

QUANTUM CRYPTOGRAPHY AND QUANTUM COMPUTATION

NETWORK SECURITY COURSE PROJECT REPORT

BY

HIDAYATH ANSARI, ADITYA PARAMESWARAN, LAKULISH ANTANI,
BHASKARA ADITYA, ANKUR TALY AND LUV KUMAR



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, BOMBAY
MUMBAI

Contents

1	Introduction	4
2	Prerequisites	4
2.1	Mathematical Background	4
2.1.1	Hilbert space	4
2.2	Bases of the Hilbert space	5
2.3	Quantum Measurements	5
2.3.1	Heisenberg’s Uncertainty principle	5
3	Quantum Cryptography	6
3.1	The BB84 protocol	6
3.1.1	Underlying Quantum Principles	7
3.1.2	Stage 1: Over a quantum channel	7
3.1.3	Stage 2: Raw key generation	7
3.1.4	Stage 3: Eavesdropping detection	8
3.2	A Three Stage Quantum Cryptography Protocol	8
3.3	Limitations of Quantum Cryptography Techniques	9
3.4	Current status and breakthroughs	9
3.5	Eavesdropping	9
4	BB84 Simulation	9
5	Quantum Algorithms	10
5.1	Qubit	10
5.2	Entanglement	10
5.3	Quantum Gates and Circuits	11
5.4	Factoring Using Quantum Computers: Reductions	11
5.5	Reduction to finding the order	12
5.6	Reduction of Order Finding to Period Finding	12
6	Current status and breakthroughs in Quantum Computing	13
7	Future Work	13
8	Our Comments	14

Abstract

Quantum Cryptography uses the principles of Quantum Mechanics to implement a cryptographic system. The key problem which is solved by using quantum techniques is that of eavesdropping detection. Conventional secret-key cryptography techniques require the communication of a secret key prior to message exchange. Quantum principles can be used to *detect* eavesdropping probabilistically when it occurs. The bits are represented as qubits, physically modelled by photons, and communicated over a quantum channel. The polarization states of photons represent 0's and 1's.

We give a brief overview of the mathematical techniques employed to model the behavior of quantum particles, and also those behind the working of quantum algorithms on quantum computers.

We examine a few Quantum Cryptography protocols ([BB84], [Ben92], [Ekert94]) to learn about how Quantum Cryptography can be used to implement a secure system for communication.

We also explore two quantum algorithms for searching in $O(\sqrt{n})$ time [Lovk96] and prime-factoring in $O(\log^3 n)$ time [Shor97] which give a running time drastically lower than conventional algorithms. To analyze these, a model of a quantum computer is required. We use the one given by Vazirani et al. [BV93] which defines a Quantum Turing Machine and suggests how to implement simple computations on it.

We also examine the latest technologies and research, and the issues regarding feasibility of quantum algorithms and cryptography.

Keywords: quantum cryptography, quantum computers, eavesdropping, qubits, quantum key distribution, prime factorization, quantum computation, quantum gates

Alice said to her friend Eve,
“Why do you practice to deceive?
You know I need to talk to Bob.
Without that I won’t have a job.

“Bob can’t know where my note has been.
He thinks that you are listening in.
He wonders if it’s safe enough
For me to send him secret stuff.

“And Bob’s right not to trust you, Eve,
With quantum tricks stuffed up your sleeve.
But he thinks we can freeze you out,
With quantum tricks we’ve learned about.

“With quantum states, what we achieve
Defeats whatever you conceive.
So even Bob has to believe
That you can’t hear us, can you Eve?”

John Preskill

1 Introduction

The great advances made in the classical computing devices are still not sufficient to solve certain categories of problems which are beyond the classical computational model. Then there are certain questions, for which we neither know the solution, nor do we know if a solution exists. Also, with every passing day, technology is trying to contain great computing power in smaller and smaller devices. But is there a limit to the size to which we can compress a computer?

Moreover, as the internet spreads through the entire globe, more and more people are getting connected and important data is getting transferred over wires, the entire system is becoming more and more vulnerable to malicious people eager to eavesdrop on secret information. Can we have a way to detect presence of such malicious people and then possibly do something about it? The answer to these questions is what compels us to study the Quantum Domain.

