
- **IBM Research**
  - "Qiskit Textbook - Describing quantum computers"

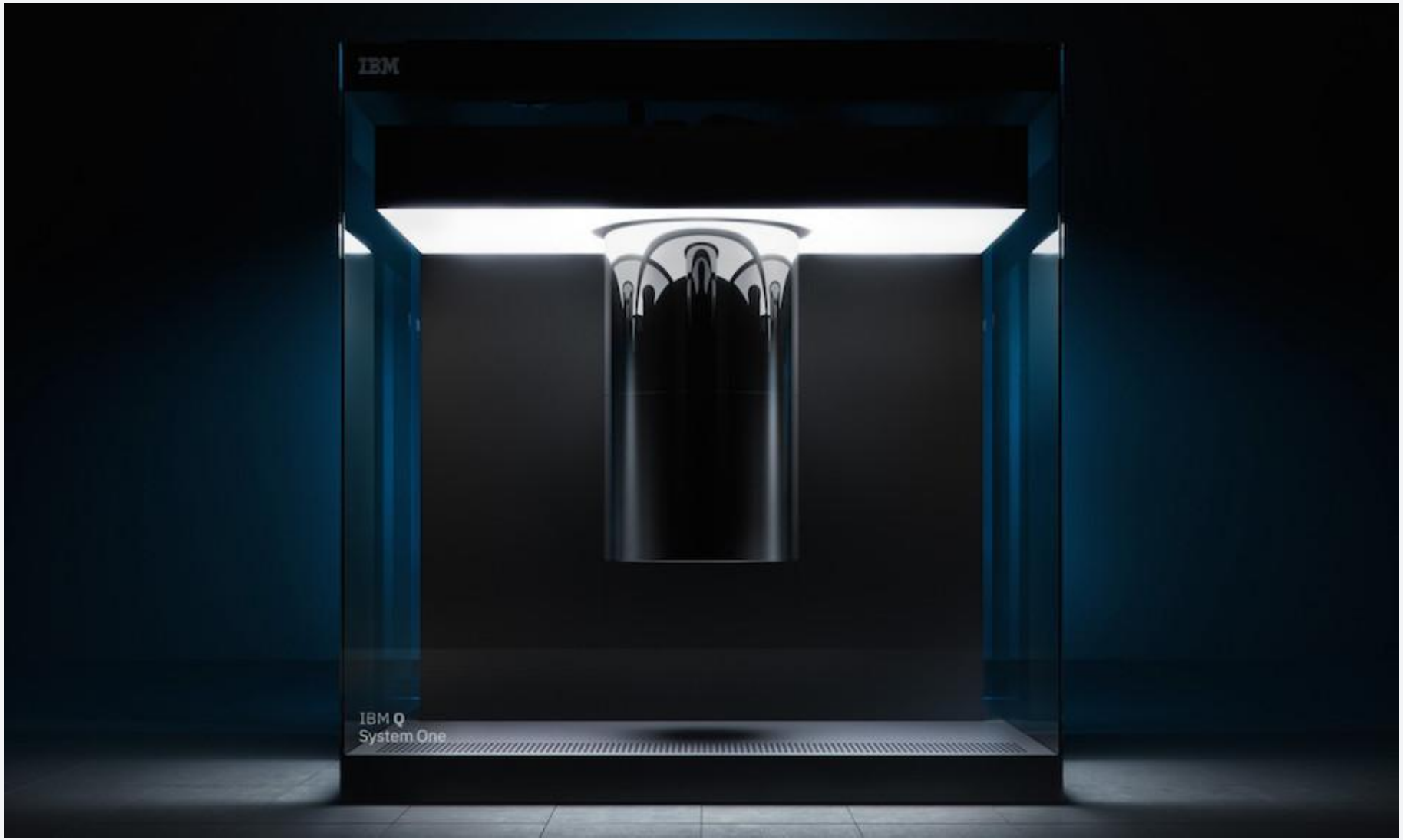
- **Up until now, no prior work focused on empirical forensic collection from real quantum computers**

Contributions:

- **We refute Overill's assertion that it is not possible to perform forensics on quantum computers:**

- **We analyze real quantum simulators and computers (never done before):**
  - IBM-Q Lima
  - IBM-Q Santiago
  - IBM Aer Simulator

- **We demonstrate a novel approach to collecting digital forensic artifacts:**
  - Gate Reversal
    - To address fidelity issues, unique quantum properties, and maintain chain of custody of evidence



