Shor's Algorithm: How Quantum Computing Affects Cybersecurity

Caroline Fedele[1,3], Asai Asaithambi[2]

[1]University of North Florida, Department of Physics, [2]University of North Florida, School of Computing, [3]NASA Goddard Space Flight Center

Motivation: Cybersecurity

RSA encryption, developed by Rivest, Shamir, and Adleman, makes up much of online security today. We rely on it every day when using web browsers, email, online banking, and any site that begins with 'https://' to protect online privacy. The basis of RSA is a mathematical problem known as *prime factorization*, where the goal is to find the prime factors, p and q of a given number N.

$$N = pq$$

If N is large enough, it is nearly impossible to recover p and q, making RSA practically impossible to hack. This assumption fails however when quantum computing, in particular Shor's algorithm, is introduced. Fig. 1 is one of today's quantum computers.

Figure 1: IBM's 50 qubit quantum computer

Important Definitions

- *Encryption*: process of encoding (securing) information, turning it into a garbled message for anyone who does not have a key to decode the information with.
- *Algorithm*: finite set of well-defined instructions for the computer to solve problems, process data, and learn from information.
- *Quantum Computing*: a completely different method of computation, utilizing a uniquely quantum mechanical principle, *superposition*

Goal: Build and Demonstrate Shor's Algorithm

Write a computer program that simulates Shor's algorithm for quickly finding prime factors.

Time Complexity

A foundational part of algorithm development is time complexity. How does the time it takes a computer to complete a task scale with the amount or size of information input? **Exponential time** algorithms fail with large enough inputs, including classical prime factorization. The best known algorithm on the biggest supercomputers would still take 3000 years to factor a standard RSA, 10^{250} digit number (Fig.2). *Superposition* allows quantum computers to perform a huge number of computations simultaneously, the basis for the speed-up in quantum algorithms. *Shor's algorithm* turns factorization into a feasible, **polynomial time** problem.

Size of *N*	Classical	Quantum
RSA-250 (10^250 digits)	3000 years	Minutes
RSA-600 (10^600 digits)	>15,000,000,000 years	Hours

Figure 2: estimated classical vs. quantum factoring times

Method: Steps

1. Choose random number $a < N$ (classical step)
   Use Euclid's algorithm to find relatively prime a and N
2. Use period-finding subroutine to find period r of function, $f(x) = a^x mod(N)$. (quantum step)
   This step is where the quantum advantage comes in. It outputs only certain values with a high probability of yielding the period.

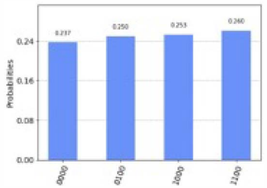

Figure 3: values determined by quantum subroutine

3. Extraction of the Period (classical step)
   Based on the measured values above, the period can be extracted by mathematical manipulation.

*This is a vast simplification of the mathematics behind Shor's algorithm

Results: Shor's Algorithm Program

We successfully demonstrated this use of both classical and quantum computation by using the python programming language for classical elements of this algorithm and a program called qiskit for the quantum elements. Qiskit is IBM's quantum simulation program, which allows virtual access to their quantum computer for tasks within the scope of the 50 qubit system. The circuit below (Fig.4) is a visual of Shor's step 2.

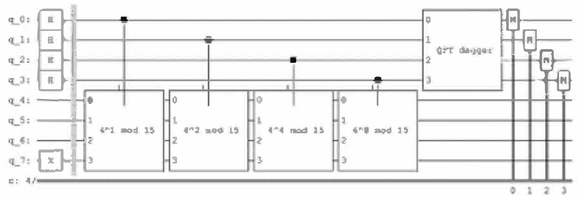

Figure 4: quantum circuit for our Shor's algorithm step 2 with 4 input qubits, factoring 15

Discussion

Fig. 5 shows our experimental comparison between a standard classical factoring algorithm and our implementation of Shor's algorithm. Because the number of input qubits available is only 32, 123 was the maximum number Shor could factor. The classical program was very efficient until numbers of about 10^{10} digits long. 10^{232} is classical computing's absolute known maximum. Quantum computing, in theory, will easily be able to factor 10^{600} once computers with 1000's of qubits exist.

N	Classical	Quantum
15	<1 sec	8.1857 sec
69	<1 sec	548.1165 sec
111	<1 sec	979.5129 sec
123	<1 sec	947.2438 sec
10^9	18 min	needs >32 qubits
*10^232	number field sieve	needs 1000s qubits
*10^600	intractable	needs 1000s qubits

*RSA standard N-size

Figure 5: classical vs. quantum testing results

Does Shor's algorithm put all internet security at risk? Not right now, but as quantum computers progress so must encryption schemes. Currently research is being done in quantum and post-quantum cryptography so we are prepared when 10,000-qubit quantum computers are developed.

References

[1] Asfaw, A. et. al. (2020). "Learn Quantum Computation Using Qiskit."
http://community.qiskit.org/textbook
[2] Rieffel, Eleanor Polak, Wolfgang. (2011). "Quantum Computing A Gentle Introduction."

Acknowledgements

Many thanks to my instructor, Asai Asaithambi, to branch 566 and my colleagues at NASA, and to the Office of Undergraduate Research for creating this opportunity.