Using Shor's Algorithm to Break RSA Encryption

Student Muhammad Abdullah Mutahar
Roll No 2023 – 10 – 0113
Instructor Dr. Sabieh Anwar
Course PHY 612 — An Introduction to Quantum Information Science and Technologies

Abstract

We demonstrate the physical implementation of Shor's algorithm after building its theoretical background. The fully functional quantum computer to implement Shor's algorithm is predicted to compute the prime factors in polynomial time. Quantum Phase Estimation forms the crux of this algorithm, breaking down the task of computing prime factors to finding the period of the periodic function $f(x) = a^x \mod N$. Computing prime factors in polynomial time allows us to surpass public key encryption schemes such as the RSA cryptography, which are widely used to protect the data being shared between many two parties.

Introduction

The advent of communication channels and transmission lines in the last century revolutionised the way information was transferred over larger distances. Different encryption systems and mechanisms were developed to secure the data that was being transferred. Before 1976, symmetric cryptosystems were largely used which relied on a single encryption key. This key must had to be exchanged securely over communication channels which was a major drawback.

Whitfield Diffie and Martin E. Hellman later introduced *public key cryptography* in 1976 [1], where they found a way of secure communication by using two keys, called the public key and the private key. This mechanism worked in the following manner. Suppose a person A has to send a message to a person B. B will have a set of predetermined public and private keys, where the public key will be shared with A. A will use it to encrypt the message and send it to B, where B will now use the private key to decrypt it.

This system is currently in place today because even though the public and private keys are connected, no one can easily guess the private key. Furthermore, public key cryptography needs a mathematical procedure that is straightforward to encrypt using the public key, but decrypting without the private key becomes computationally challenging and mathematically intractable on a classical computer. This mathematical term is called the trapdoor function. One example of commonly used public key cryptography which we would encounter next is the RSA mechanism and we would shortly see how the development of Shor's algorithm resulted in a possibility to break this encryption mechanism.

1 RSA Cryptosystem

R. L. Rivest, A. Shamir, and L. Adleman publicly implemented a technique for public key cryptography in 1977 [6], which came to be known as RSA cryptosystem. The technique has the following implementation composing of key generation and information transfer protocol. Any

message we want to send first has to be cut down into pieces and converted into integers. The purpose of converting it into integers is to change strings into numbers for encryption.

1.1 Key Generation

RSA technique is fundamentally established on the hardship of factoring large integers into prime numbers. The steps for generating the keys are these:

1. Choose two integers, a and b, such that a and b are prime numbers. If you randomly choose a very large number, you can do a primality test to check whether it is prime or not because the primality test is less costly than going all the way from 1 and checking all the prime numbers and then picking a large prime number from there. Typically, the 2048 bit key is used in RSA, containing 617 decimal digits.

2. Construct a composite number n such that:

$$n = a \times b \tag{1}$$

3. Compute the Euler function $\phi(a, b)$ which is defined in the following way:

$$\phi(a, b) = (a - 1)(b - 1) \tag{2}$$

4. Select a number e which is co-prime with ϕ.

5. Compute the multiplicative inverse of e defined in the following way:

$$d \times e \equiv 1 \mod \phi \tag{3}$$

1.2 Transmission Protocol

Suppose there are two people Alice and Bob. Alice makes a set of two keys with (e, n) as her public key and (d, n) as her private key. Bob wants to send a message M to Alice. He acquires Alice's public key (e, n) and the following procedure is followed for transmission:

1. Bob encrypts his message M using the public key (e, n):

$$C \equiv M^e \mod n \tag{4}$$

2. He transmits the encrypted message C to Alice via a secure communication channel.

3. Alice decrypts the message C via the following manner:

$$C^d \mod n \equiv M \tag{5}$$

The success of the RSA encryption relies on the fact that prime factorization has a high time complexity and if the number is very large, the problem becomes intractable classically. Now we would see how Shor's algorithm can help us acheive this task.

2 Shor's Algorithm

Peter Shor, an American mathematician, developed this algorithm in 1994 which could be used to compute the prime factors of a large number N in polynomial time [7]. Shor's algortihm is essentially composed of a period finding algorithm as we would see. Suppose that we have a composite number N, whose prime factors are to be computed. The algorithm works in the following manner:

1. Choose a number a, which is co-prime with N.
2. Find the period of the function $f(x) = a^x \mod N$. This reduces to finding $f(r) = 1(\mod N)$, where r is the period of $f(x)$.
3. if r is even or $a^{r/2}$ has an integer value, then proceed further. Otherwise, choose a different a.