[1] https://static.highsnobiety.com/wp-content/uploads/2019/01/08202808/ibm-q-system-one-commercial-quantum-computer-00.jpg/

[2] https://venturebeat.com/2021/04/09/ibm-releases-qiskit-modules-that-use-quantum-computers-to-improve-machine-learning/

Quantum primer

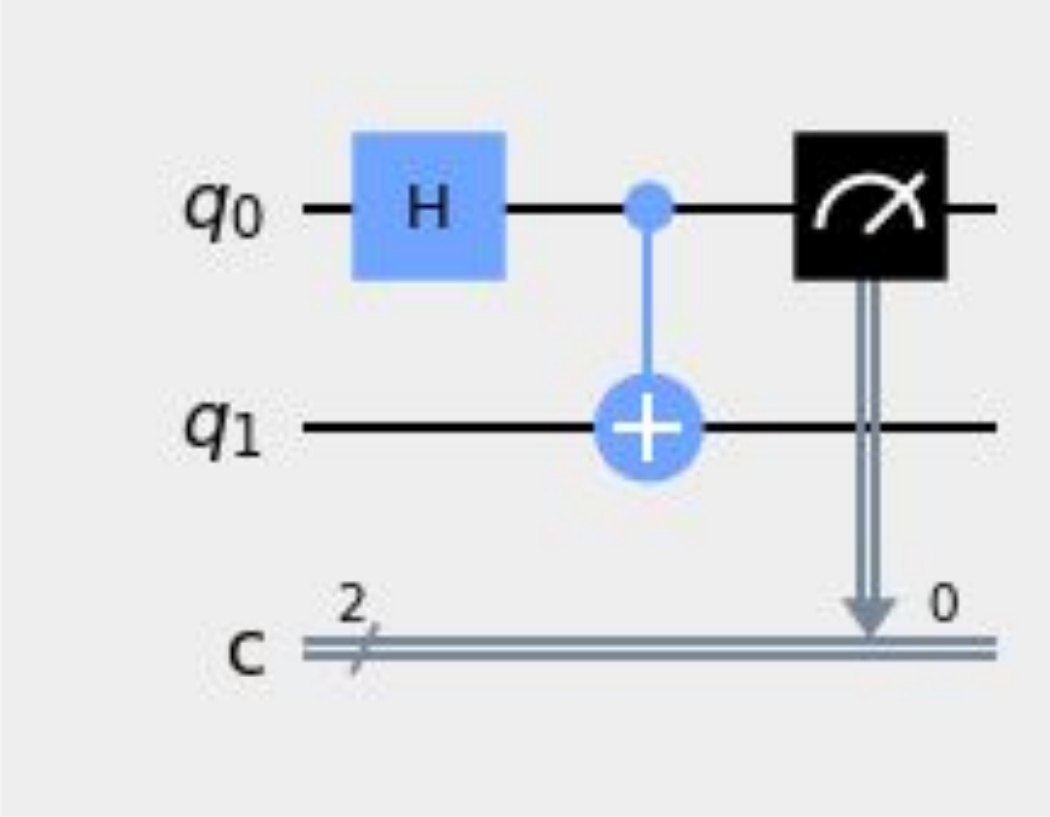
“Given for one instant an intelligence which could comprehend all the forces by which nature is animated…nothing would be uncertain”

- Marquis de Laplace, 1902

Quantum primer

- **Key concepts:**
- **1925 Schrödinger equation --** $i\hbar\Psi = H\Psi$
- **Superposition** -- a special mixture of the energy levels
- **Entanglement** -- case where elements cannot be described independently of one another
- **NISQ** – Noisy Intermediate Scale Quantum

- **One of Quantum computing's key differences is that binary values in exotic states may exhibit the values:**
  - *1, 0, or 1 and 0* ***simultaneously***



Quantum primer

- Logic of quantum computers not strictly binary
- Quantum versus classical logic gates
- States of data those signals represent “very consequential” for investigators
- **Quantum operational approach:**
  - Preparation: The logic is crafted for use
  - Quantum state: The logic is executed
  - Measurement: The results of the logic are recorded

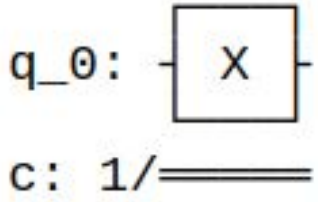
Table 1. Quantum gate corollaries to Classical gates