A quantum computer is a computational device modeled on the quantum mechanical concepts like superposition and entanglement. These devices use some quantum phenomenon (like polarization of light) to represent the bits and operate on them using principles of quantum mechanics to manipulate the state space. The state space in a quantum computer is probabilistic in nature and hence has the potential to cover exponential number of states while doing computation. This opens an avenue for computational speed ups using a quantum computer.

Similarly, quantum cryptography technique make extensive use of underlying principles of quantum mechanics and Heisenberg Uncertainty principle for ensuring secure cryptography, which is not only resistant to eavesdropping (again due to probabilistic nature of it), but also has the potential to inform the communicating parties if a conversation has been compromised. Conventional cryptosystems have always relied on the difficulty of working with large numbers.

2 Prerequisites

2.1 Mathematical Background

Let us start by recalling Hilbert spaces.

2.1.1 Hilbert space

A Hilbert space is nothing but a vector space over the complex numbers \mathcal{C} with a complex valued inner product defined

$$(-, -) : \mathcal{H} \times \mathcal{H} \rightarrow \mathcal{C}$$

which is complete with respect to the norm $\|u\| = \sqrt{(u, u)}$.

The three basic axioms satisfied by an inner product are as follows

- Positive Definiteness $(u, u) \geq 0$ and $(u, u) = 0$ iff $u = 0$
- Conjugate Symmetry $(u, v) = (v, u)^*$
- Linearity in the second variable $(u, v + w) = (u, v) + (u, w)$. Moreover $(u, \lambda v) = \lambda(u, v)$

In the Quantum framework, the elements of the Hilbert space \mathcal{H} are called as *state kets* or simply *kets*. These would be denoted by $|label\rangle$ (where *label* is just some label). We define $\mathcal{H}^\#$ as the set of all possible morphisms of \mathcal{H} into the Hilbert space of all complex numbers.

$$\mathcal{H}^\# = Hom_{\mathcal{C}}(\mathcal{H}, \mathcal{C})$$

The elements of $\mathcal{H}^\#$ are called *bra* vectors and are denoted as $\langle label |$ (where *label* denotes some label). We shall denote the application of a ket $|label_1\rangle$ to a bra $|label_2\rangle$ as

$$\langle label_1 || label_2 \rangle$$

which is called a *bra-c-ket*.

There is a monomorphism (which is an isomorphism if the underlying Hilbert space is finite dimensional). So we have $|label\rangle \longrightarrow (|label\rangle, _)$ Hence,

$$\langle label_1 || label_2 \rangle = (1, 2)$$

Thus the *bracket* denotes an *inner product* of two state kets.

2.2 Bases of the Hilbert space

Now the values taken by any Quantum mechanical observable form a Hilbert space. Two kets $|\alpha\rangle$ and $|\beta\rangle$ in the Hilbert space are supposed to represent the same quantum mechanical states if there exists a complex number λ such that $|\alpha\rangle = \lambda|\beta\rangle$.

For every Hilbert space we can define an orthonormal basis and every state ket in the Hilbert space can be expressed as a linear combination of this basis (Note that for a particular Hilbert space there can be several orthonormal bases). For example: Consider the Hilbert space representing the polarization of a photon. Each different *ket* represents a plane of polarization of the light. This Hilbert space can have various possible orthonormal bases: the rectilinear basis ($|\uparrow\rangle, |\leftrightarrow\rangle$), spin basis ($|\curvearrowright\rangle, |\curvearrowleft\rangle$), diagonal basis (*vert* $|\nearrow\rangle, |\nwarrow\rangle$) etc. The relation between these bases is given in figure 1.

$$\begin{cases} |\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\leftrightarrow\rangle) \\ |\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\leftrightarrow\rangle) \end{cases} \quad \begin{cases} |\nearrow\rangle = \frac{1+i}{2}|\curvearrowright\rangle + \frac{1-i}{2}|\curvearrowleft\rangle \\ |\nwarrow\rangle = \frac{1-i}{2}|\curvearrowright\rangle + \frac{1+i}{2}|\curvearrowleft\rangle \end{cases}$$

$$\begin{cases} |\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle) \\ |\leftrightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\nwarrow\rangle) \end{cases} \quad \begin{cases} |\uparrow\rangle = \frac{1}{\sqrt{2}}(|\curvearrowright\rangle + |\curvearrowleft\rangle) \\ |\leftrightarrow\rangle = \frac{i}{\sqrt{2}}(|\curvearrowright\rangle - |\curvearrowleft\rangle) \end{cases}$$

Figure 1: Relation between the basis

2.3 Quantum Measurements

We start by looking at the statement of *Heisenberg's uncertainty principle*

2.3.1 Heisenberg's Uncertainty principle

Two independent observables of a quantum system cannot be measured with arbitrary precision simultaneously.

