Shor we can! or No Shor Thing?

Samuel C, Ljosha K, Daric Zhou

University of California, Santa Barbara

Abstract

TODO: write a brief summary of what we talk about in the poster TODO: make sure to put in your names and everything as well at the very top in the title.tex file.

Cryptography and RSA

TODO: Insert visual graphic (YES THIS CAN BE CARTOON-ISH) depicting the correspondence between Bob, Eve, and Alice. (This will get across the point of who the "actors" are in our "story", and who is sending a message to whom.)

Fermat's Little Theorem

For any $x \in \mathbb{Z}$, we have $x^{\varphi(n)} \equiv 1 \pmod{n}$, where φ is the *Euler φ function*:

$$\varphi(m) = \#\{\text{integers } 1 < k < m \mid \gcd(k, m) = 1\}$$

The RSA Algorithm

Bob's Private Knowledge

$p = 17$ $\quad q = 5$

$n = pq = 85$ $\quad \varphi(n) = (p-1)(q-1) = 64$

$e = 7$ $\quad d \equiv e^{-1} \pmod{\varphi(n)} = 55$

Bob's Public Key

$n = 85$ $\quad e = 7$

Bob Checks

p and q are prime

$\gcd(e, \varphi(n)) = 1$

Alice Computes

Encode her message m as the number $m = 11$

Compute $c \equiv m^e \pmod{n}$ or $71 \equiv 11^7 \pmod{85}$

and sends c to Bob

Bob Decrypts

I compute $c^d \pmod{n}$ and get

$71^{55} \equiv 11 \pmod{85}$

because, by Fermat's Little Theorem,

$c^d \equiv m^{ed} \equiv m^{1+\beta\varphi(n)} \equiv m \pmod{n}.$

Eve Wants to Know

I know $85 = pq$ for *some* primes p and q.

If I knew p and q, then I could compute $\varphi(n) = (p-1)(q-1)$.

Then I could compute $d \equiv e^{-1} \pmod{\varphi(n)}$, and decrypt any messages sent to Bob with this public key.

But what are the prime factors of 85???

Eve Interferes and accesses c, but...

I only see c, n, and e. I know that $c \equiv m^e \pmod{n}$, but I can't figure out what m is.

Quantum Computing

Based on qubits with standard bra-ket notation: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ which can be represented by the Bloch sphere. The kets are basis states and α, β are probability amplitudes such that $|\alpha|^2 + |\beta|^2 = 1$. Operations on qubits are performed through quantum logic gates. Quantum probability amplitudes can be destructive since they are not necessarily positive, unlike classical probability amplitudes.

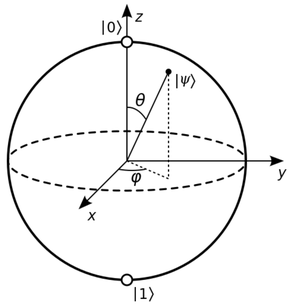


Fig. 1: The Bloch Sphere

Image from [1]

Similar to regular bits, qubits are measured to be in one basis state due to Quantum Measurement Theory. If in the Bloch sphere we can only have 1 or 0 for example, similar to a regular bit we can only measure one or the other. Due to the nature of qubits, you can store much more information since it can be a superposition of the states. In other words the classical bit is a qubit in a standard basis state. Similar to classical computing, Quantum computing system have logical gates that can perform operations on the qubits. These linear transformations can act as matrix operators. One you will need to know for a full understanding of Shor's Algorithm is the Hadamard gate. This gate performs a rotation of π in the Bloch sphere.