The crux of this algorithm relies in finding the period r, which if found correctly results in instant factorisation of N. The method is as follows:

$$\begin{aligned} \left[a^{r/2}\right]^2 &= 1(\mod N) \\ \left[a^{r/2}\right]^2 - 1 &= 0(\mod N) \\ \left(a^{r/2}+1\right)\left(a^{r/2}-1\right) &= 0(\mod N) \end{aligned} \tag{6}$$

This means, either $\left(a^{r/2}-1\right)$ or $\left(a^{r/2}+1\right)$ or both share factors with N. Therefore, factors of N can either of:

$$\gcd\left(a^{r/2} \pm 1, N\right) \tag{7}$$

All computations can be performed classically in polynomial time, however, the period finding algorithm has an exponential time complexity and the problem becomes intractable for very large N. Here the usefulness of quantum computers kicks in, in terms of quantum phase estimation carried out by inverse Quantum Fourier Transform (QFT). This allows for the period r to be found in polynomial time.

Let's further discuss how a quantum computer could physically implement this algorithm. The basic idea is to construct a quantum circuit which allows us to compute the values for $f(x) = a^x$, and then find its period. We can develop an oracle V whose action is defined as follows:

$$V|x\rangle|y\rangle = |x\rangle|ay\rangle \tag{8}$$

We develop our circuit such that $|x\rangle$ is contained on the first register (control register) which is composed of m qubits and $|ay\rangle$ is contained on the second register (work register) which composes of n qubits. We restrict n such that $n = \lceil \log_2 N \rceil$, which in turn restricts the maximum value of $|ay\rangle$ and the physical stored value is $|ay \mod N\rangle$. Repeated actions of V, x number of times would yield our desired output on the second register provided $|y\rangle = |1\rangle$. This is encapsulated by our intended oracle U:

$$U|x\rangle|1\rangle = V^x|x\rangle|1\rangle = |x\rangle|a^x \mod N\rangle \tag{9}$$

The periodicity of the function $f(x) = a^x \mod N$ implies that the repeated action of V eventually results in same set of $|a^x \mod N\rangle$ after $x > r$. If we take a sum of this cyclic set, it

must be an eigenvalue of U since all the outputs would be present in that set. We define this as:

$$|V\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \left|a^k \mod N\right\rangle \tag{10}$$

This is an eigenvector of U with eigenvalue 1. We can assign phases proportional to k to each basis vector, and can also further associate these phases up to a factor s depending upon the eigenvector $|u_s\rangle$.

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} \left|a^k \mod N\right\rangle \tag{11}$$

This arbitrary eigenvector yields an eigenvalue of:

$$U|u_s\rangle = e^{\frac{2\pi i s}{r}} |u_s\rangle \tag{12}$$

In all $|u_s\rangle$, the basis state $|1\rangle$ has no phase attached to it as $k = 0$, however this is not true for the rest of the basis states. If we sum up the eigenvectors $|u_s\rangle$ of U, $|1\rangle$ would survive, however, the sum of the phases of all other basis states would add up to zero. This follows from the fact that sum of the roots of unity equal zero.

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \tag{13}$$

Hence our initial step of taking $|y\rangle = |1\rangle$ was justified in order to achieve the desired outcome from the oracle U, as $|1\rangle$ additionally turns out to be the sum of eigenvectors of U, allowing us to transmit the phase $\frac{s}{r}$ of $|u_s\rangle$ to the control registers as part of the Quantum Phase Estimation protocol. This phase encoding the period r of the function $f(x) = a^x \mod N$ could then be extracted via IQFT.

2.1 Scheme of working

2.1.1 Initialization

Prepare $|0\rangle^{\otimes m} |0\rangle^{\otimes n}$ with $m = 2n$. Apply $H^{\otimes m}$ on the control register and the NOT gate on the n^{th} qubit on the work register, thus creating a superposition of 2^n states on the control register and $|1\rangle$ on the work register.

$$|0\rangle^{\otimes m} |0\rangle^{\otimes n} \to \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |1\rangle \tag{14}$$