Let us investigate the idea of Quantum Measurement in the Hilbert space framework explained in the above section. Let \mathcal{H} be a Hilbert space representing the values of a Quantum

observable E . Let $|e_1\rangle, \dots, |e_n\rangle$ be an orthonormal basis of this Hilbert space. Thus any state ket $|\alpha\rangle$ can be written as a linear combination of the basis kets.

$|\alpha\rangle = \alpha_1|e_1\rangle + \dots + \alpha_n|e_n\rangle$ where $\alpha_1, \dots, \alpha_n$ are complex numbers.

However at this point it is important to note that above expression does not mean that the quantum state of this observable is a superposition of the states represented by $|e_i\rangle$ s. The interpretation of the above expression is as follows

- $\forall i, \alpha_i = \langle \alpha | e_i \rangle$
- $(\alpha_i)^2$ gives the probability of measuring the observable in the state $|e_i\rangle$
- As expected $\sum_{i=1}^n (\alpha_i)^2 = 1$

Consider the Hilbert space representing the polarization of the photon. Let us consider the diagonal basis and consider the representation of the ket $|\uparrow\rangle$ in terms of this basis.

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle)$$

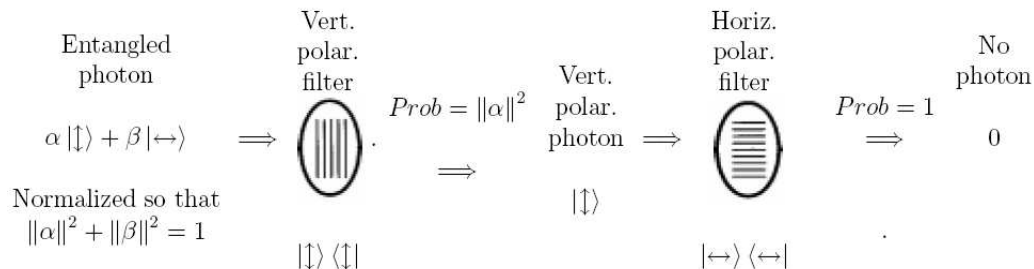
This means that if we send vertically polarized light through a polarizer inclined at 45° then we would measure a photon to be polarized with an angle 45° with probability $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$

3 Quantum Cryptography

Quantum cryptography involves the use of quantum techniques to further secure conventional cryptographic processes. One aspect in which quantum principles find good use is in key exchange. Conventional secret-key cryptography requires the exchange of a mutual “one-time pad” to be perfectly secure. This can be practically achieved using quantum channels. A quantum channel is a communication channel where a bit are represented by the state of a two-state quantum system. There have been multiple algorithms developed to harness this advantage and establish the secure exchange of a key [BB84] [Ben92] [Ekert91]. We look at one of these algorithms, developed by Bennett and Brassard.

3.1 The BB84 protocol

The key exchange according to this method can be divided into two stages, where the communication happens over a quantum channel and over a (conventional) public channel respectively. The biggest advantage of this protocol is that it *detects* eavesdropping if it has occurred, with very high precision.



3.1.1 Underlying Quantum Principles

Alice and Bob use a quantum system in which quantum bits are represented by the polarization state of photons. The photons can have one of two polarization states in either of two bases. The states in each basis are orthogonal, i.e. the kets of the basis states are orthogonal in the quantum state space. Two orthonormal bases are

- Circularly Polarized : $|\curvearrowright\rangle$ and $|\curvearrowleft\rangle$
- Linearly Polarized : $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$

The idea is that measuring a photons polarization in the wrong basis gives no information about the encoded bit, and furthermore destroys it. This is a direct consequence of Heisenberg's Uncertainty Principle.

The bases are related in this fashion:

$$\begin{aligned}|\updownarrow\rangle &= \frac{1}{\sqrt{2}}(|\curvearrowright\rangle + |\curvearrowleft\rangle) \\ |\leftrightarrow\rangle &= \frac{1}{\sqrt{2}}(|\curvearrowright\rangle - |\curvearrowleft\rangle)\end{aligned}$$

Measuring a photon's polarization requires choosing a measuring device which can distinguish between the two basis states of *any one* basis. If we have photons encoded in the linear basis and we try to measure with a detector for circularly polarized light, we measure vertical and horizontal polarization with equal probability, both $\frac{1}{2}$. In this way, the information is obscured if one measures using the incorrect basis.