Quantum Fourier Transform

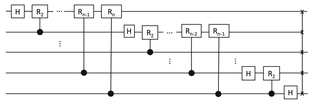


Fig. 2: Quantum Fourier Transform

Image from [3]

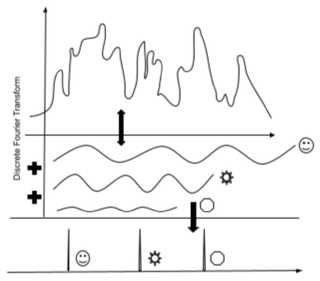
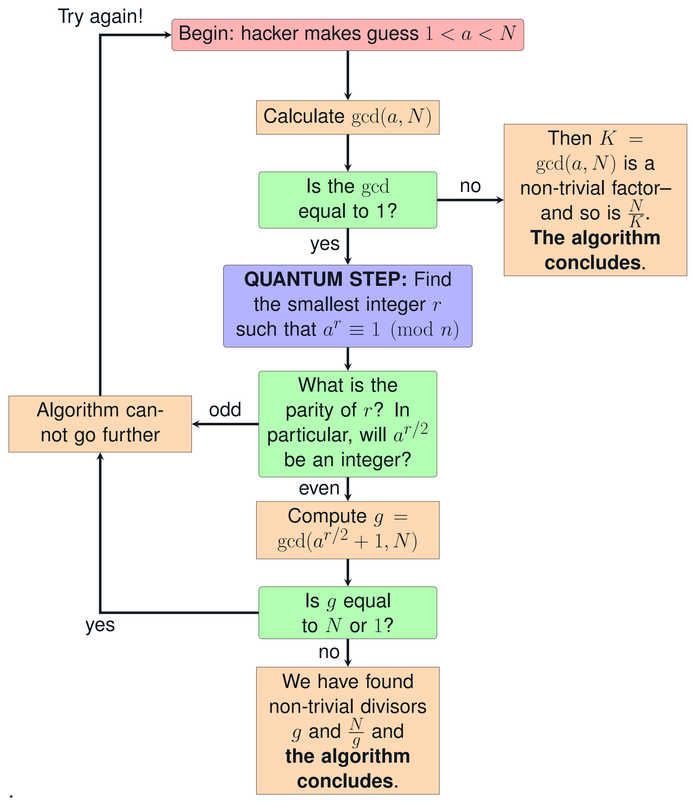


Fig. 3: Discrete Fourier Transform

The Discrete Fourier Transform takes a sequence (a discrete function) and through a matrix that looks like a matrix of powers of $\omega_N = e^{-i\pi/2}$. This is useful for the transformation of the sequence into a frequency function that can break down an otherwise incomprehensible function. An example of this is shown above. A Quantum Fourier transform instead takes an input of a wave function $\psi = \sum a_k|k\rangle$ and outputs another wave function that will start at 0 and fix any offset we will see with previous transformations in Shor's algorithm (next section).

Shor's Algorithm



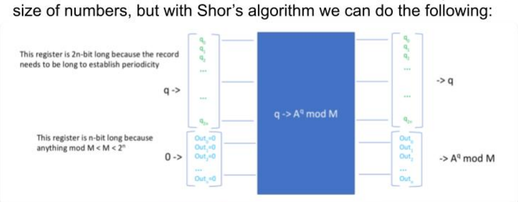
.

Shor's algorithm simply finds the periodicity, p, for the integer function.In other words, how to write A^q mod M = 1 ⇔ A^q=kM+1. For example, if M=15 and A=7 we can easily see p=4:

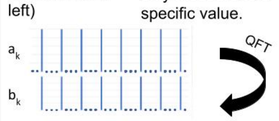
0	1	2	3	4	5	6	7
1	7	4	13	1	7	4	13

q
7^qmod15

With classical computers cost of computation of this period grows exponentially with size of numbers, but with Shor's algorithm we can do the following:



Graphically this looks like (see left)



After the quantum gate we and "entanglement" operation we get an output that needs to be put through Quantum Fourier Transform to convert the "shift" to the "phase" by nature of how superpositional measurements can only measure to a specific value.

Fig. 4: Shor's Algorithm

Image from [4]

Acknowledgements & References