2.1.2 Modular exponentiation function (MEF)

Apply the unitary operation U that implements the modular exponentiation function $a^x \mod N$ on the work register whenever the control register is in state $|x\rangle$:

$$\begin{aligned} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |1\rangle &\to \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \left|a^x \mod N\right\rangle \\ &= \frac{1}{\sqrt{r2^n}} \sum_{s=0}^{r-1} \sum_{x=0}^{2^n-1} e^{i2\pi s x/r} |x\rangle |u_s\rangle \end{aligned} \tag{15}$$

2.1.3 Inverse Quantum Fourier Transform (QFT)

Apply the inverse quantum Fourier transform on the control register:

$$\frac{1}{\sqrt{r2^n}} \sum_{s=0}^{r-1} \sum_{x=0}^{2^n-1} e^{i2\pi sx/r} |x\rangle |u_s\rangle \rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\phi_s\rangle |u_s\rangle \tag{16}$$

2.1.4 Measurements

Measure the qubits of the control register in computational basis. The inverse QFT yields peaks in probability of the states $|\phi_s\rangle$ where $\phi_s \approx 2^n s/r$. There is a high probability of obtaining the location of the these peaks after only a few runs. The number of qubits m determine the accuracy of ϕ_s.

2.1.5 Continued fractions

Compute $\phi = \phi_s/2^n$ and then apply continued fractions to ϕ with maximum denominator value of N in order to extract r from the convergents.

2.2 Quantum Circuit

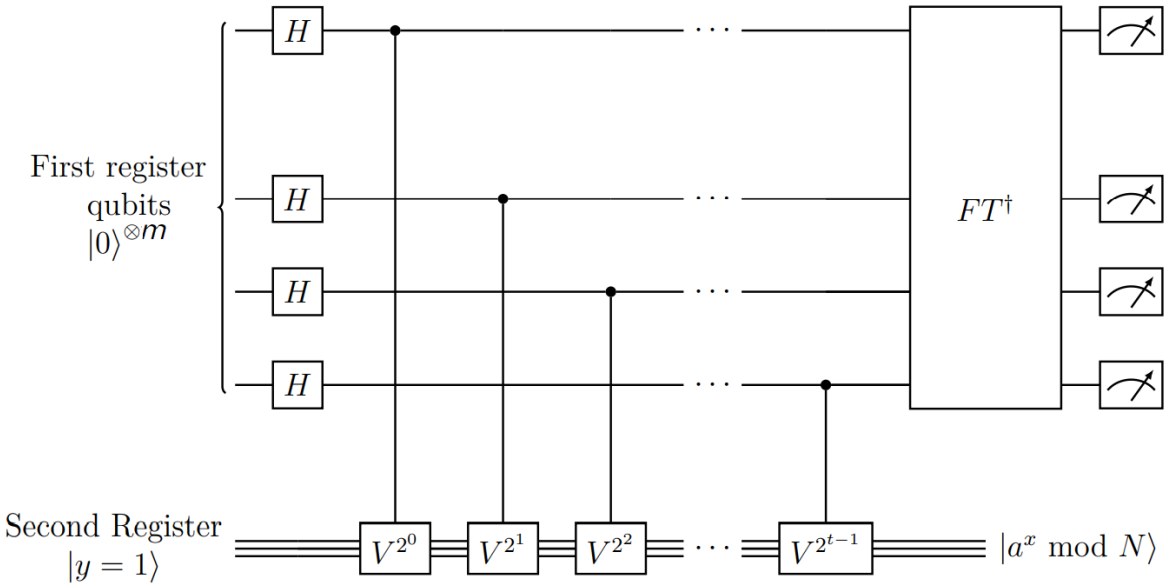

Figure 1: Circuit for period finding of the function $f(x) = a^x \mod N$

References

[1] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

[2] David McMahon. *Quantum computing explained*. John Wiley & Sons, 2007.

[3] Hamed Mohammadbagherpoor et al. "Experimental challenges of implementing quantum phase estimation algorithms on ibm quantum computer". In: *arXiv preprint arXiv:1903.07605* (2019).

[4] Chris Monroe et al. "Demonstration of a fundamental quantum logic gate". In: *Physical review letters 75.25* (1995), p. 4714.

[5] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. 2002

[6] Ronald L Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[7] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science. Ieee*. 1994, pp. 124–134.

[8] Yaakov S Weinstein et al. "Implementation of the quantum Fourier transform". In: *Physical review letters* 86.9 (2001), p. 1889.

[9] Skosana, U., Tame, M. "Demonstration of Shor's factoring algorithm for N = 21 on IBM quantum processors". *Sci Rep 11, 16599* (2021).