Quantum	Corollary to:	Classical
Pauli X	=	NOT
“controlled” not cnot	=	XOR
“Toffoli” ccnot (Deutsch)	=	AND
NAND gate	=	Two NOTs
cswap gate	≠	No equivalent
Hadamard	≠	No equivalent
Pauli- Y and Z Gate	≠	No equivalent

Data Collection:

- Implemented simulator and real NISQ systems
- Leveraged IBM Quantum Experience and Qiskit
- Linux and NetBSD systems, we have devised Qubit circuits with Qiskit
- Programming preparation phase in Python Jupyter-Notebooks
- At runtime, program executed on the IBM Quantum Experience Service for quantum computation

```
qc = QuantumCircuit(1,1)
# quantum and classical circuit
qc.x(0)
#Pauli X Gate
qc.draw()
# display function of circuit
```

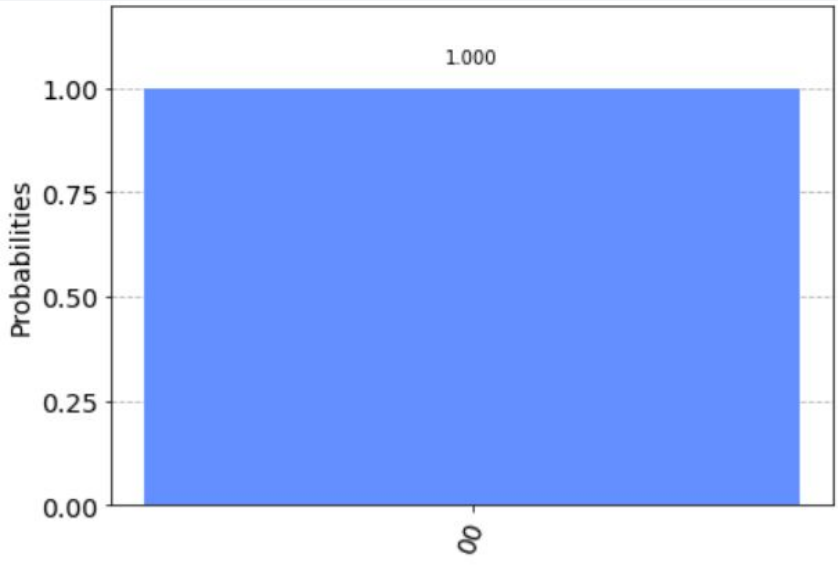


Methodology and Empirical Results: Gate reversal

"Think of reversal like a domino game. After the dominoes collapse into chaos, the exact alignment of them can only be restored if they are replaced by the exact displacements from their undisturbed state."

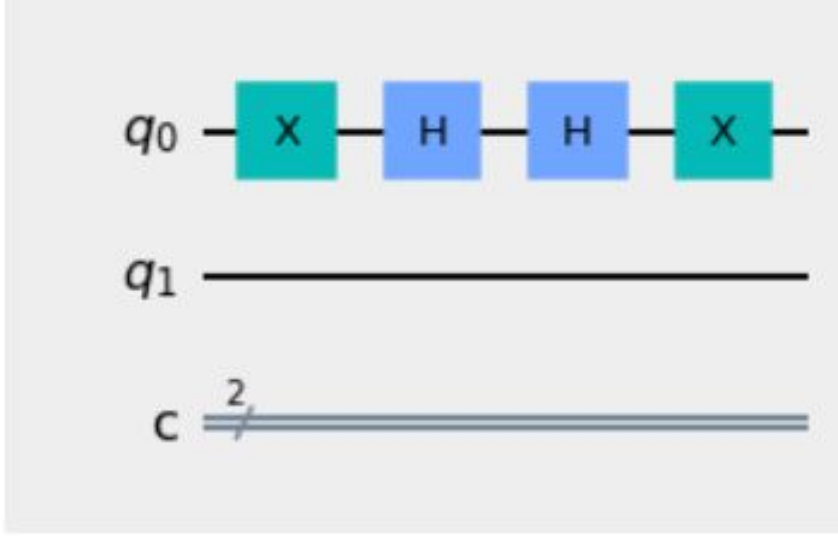
[3] https://sbly-web-prod-shareably.netdna-ssl.com/wp-content/uploads/2020/06/05141558/cats1.png