Additionally, the principles of quantum physics state that after this measurement, any other measurement (using the same incorrect basis) gives the same result obtained previously, therefore obliterating any track of the originally encoded bit. Using the correct basis thereafter gives a random result all over again, by the same reasoning as above.

The above phenomenon is fundamental to the correct operation of the BB84 protocol.

3.1.2 Stage 1: Over a quantum channel

The first attempt at communicating the key occurs over a quantum channel. Alice generates a large random bit string where each bit is equally likely to be 0 or 1. This is then sent to Bob over the quantum channel by encoding each bit in one of the two bases, choosing either basis with equal probability for each bit. Bob makes measurements on received photons, by randomly choosing a basis on his known (with equal probability) for each bit. Note that due to this, Bob may choose a different basis than the one in which Alice originally encoded it. These incorrect measurements are taken care of in the next stage of the protocol.

3.1.3 Stage 2: Raw key generation

The purpose of this stage is to identify and eliminate those bit positions where Alice and Bob used different bases. This is done over a public channel. Bob tells Alice which *basis* he used for each position, and Alice in turn replies telling him which ones were incorrect. These positions are then discarded by both. Note that no information about the actual values of the bits is exchanged. If there has been no eavesdropping nor transmission errors due to noise, the remaining bit strings, called the *raw key*, at both locations are the same.

3.1.4 Stage 3: Eavesdropping detection

However, if an eavesdropper Eve has been at work, she may have introduced inconsistencies in the raw key. A measurement by Eve works in the same way as a measurement by Bob. Therefore, if the measurement made by Eve is in the incorrect basis, it may change the encoded bit that Bob measures when he gets the photon.

Eavesdropping is detected as follows: A random subset, say of length m , of the raw key is agreed upon by Alice and Bob, and those bits are compared publicly. If any two corresponding bits differ, this indicates the presence of an eavesdropper and so Alice and Bob return to Stage 1. If not, the exchanged bits are discarded and the rest of the raw key is used as the final secret key.

If Eve eavesdrops on every bit with an independent probability λ each, the probability that she goes undetected is $(1 - \frac{\lambda}{4})^m$. This can be proved as follows.

Each basis is chosen with probability $\frac{1}{2}$. In the correct basis, there is no way of measuring wrongly. In the incorrect basis, a measurement may give an incorrect bit value with probability $\frac{1}{2}$. Therefore, the probability that any measurement gives the incorrect value: $0 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$

For a bit to be measured wrongly in the presence of eavesdropping, the following must occur: Eve decides to eavesdrop (λ) and chooses the incorrect basis, and Bob gets an incorrect measurement on the photon he receives. The probability of this happening is therefore $\frac{\lambda}{4}$, implying that the probability of eavesdropping going undetected for m bits is then $(1 - \frac{\lambda}{4})^m$.

The entire preceding discussion assumes the absence of noise in the quantum channel. In the case of noise, further steps have to be taken to verify that the key is the same at both ends. These steps involve parity-checking of various subsets and binary searching to pin down and eliminate the erroneous bit.

We have implemented from the bottom-up a simulation of the BB84 protocol to exchange keys. It is coded in C++ and simulates the above stages as described.

3.2 A Three Stage Quantum Cryptography Protocol

We now describe the details of a secret key quantum cryptographic protocol as described by S. Kak [kak]. We describe this to illustrate that key exchange protocols need not be limited to BB84 and its variants, and there can be other protocols in the same flavour as well.

In this protocol, we use a quantum channel to exchange information throughout, and not just at the first stage. Another advantage is that we don't need to consider just two sets of basis. We don't restrict our quantum bits to be in one of 4 states, instead we allow any possible state.

The primary idea in this protocol is to exchange a shared key using rotations. Given an input X , A applies a transformation U_A to X and sends it to B. B applies transformation U_B and sends it back to A. A then applies the inverse of his secret transform U_A^{-1} to this bit and sends it back to B. B is then able to extract the shared key by applying the inverse of his transformation U_B^{-1} . The transformations U_A and U_B are A's and B's secret property. They could be a rotation matrix, for example:

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

Note that the transformations must necessarily be commutative. Eavesdropping can be detected by using either parity bits in the end of X .

