Analysis and Implementation of Quantum Computing Algorithms

Caroline Fedele[1], Asai Asaithambi[2]

[1]Department of Physics, University of North Florida, [2]School of Computing, University of North Florida

Objectives

- Develop new circuit models & reliable method for quantum processing
- Analyze execution time complexity and memory required for the solution of some classical problems using both systems
- Simulate Shor's algorithm for quantum integer factorization, showing break down of classical RSA cryptography scheme.

What is Quantum Computing?

Quantum computing is a new and very powerful paradigm in the field of computing, capable of revolutionizing capabilities of many industries including the medical field, materials science, economics, machine learning, and cybersecurity. Quantum computers are now being physically developed at IBM and Google but there exists a gap between what they can do theoretically and what has been put into practice. The aim of this research is to help close that gap. We will build quantum circuits to represent algorithms and test in a quantum computer simulation. The inherent parallelism of quantum computing allows us to efficiently solve problems classical computers cannot. We observe quantum computing supremacy with problems deemed *intractable*: the solution can only be found through exhaustive search. Among these is one extremely relevant to cybersecurity, known as **Shor's algorithm**, an efficient algorithm for integer factorization, which breaks down well-established methods of cryptography. An aim of this research we will specifically demonstrate how Shor's algorithm can be built in a quantum system.

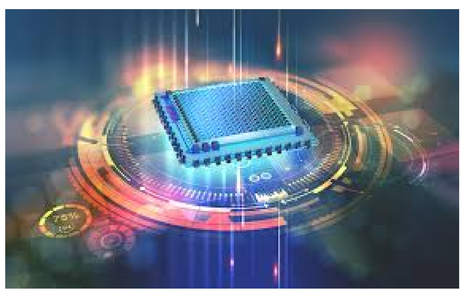

Figure 1:qubit graphic rendering

Relevance to Cybersecurity

It is vital we study quantum computing and be prepared when physical systems become sufficiently advanced, particularly because of its threat to encryption integrity. Almost all methods governing secure data transmission are based on one difficult math problem that makes up the RSA cryptosystem: the problem of finding two prime factors of large integers (order of 10^{100} digits). One quantum algorithm, **Shor's algorithm**, breaks this down completely. This algorithm utilizes modular arithmetic as well as existing quantum algorithms, the quantum Fourier transform and modular exponentiation, to reduce this from an NP-problem (exponential time complexity) to a P-problem (polynomial time complexity).

Key Goal: A Reliable & Accurate Quantum System

Building circuits of existing **quantum algorithms**, including Shor's algorithm, and investigating possible new algorithms.

Physics & Mathematics

Superposition: allows qubit to be in state of 0 and 1 simultaneously. A bloch sphere (below) represents qubit state space.

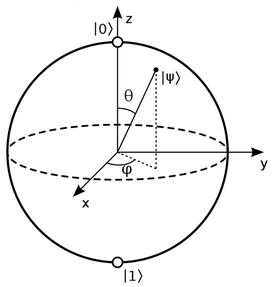

Figure 2:Bloch sphere: visualization of qubit state-space

Qubit: represented by any 2-D superposition of states.

Fourier Transform: key transformation acting on a quantum state.

Modular Exponentiation: method of exponentiation performed over a particular value, the modulus, another key algorithm in quantum computing.

Plan to Utilize Quantum Regime

Necessary steps: background research

1. Mathematical & literature review
   - understand fundamental physics - quantum mechanics, especially *superposition* and *entanglement*
   - understand mathematics of parallel computing and algorithm development
   - scour existing literature, know what has been tried
2. Investigation of classical vs. quantum algorithms
   - program classical algorithm using java, obtain time complexity & memory information
   - analyze problems mathematically to develop/understand quantum algorithms
3. Implementation of Shor's Algorithm
   - Use QISkit (IBM's online quantum tool) for existing quantum algorithms to develop reliable approach.
   - demonstrate approach and build quantum circuit for Shor's algorithm.

Expected outcome

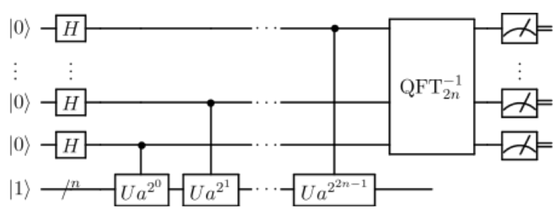

Figure 3:example Shor's algorithm subroutine

Using qiskit, a quantum computer simulation, we can register qubits to the appropriate functions for a given algorithm, and thus build quantum algorithms.

Qiskit

Figure 4:Qiskit: program for building quantum circuits

Conclusion

There is currently a gap between proposed superior quantum solutions and problems demonstrably solved using quantum algorithms. By following the steps proposed in this research plan, coming one step closer to closing that gap between theory and practice. It is important to explore and advance our knowledge of quantum computing so we are prepared for when it, and so that in the future our understanding of encryption is deepened and new quantum-proof methods can be developed.

- **State of project:** much of technical background review has been completed. Investigation of quantum algorithms and implementation of Shor's algorithm are the proposed next steps of this study.

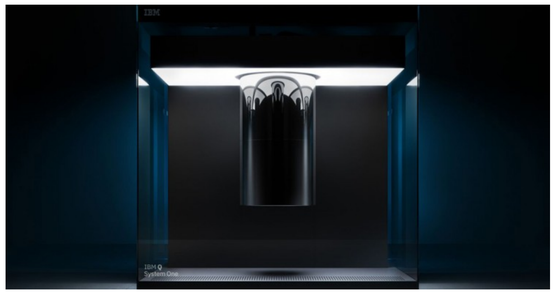

Figure 5:IBM 53-qubit Quantum Computer

References

[1] Martonosi, M. and Roetteler, M. "Next Steps in Quantum Computing: Computer Science's Role." November 2018.

[2] Baumhof, Andreas. "Breaking RSA Encryption – An Update on the State-of-the-Art." June 2019.

Acknowledgements

Many thanks to my mentor, Asai Asaithambi, for instructing me in this subject, and to the UNF Physics and Computing departments for facilitating this opportunity.

UNF UNIVERSITY of NORTH FLORIDA