Methodology and Empirical Results: Gate Reversal

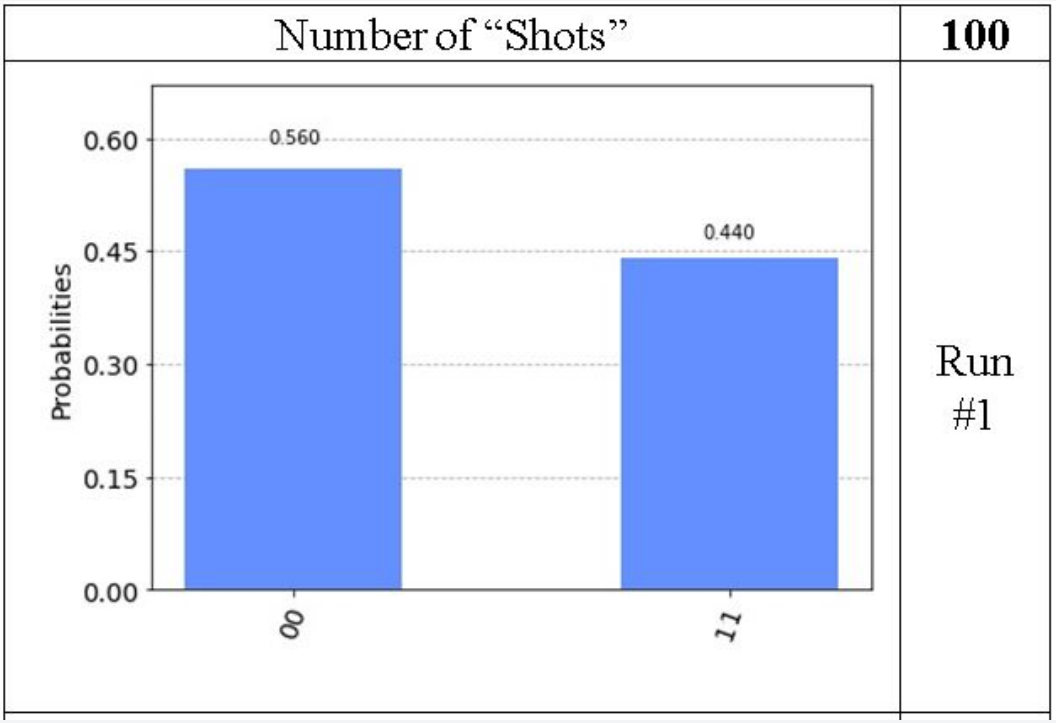


Steps to take include:

- Ensure the initialized value of the qubit is 0
- Review the logic of the original circuit
- In our case, apply Hadamard, then Pauli-X gates in reverse order on q0
- Ensure that any reversal “mirrors” the initial application
- Ensure probabilities produce the initial state (all probabilities add to unity, or 1)



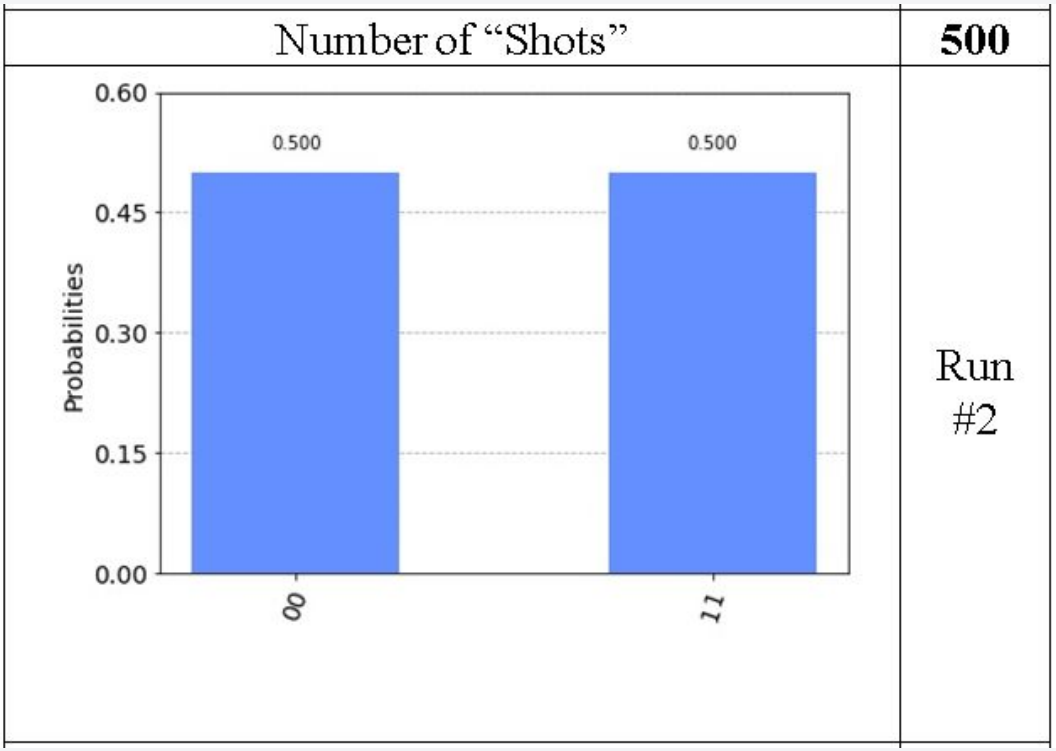
Methodology and Empirical Results: Gate Reversal Noise and Errors