A key distribution protocol could be the following: A and B both take a predecided bit string X , perhaps from a certification authority, apply their respective transformations on it and send it to each other. The shared key is obtained by applying one's own transformation to the bit string received from the other party.

3.3 Limitations of Quantum Cryptography Techniques

In spite of all the powers that Quantum methods have, these systems are very vulnerable to decoherence. Qubits can get corrupted or flipped due to perturbations from the surroundings. Also like any other signal, there is a problem of attenuation over distance. But in case of quantum, the matter is worse.

Current techniques of Quantum Cryptography face the limitation of non-existence of devices that can be used to clone the signal. To clone a particular signal, measurements are required to be made, which by the very nature of quantum cryptography will destroy the original signal because the cloning device does not know the correct order of basis that was used.

Also, if we make amends in the protocol to allow for a device like router to make correct measurements and then further clone and amplify signal, then the same technique can be used for eavesdropping thereby losing the whole point of quantum cryptography. So this amounts to saying that a quantum system should have direct-dedicated point to point links between any two entities that wish to communicate. These raise a lot of serious questions on the feasibility of quantum devices.

3.4 Current status and breakthroughs

Despite these limitations, there have been attempts to apply quantum methods, at a much scaled down level though. Teams from Harvard, Boston University and BBN Technologies are trying to build DARPA (Defense Advanced Research Projects Agency) quantum network, of which the first link has been laid and functional since December 2002.

In addition to these teams at Geneva, Los Alamos and IBM are performing QKD through telecom fibers. There are systems that can support distances upto 70 km through fiber, though at very low bit rates. Also, teams from Los Alamos and Qinetiq are performing free-space Quantum Cryptography, both through day and night skies upto a distance of 23 km.

3.5 Eavesdropping

Various eavesdropping strategies have been developed, such as opaque and translucent eavesdropping. Opaque eavesdropping involves the capture, measurement, and retransmission of photons. Translucent eavesdropping is a technique wherein the photon is very gently disturbed in order to glean some information from it [Ekert94].

This can be accomplished by letting a photon pass through a birefringent crystal and then measuring the recoil of the crystal due to momentum conservation. If the width of the crystal is set appropriately, the resultant photon is only slightly depolarized. Cloning is possible only when it is known that the photon is in one of a definite set of orthonormal states.

If a set of nonorthogonal states is used, this gives us the opportunity to detect any eavesdropping attempt by measuring an unusual error rate in exchanged bits, beyond the expected statistical error rate.

4 BB84 Simulation

We have implemented a simulation of the BB84 protocol in C++ using the STL Library. The salient features of this implementation are the following:

- We use `vector<bool>` to represent the keys and the basis. We represent the two (circular and vertical) polarizations as 0 and 1.

- We input the desired size of the key (n), and the number of verification bits (m). We generate A's key and basis randomly using the function `genRand dom(vector<bool>)` which fills up a boolean vector with 0's and 1's randomly.
- The `measure(a_key, a_basis, b_key, b_basis, lambda)` function measures a's key with b's basis.
 - The values obtained are saved in B's key vector. The basis for the input vector is then modified.
 - This function works just like an actual measurement would. Once basis is used to measure a certain key entry, the key value gets fixed at that value.
 - The same function is used for both B and C. Like in the theory given above, the `lambda` is the probability that C will eavesdrop at any given bit. If the function is being called by B, we set `lambda = 1`
- We simulate A and B's basis comparison over the public channel by comparing the i th values of the two vectors `a_basis` and `b_basis`, to generate a raw key. If the size of this raw key is less than the number of verification bits, then we flag an error and exit.
- We then pick up m random bits from `a_key` and `b_key` and check their values. If we find any error (i.e. the values of the vectors do not match at the random indices) then we signal eavesdropping. Else we output the remaining bits and exit.

5 Quantum Algorithms

5.1 Qubit

A qubit or a quantum bit is the basic unit of computation in a quantum computer. Physically, a qubit can be thought of as an electron in a Hydrogen atom. There are two possible states an electron in a hydrogen atom can be in – the ground and the excited state. The ground state corresponds to the value of the qubit being 0, and the excited state corresponds to 1. We represent the ground state as $|0\rangle$ and excited state as $|1\rangle$. By the basic principles of quantum mechanics, the general state (denoted $|\alpha\rangle$) of an electron is given by a superposition of these two states.

$$|\alpha\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

where $\alpha_1, \alpha_2 \in \mathbb{C}$ and $|\alpha_1|^2 + |\alpha_2|^2 = 1$. By this we mean that if a measurement is made on the state of the electron, we find it to be $|0\rangle$ with probability $|\alpha_1|^2$ and $|1\rangle$ with probability $|\alpha_2|^2$.

