Shor's Algorithm: A Quantum Leap in Factorization

Lets Decrypt the Algorithm

Tyler Rose

t.atwood.rose@gmail.com
Euler Circle

July 16, 2024

Overview

The Cryptographic Landscape

- As of 2021:
  - 52% of HTTPS servers use RSA
  - 75% of digital certificates use RSA
- Safeguarding trillions of online transactions
- But a quantum storm is brewing...

Image Source: https://threatpost.com/why-web-browser-padlocks-shouldnt-be-trusted/159659/

Key Point

RSA encryption is the backbone of current internet security.

The Quantum Revolution

- Quantum computing is evolving rapidly
- Quantum volumes increasing 10 fold yearly since 2020
- Potential to completely shift the cryptographic landscape

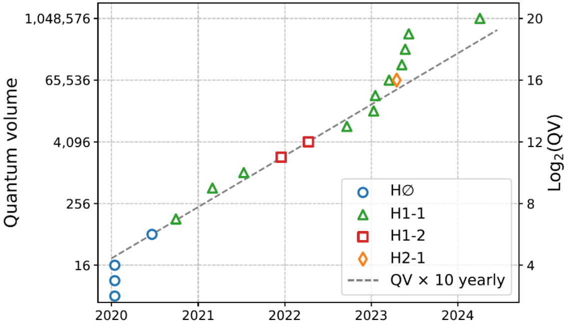


Image: Exponential growth of quantum volume (https://www.quantinuum.com/news/quantinuum-extends-its-significant-lead-in-quantum-computing-achieving-historic-milestones-for-hardware-fidelity-and-quantum-volume)

The Problem of Integer Factorization

- Central problem in number theory and computer science
- Difficulty increases exponentially with number size
- Example: Factoring a 2048-bit number
  - Classical computers: Billions of years
  - Quantum computers with Shor's algorithm: Hours or days
- Forms the foundation of many cryptographic systems, especially RSA

Definition: Integer Factorization

The process of decomposing a composite number into a product of smaller integers.

Peter Shor and His Algorithm

- Peter Shor: American mathematician and MIT professor
- Developed Shor's algorithm in 1994 at AT&T Bell Laboratories
- One of the algorithms to show quantum computers could exponentially outperform classical computers on a problem of wide interest
- Sparked intense interest in quantum computing and quantum-resistant cryptography

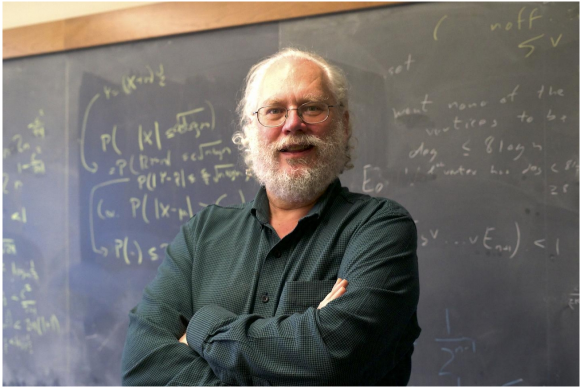


Image: Peter Shor

The Breakthrough: Polynomial-Time Factorization

- Shor's algorithm: Integer factorization in polynomial time on a quantum computer
- Dramatic improvement over classical methods
- Can factor an n-bit number in $O(n^3)$ time and $O(n)$ space
- Implications:
  - Many current cryptographic systems will be vulnerable to attack
  - Need for quantum-resistant cryptography

Key Insight

Shor's algorithm reduces factoring to finding the period of a quantum function.

Qubits: The Fundamental Unit

- Qubit: Quantum bit, the basic unit of quantum information
- Unlike classical bits, qubits can be in superposition
- Represented as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- α and β are complex numbers: $|\alpha|^2 + |\beta|^2 = 1$

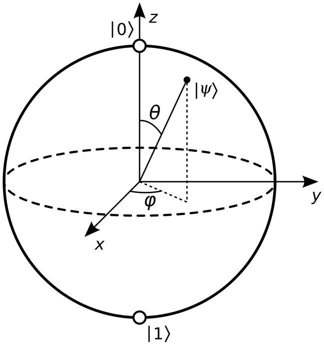


Image: Bloch sphere representation of a qubit

Superposition Principle

A qubit can exist in a superposition of multiple states until measured.

Quantum State Representation

- Quantum states are represented by vectors in complex Hilbert space
- For a single qubit:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- General state:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

- Multiple qubits: tensor product of individual qubit states

Key Point

The state space grows exponentially with the number of qubits!

Tensor Product: Combining Quantum Systems

- Tensor product () combines individual qubit states
- For two qubits $|\psi_1\rangle = a|0\rangle + b|1\rangle$ and $|\psi_2\rangle = c|0\rangle + d|1\rangle$:

$$|\psi_1\rangle \otimes |\psi_2\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

- State space grows exponentially: n qubits require 2^n amplitudes

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

Key Point

Tensor product enables description of multi-qubit systems!