Possible issues:

- Real hardware presently is extremely noisy

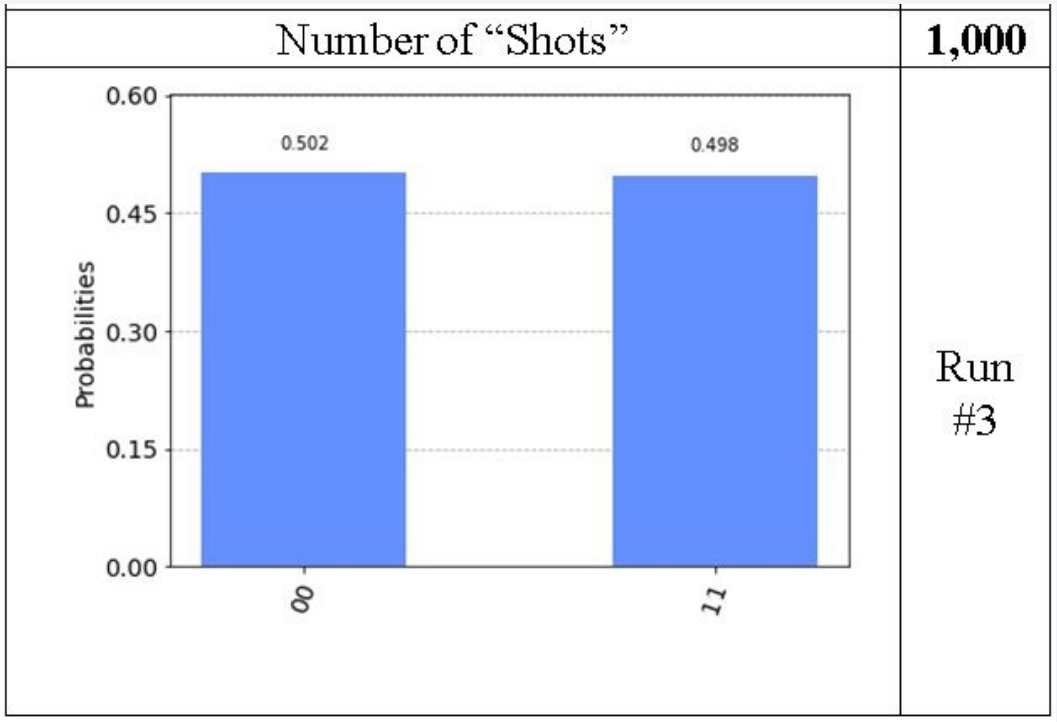
Methodology and Empirical Results: Gate Reversal Noise and Errors



Possible issues:

- Real hardware presently is extremely noisy
- The number of shots effectively shows error with each run