5.2 Entanglement

If we have two electrons, then we have four possible states that the electrons can be in (00, 01, 11, 10). Each of these states has some probability, and the joint state is represented as:

$$|\alpha\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \text{ where } |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

In general we cannot specify the state of each individual electron alone. The electrons are said to be *entangled*. If we measure the value of one of the qubits, then the joint states are restricted to the ones the qubit measured has the value measured. In the new state the values of the coefficients scale up so that the sum of the squares of the coefficients add up to 1. In the

above equation, if we measure the value of the second qubit, and its value is 1, then the new joint state is:

$$|\alpha\rangle = \frac{\alpha_{01}}{\sqrt{|\alpha_{01}|^2 + |\alpha_{11}|^2}}|01\rangle + \frac{\alpha_{11}}{\sqrt{|\alpha_{01}|^2 + |\alpha_{11}|^2}}|11\rangle$$

To see the power of this concept, consider the case when the coefficients in the equation above are $\alpha_{00} = \alpha_{11} = 0, \alpha_{01} = \alpha_{10} = \frac{1}{\sqrt{2}}$. If the two electrons are generated in a joint state of this form, then they will be so forever. Consider two electrons that were generated together with this joint state. Now even if we separate these two electrons to distances far away, the joint state is still maintained, and if we measure the value of the second qubit, then the value of the first qubit gets fixed as its complement. If we get the value 1, then $|\alpha\rangle = |01\rangle$. This happens even though the electrons may be large distances away. *Thus quantum information travels faster than the speed of light!*

5.3 Quantum Gates and Circuits

Just like we have AND, OR and NOT gates on a normal computer which take as input bits, we assume that a quantum computer has gates, which take as input quantum bits. A typical gate is the Hadamard gate. It operates on a single qubit. The operation is defined by the following two equations.

$$\begin{aligned} H(|0\rangle) &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ H(|1\rangle) &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{aligned}$$

If the input qubit is a superposition of the two states, then the output is what we expect because of linearity – $H(\alpha_1|0\rangle + \alpha_2|1\rangle) = \frac{\alpha_1 + \alpha_2}{\sqrt{2}}|0\rangle + \frac{\alpha_1 - \alpha_2}{\sqrt{2}}|1\rangle$. Now, suppose we have a system having two (entangled) qubits, say in the state $|00\rangle$. What happens if we apply the Hadamard gate to one of the qubits, say the first one. In this case, the new state of the system is given by $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$. This has an interesting consequence. Suppose we have n entangled qubits, and the current state is given by $|\alpha\rangle = \sum_{s \in \{0,1\}^n} \alpha_s |s\rangle$. Say we apply the Hadamard gate to the first qubit. Each term in the summation now ‘splits’ as we have seen above, so the application of a single gate could potentially change *all* the 2^n coefficients.

This is one of the main reasons for the power of quantum algorithms. We will see soon how this fact can be used in the computation of the fast fourier transform in time $O(\log^2(n))$.

5.4 Factoring Using Quantum Computers: Reductions

We now consider the problem of factoring a large odd composite number using quantum algorithms. The problem is of importance because most of the existing cryptosystems rely on the fact that there are no known efficient algorithms for this problem. The best classical algorithm is still exponential in $\log(n)$. We present an algorithm of Shor [Shor97] which factors an integer N in time $\log^3 N$.

The algorithm involves a series of reductions:

1. Factoring a number is reduced to finding a non-trivial square root
2. Finding a non-trivial square root is reduced to finding the order of a random integer modulo n
3. Finding the order is reduced to finding the period of a quantum superposition

4. Finding the period of a quantum superposition is done by using the quantum fast fourier transform.

We will describe in detail each of these steps in the following sections.

5.5 Reduction to finding the order

We now describe the first two reductions in the scheme presented above. The first one is easy. Suppose we are given a number $N = pq$, where p and q are odd primes. A number x is said to be a non-trivial square root modulo N if $x^2 \equiv 1 \pmod{N}$ and $x \not\equiv \pm 1 \pmod{N}$.