Quantum Fourier Transform (QFT)

- Quantum analogue of the classical Fourier transform
- Crucial component in many quantum algorithms, including Shor's
- Transforms quantum state from computational basis to Fourier basis
- For an n-qubit state $|x\rangle$:

$$QFT|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi ixy/2^n}|y\rangle$$

- Can be implemented efficiently using $O(n^2)$ quantum gates

QFT Superpower

QFT can extract periodicity information from quantum states!

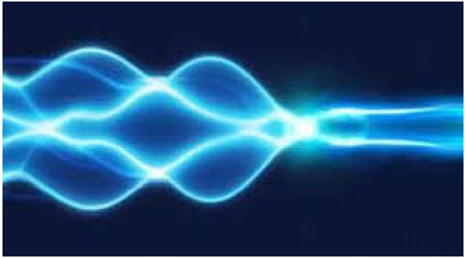
Quantum Parallelism and Interference

Quantum Parallelism:

- Ability to perform operations on many computational states at the same time
- Enabled by superposition
- Example: Evaluating a function for multiple inputs

Quantum Interference:

- Amplitudes can interfere constructively or destructively
- Crucial for extracting useful information from quantum computations



Quantum interference

Key Insight

Quantum parallelism and interference are key to quantum speedups!

Reducing Factoring to Period Finding

- Key insight: Factoring can be reduced to finding the period of a function
- For a number N to be factored, define:

$$f(x) = a^x \mod N$$

  where a is coprime to N
- This function is periodic: $f(x) = f(x + r)$ for some r
- Finding this period r can lead to factors of N

Key Point

Period finding is hard classically but efficient quantumly!

From Period to Factors

- If we find the period r:
  - Compute $a^{r/2} \mod N$
  - If this equals $\pm 1 \mod N$, try next a
  - Otherwise, $\gcd(a^{r/2} \pm 1, N)$ likely gives a factor
- Example: For $N = 15, a = 7$
  - Period $r = 4$
  - $7^2 \mod 15 = 4$
  - $\gcd(4 - 1, 15) = 3$ and $\gcd(4 + 1, 15) = 5$

Overview of Shor's Algorithm

1. Quantum state preparation
2. Modular exponentiation
3. Quantum Fourier Transform
4. Measurement and classical post-processing

Step 1: Quantum State Preparation

- Initialize two quantum registers:
  - Input register: $n = 2\lceil \log_2 N \rceil$ qubits
  - Output register: $\lceil \log_2 N \rceil$ qubits
- Apply Hadamard gates to create superposition:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle$$

Key Point

This superposition allows us to evaluate the function for all inputs simultaneously!

Step 2: Modular Exponentiation

- Apply the function $f(x) = a^x \mod N$ to the superposition:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |a^x \mod N\rangle$$

- Implemented using controlled modular multiplication
- Most computationally intensive part of the algorithm

Step 3: Quantum Fourier Transform

- Apply QFT to the input register:

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} e^{2\pi i x y / 2^n} |y\rangle |a^x \mod N\rangle$$

- Transforms periodicity in function values to phase differences
- Efficient implementation using $O(n^2)$ gates

Key Insight

QFT allows us to extract period information efficiently!

Step 4: Measurement and Classical Post-processing

1. Measure the input register to obtain y
2. Use continued fraction expansion to find r' approximating $\frac{2^n}{y}$
3. Check if $a^{r'} \equiv 1 \pmod{N}$
4. If r' is even, compute $\gcd(a^{r'/2} \pm 1, N)$
5. If we find a non-trivial factor, we're done; otherwise, repeat

Success Probability

The algorithm succeeds with probability $\Omega(1/\log\log N)$ per iteration

Implications for Cryptography

- Shor's algorithm threatens RSA and other public-key cryptosystems
- Need for quantum-resistant cryptography:
  - Lattice-based cryptography
  - Hash-based signatures
  - Code-based cryptography
  - Multivariate cryptography
- NIST Post-Quantum Cryptography Standardization

Key Point

We need to prepare for a post-quantum cryptographic landscape!

Current State and Future Prospects

- Largest number factored using Shor's: 21 (as of 2012)
- Challenges:
  - Quantum error correction
  - Maintaining coherence
  - Scaling up number of qubits
- Ongoing research to improve implementation
- Potential impact beyond cryptography

Recap and Final Thoughts

- Shor's algorithm: A quantum solution to integer factorization
- Exponential speedup over classical algorithms
- Key components:
    - Quantum parallelism
    - Period finding
    - Quantum Fourier Transform
- Significant implications for cryptography and beyond
- Drives development in quantum computing and post-quantum cryptography

Final Thought

Shor's algorithm exemplifies the transformative potential of quantum computing!