Methodology and Empirical Results: Gate Reversal Noise and Errors



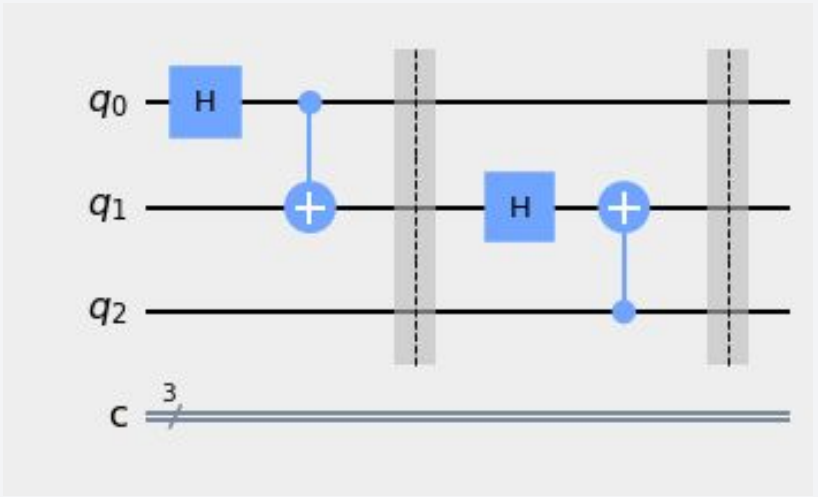
Possible issues:

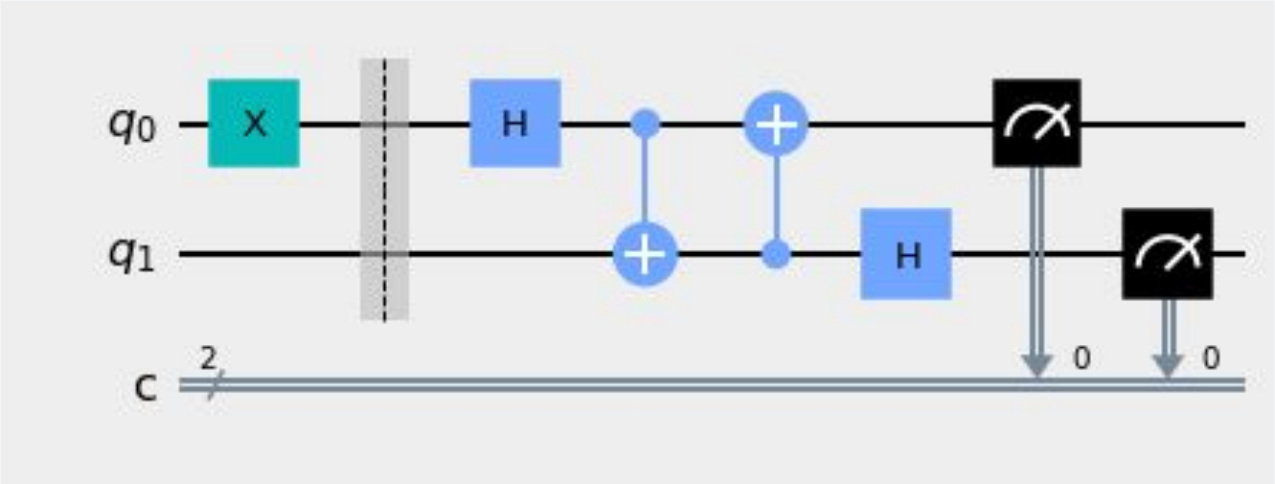
- Real NISQ hardware presently is extremely noisy
- The number of shots effectively shows error with each run
- The results theoretically should be 50/50 with a Hadamard, however as tested on real hardware, this varied significantly
- Note to investigator, gate reversal approach helps establish fidelities otherwise questionable

Methodology and Empirical Results: Gate Reversal Entangled cases

- The qubits may be initialized, and entangled by a third-party

- If the q0 is entangled, it could be transmitted to a second party, before it is encoded. In other words, the proverbial message sent before it is written, and then written later or perhaps never at all.