Theorem 1. *Factoring is as easy as finding a non-trivial square root.*

Proof. Suppose x is a non-trivial square root modulo N . Then, we have $(x + 1)(x - 1) \equiv 0 \pmod{N}$, so $N \mid (x - 1)(x + 1)$. Since neither $x - 1$ nor $x + 1$ is a multiple of N (x is a non-trivial square root), precisely one of p, q should divide $(x - 1)$. Thus, computing $\gcd(x - 1, N)$ gives one of the factors of N . \square

Next, recall that the order of x modulo N is the smallest integer r such that $x^r \equiv 1 \pmod{N}$. Now, suppose we have an x whose order is even (say it's r) and further we have $x^{r/2} \not\equiv \pm 1 \pmod{N}$. Then, $x^{r/2}$ is a non-trivial square root modulo N . Now, we try to show that a number x picked at random from $\{0, 1, \dots, N - 1\}$ satisfies this condition with probability at least $3/8$. Thus, if we pick a constant number of x 's, we find one which satisfies the conditions with high probability. We will prove the above in two steps.

Theorem 2. *Suppose $N = pq$, and x is a number picked randomly from $\{0, 1, \dots, N - 1\}$. Let r be the order of x modulo N . Then, with probability at least $3/8$, r is even. Moreover, $x^{r/2} \not\equiv \pm 1 \pmod{N}$.*

Proof. First, observe that at least half the integers in \mathbb{Z}_p have an even order modulo p . This is because any x of an odd order must be a solution of $x^{(p-1)/2} \equiv 1 \pmod{p}$, and thus there can be at most $(p - 1)/2$ such x 's (because the number of solutions to a k th degree equation in \mathbb{Z}_p is at most k).

Suppose an integer x has an odd order modulo N . Then we claim that it has an odd order modulo both p and q . This is because if $x^r \equiv 1 \pmod{N}$, then $x^r \equiv 1 \pmod{p}$, so $\text{ord}(x, p) \mid r$ implying $\text{ord}(x, p)$ is odd (the same argument holds for q). Thus, by chinese remainder theorem, at most $1/4$ th of the integers modulo N can have odd order. Thus, at least $3/4$ th of the integers modulo N have an even order. It can be proved by similar methods (see [Shor97] for details) that for at least half of these we have $x^{r/2} \not\equiv \pm 1 \pmod{N}$. This proves the result. \square

Thus, we reduced the problem of finding the prime factorization to one of finding the order of a random number modulo N .

5.6 Reduction of Order Finding to Period Finding

Consider the following superposition formed with two sets of registers of k bits each (where the second register is computed \pmod{N})

$$|\alpha\rangle = \frac{1}{\sqrt{M}}(|0, x^0\rangle + |1, x^1\rangle + \dots + |(M - 1), x^{(M-1)}\rangle)$$

we have $M = 2^k (> N)$. Consider the situation when the second set of registers are measured, and gives a value V modulo N . Now, the property of entanglement ensures that the values in the

resulting superposition are only those for which $x^i \equiv V \pmod{N}$. Thus we have restricted the first set of registers to be only $i, i+r, i+2r, \dots, i+(M/r-1)r$, where r is the order of x modulo N . We now need to isolate the value of r . Note that we cannot sample this superposition more than once, because the value of V we obtain when the experiment is repeated could be different. We solve this problem using quantum FFT.

The quantum fast fourier transformation is used to transform the superposition: $\sum_{j=0}^{M/r-1} C|jr+i\rangle$ with offset i to one which does not have any offset, so if we make a measurement, we obtain a multiple of r . Now we can easily generate and sample the $\sum_{j=0}^{M/r-1} C|jr\rangle$ a number of times to get a set of multiples of the period, whose gcd gives us the required period (with high probability).

6 Current status and breakthroughs in Quantum Computing

- Research teams at Waterloo and Massachusetts have benchmarked a quantum control method on a 12-Qubit system. This is the largest quantum information processor to date. Despite decoherence, the researchers were able to reach a state in which all 12 qubits were coherent.
- The first quantum byte, created by scientists at The Institute of Quantum Optics and Quantum Information at the University of Innsbruck in Austria (December 2005).
- Researchers at University of Michigan build a quantum computer chip for atomic qubits. This offers some hope for making a practical quantum computer using the semiconductor manufacturing technology, and hopefully can be put to use commercially (In 2005).
- University of Illinois at Urbana-Champaign scientists demonstrate potential for multiple qubits per particle (In 2005).
- Peter Zoller of University of Innsbruck in Austria, discovers a method of using cryogenic molecules to make stable quantum memories (year 2006).
- Researchers at the University of Pittsburgh created semiconductor particles smaller than 10 nanometers in scale, also known as quantum dots (year 2006).