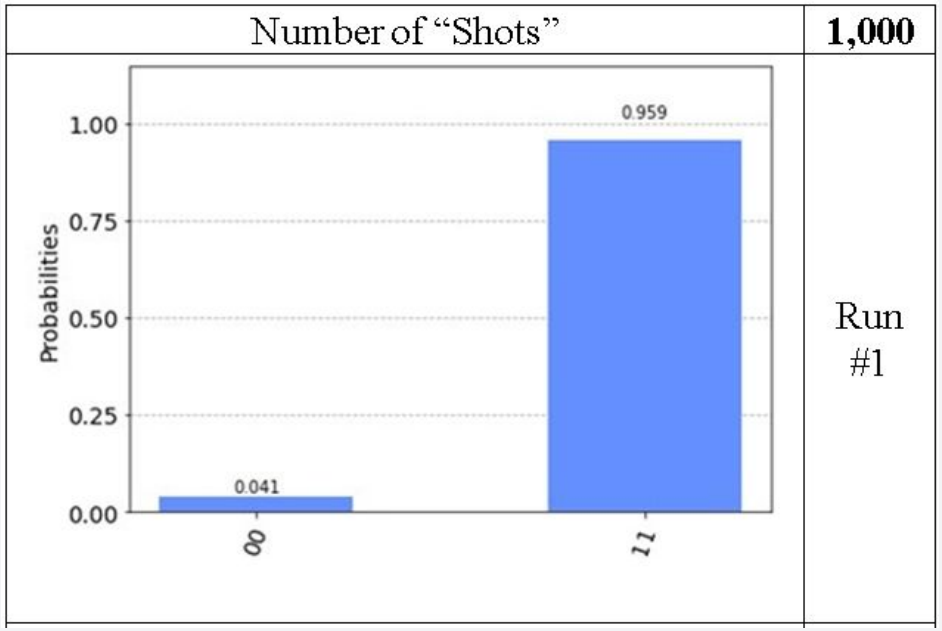


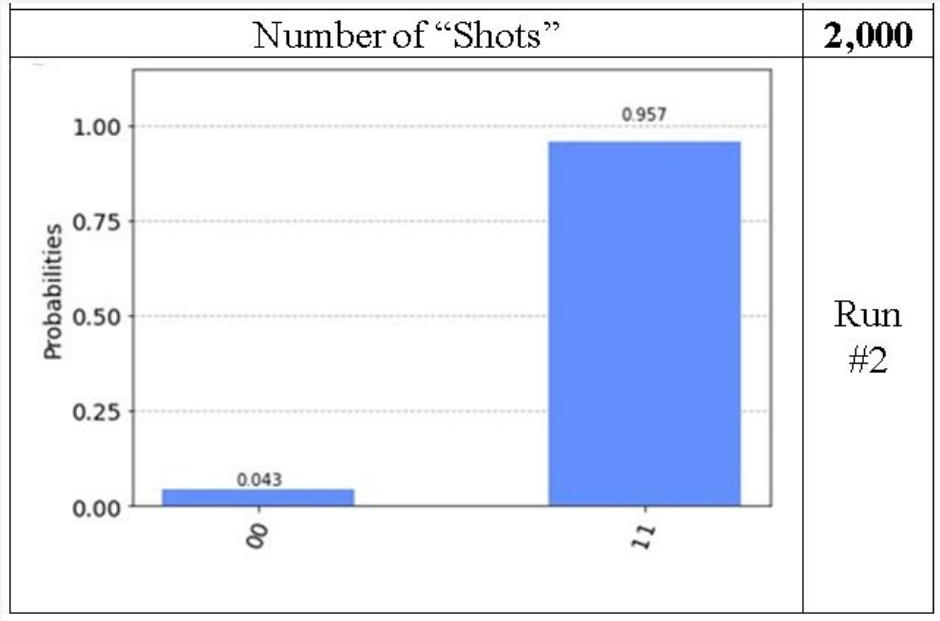


Bell State

Encoded Quantum Bell State

Methodology and Empirical Results: Gate Reversal Noise and Errors





Bell State Recovery Results:

- Roughly 5% error at 1,000 and 2,000 shots
- We were with high-confidence (95%) to recover original values

Live Forensic Implications

Richard Overill's assertion that it is not possible to perform live forensics on quantum systems is misleading and incorrect because, measurement of a quantum superposed, and entangled state is not entirely necessary to determine data input into a quantum system, gates are.

Future Work:

- Quantum Anti-forensics with deferred measurement
- Quantum Hardware approaches
- Quantum computers and relationships with people
- Quantum post-mortem forensics

Acknowledgements

- We thank the reviewers and our Shepherd for their constructive feedback that greatly enhanced this work. This work was partially supported by a grant from the U.S. National Science Foundation (NSF), Office of Advanced Cyberinfrastructure (OAC), #2104273.

- We acknowledge the use of IBM Quantum services for this work. The views expressed are those of the authors, and do not reflect the official policy or position of IBM or the IBM Quantum team. Special thanks to the NetBSD foundation, the Qiskit Community, and all other open-source projects for their efforts in providing quality software for research. Special thanks to Qiskit for their excellent documentation.

- Lastly, special thanks to UTSA quantum mechanics professor Dr. Tyler Sutherland for his advice and counsel regarding technical concepts, and support in making this paper possible.

Thank You!