7 Future Work

The most important question that is yet to be answered in this area is whether quantum computers can solve any \mathcal{NP} complete problems. The factorization problem, which we have seen to be solvable in polynomial time, has not been proved to be \mathcal{NP} complete (although there is no known classical algorithm which runs in polynomial time). There have been some attempts to solve the shortest vector problem using the quantum method, but the question is still open.

Also, we have not reviewed literature on further eavesdropping techniques and the algorithm due to Grover on searching in a database in $O(\sqrt{N})$ time. These would be interesting avenues for further study. Also, our simulation currently handles the BB84 protocol without noise. It would be nice to extend this to handle errors in channels, and implement automatic error correction.

A major drawback in this study is that current literature on the state of quantum computing is either not available or is classified, as a result of which we are not aware of the most recent developments in this regard.

8 Our Comments

Based on what have read and learnt about the field of Quantum Cryptography and Quantum Computing in general, there a few important issues that we feel need to be tackled before Quantum technology can emerge from the researcher's laboratory into the mainstream and become a part of everyday computing and security technology. The most severe limitation of quantum computers at their current stage of development is the fact that they are large and expensive, and are custom-built by researchers in a very controlled laboratory environment. It remains to be seen whether quantum computers of a reasonable size (say comparable to personal computers 20 years ago) can be built and packaged in a form amenable to mass-production.

This will require addressing the issue of decoherence in large and complicated quantum logic circuits. Even if this is possible, it may not be possible in a cost-effective way. Moreover, today's small toy quantum computers require large amounts of power, and extending the technology to practical everyday quantum computers will require significant research and development efforts towards lowering the power consumption of quantum computers. Other related issues include considerations such as maintaining optimal temperatures and media concentrations for proper operation of the quantum circuitry.

Another issue with quantum computers is the fact that a program has to be run many times and the distribution of the outputs has to be analyzed to determine the "correct" output of the program. It remains to be seen how this model of computation fits in with everyday computational tasks such as simple addition, or managing a company's accounts. As for quantum cryptographic techniques, the central concern is that of building practical quantum communication channels. The biggest problem is that using repeaters in quantum channels is not possible since it would amount to eavesdropping, and would destroy the information contained in the transmitted qubits. Research efforts are underway to integrate quantum channels into the IP and IPSec framework by incorporating quantum links in the link layer.

Whether this can scaled up for mass deployment as the next generation of the Internet, remains to be seen. This will, of course, require building quantum channels which can transmit qubits over significant distances, since the current limits (70km over fiber optic cable and 23km through the air) are too low for practical usage.

References

- [BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pages 175– 179, 1984.
- [Ben92] C. H. Bennett. Quantum cryptography using any two nonorthogonal states, Physical Review Letters, Vol. 68, No. 21, 25 May 1992, pp 3121 - 3124.
- [Ekert91] Ekert, Artur K., Quantum cryptography based on Bell's theorem, Physical Review Letters, Vol. 67, No. 6, 5 August 1991, pp 661 - 663.
- [Shor97] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing 26, pp. 1484-1509, 1997
- [Lovk96] L. K. Grover, A fast quantum mechanical algorithm for database search. In Proceedings of 28th Annual ACM Symposium on Theory of Computing (STOC), pages 212-219, May 1996.
- [Ekert94] Artur K. Ekert et. al., Eavesdropping on quantum-cryptographical systems, Phys. Rev. A 50, 1047105, 1994
- [S JL] S. J. Lomonaco, A quick glance at Quantum Cryptography, quant-ph/9811056, 1998
- [NG01] N. Gisin et. al., Quantum Cryptography, quant-ph/0101098, 2001
- [BV93] E. Bernstein and U. Vazirani, Quantum Complexity Theory, SIAM J. Comput., 1997
- [kak] S. Kak, A Three stage quantum Cryptography Protocol, arXiv quant-ph/0503027, 2005.