University of Tehran

College of Engineering

School of Electrical and Computer Engineering

Long Distance Quantum Communication Using Repeaters

A thesis submitted to the Undergraduate Studies Office

In partial fulfilment of the requirements for

The degree of Undergraduate in

Electrical Engineering

By:

Mohadeseh Azari

Supervisor:

Dr. Saleh Rahimi-Keshari (Faculty of Physics) / Dr. Leila Yousefi (Faculty of Electrical and Computer Engineering)

Table of Contents

Chapter One 3

RSA Algorithm 3

Quantum Mechanics 3

Shor's Algorithm 3

Bernstein-Vazirani algorithm 4

QKD 5

Chapter Two 5

Qubit & Quantum Measurement 5

Quantum Entanglement 6

Quantum Teleportation 6

SDC: Super Dense Coding 7

Chapter Three 7

Quantum Purification 7

Conclusion 9

Reference 9

Appendix 10

Appendix A 10

Appendix B 13

Quantum Communication using Quantum Repeater

***Abstract*—In 1687, Sir. Isaac Newton published his book *Philosophiæ Naturalis Principia Mathematica* for the first time. As time goes by, we have employed the laws of Classical Physics to build skyscrapers, suspension bridges on the water's surface, satellites, and other significant applications. Quantum mechanics is the bigger picture from which Classical Mechanics can be derived. Quantum Mechanics passed a long road to reach this point and is now on its way to practical application. Quantum Communication utilizes Classical Communication and Quantum Mechanics to Stablish a feasible Quantum Network. In this project, the primary purpose is to analyse different modules of a Simple Network and understand Quantum technology's boundaries. In Chapter One, at first, there will be a timeline of Classical Communication. Then, an explanation of conditions that threaten Classical Security. Quantum methods for security plus some updated Experiments are discussed. Finally, the rule of Quantum repeaters in a Quantum Network will be explained. In Chapter Two, the concept of Qubit, Superposition and Entanglement will be explained. Also, two crucial modules for Quantum Communication, Quantum teleportation and Super Dense Coding, will be analysed. Chapter Three shows the structure for a Quantum Repeater and the process for Quantum Purification.**

***Keywords*— communication, entanglement, Qubit, repeater**

Chapter One

From Latin communicare, the word communication is an ancient concept in human history. From the early smoke signals into optical fibers, we always searched for a fast and sufficient way of Communication.

Communication is the tool for exchanging information, and through its history, the basic unit of information has been changed.

Nowadays, our famous unit of information is "Bit." When someone thinks of telecommunication, the picture in their mind would be a handful of 0 and 1s carrying a signal. The early ideas of Communication in terms of bits belong to Samuel Morse. [1] The idea behind Morse code was to convert each alphabet letter into a series of ditz and dahs (dots and dashes). So the substitute for Samuel would be · · · · - - - · · - · · · - · ·, which is quite long. Morse dominated regular Communication in confidentiality, one of the essential features of every Communication.

"As a unit of information, the bit is also known as a *Shannon*, named after Claude E. Shannon."

Claude Shannon –the father of information theory – made a revolution in the communication and information world.

The beginning of bits carved the way for the birth of the digital world [2]. Any two-level logical state can be represented by "0" or "1", "on" or "off," "light" or "darkness." The bitwise Communication was faster and more efficient and began to rule our world and make it the digital world around us. However, every Communication needs to be secure. One of the advantages of the Morse code was its confidentiality. Not everyone could understand Morse code, and that made the message partially secure. RSA protocol is the security protocol for today's Communication.

RSA Algorithm

RSA algorithm, which is short for (Rivest–Shamir–Adleman) [4], is an asymmetric cryptographic algorithm. It uses the public and private key pairs to assure confidentiality.

There are some groups of mathematical problems which require computational power to be solved [3]. Most security algorithms rely on these mathematical problems for their security, and as long as we have limits for computation power, algorithms based on these problems are secured. RSA algorithm is not an exception.

RSA algorithm relies on factoring problems for the creation of a secure key.

$$e.d \overset{\varphi(n)}{\equiv} 1 \qquad \varphi(n) = (p-1)(q-1)$$

Here the calculation of "d" without knowing {p, q} requires a great deal of time which makes the RSA algorithm secure. Nevertheless, as discussed earlier, these algorithms are secure conditionally, and if one has enough computational power, the RSA algorithm can be breakable. The security of these algorithms is linked to the power of computers.

Quantum Mechanics

From 1900, the early hypothesis of Max Planck to the 1935 EPR article [9] till todays researches, Quantum mechanics showed great potential in various fields, and one of them is computational power. The works of Richard Feynman first introduced the idea of the Quantum computers, and some great Quantum algorithm has been introduced till now.

Shor's Algorithm

One of the most significant breakthroughs in Quantum Algorithms is undoubtedly Shor's algorithm [5],[6]. As discussed earlier, the RSA protocol used Factoring for its coding since classical computers could break the number into

its factors in a super polynomial time. However, using Shor's algorithm, the number N can be divided into factors, p, and q in a polynomial time.

As demonstrated in Appendix B, one can question the possibility of implementing Shor's algorithm in a classical computer. To answer that, first, we have to answer the problem of Period Finding and its connection to Factoring. In the second step of Shor's algorithm, we face the problem of Period Finding. Period Finding can seem to be easily implemented, but the period of a function can be perplexing, and finding its period can demand a tremendous amount of time. By utilizing the Quantum properties of a Quantum Circuit, Shor's algorithm can solve the problem in a smaller order of time.

The only part of the hardware that needs to be a Quantum Simulator is finding the period of a function. Moreover, the post-processing can be done by a Classical Simulator.

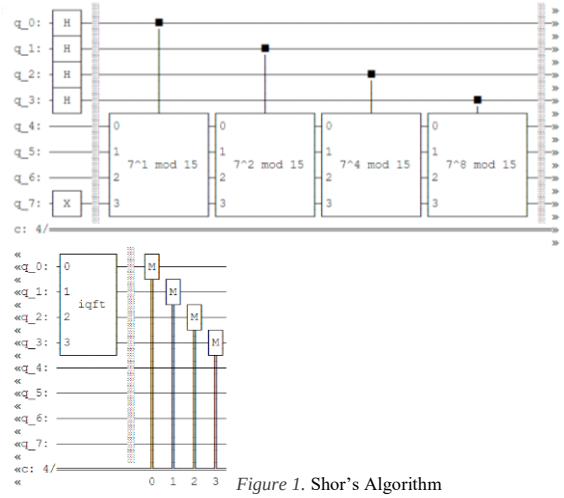


Figure 1. Shor's Algorithm

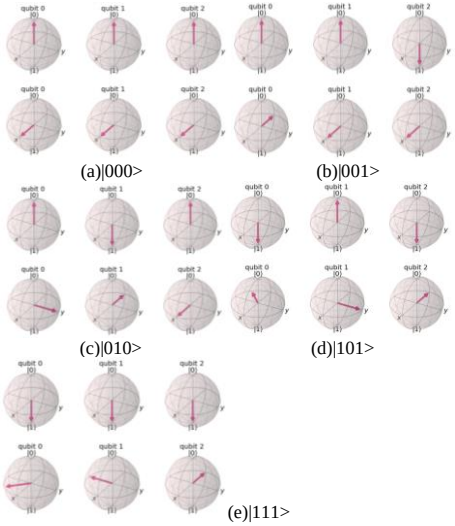


Figure 2.. QFT of a 3-Qubit system

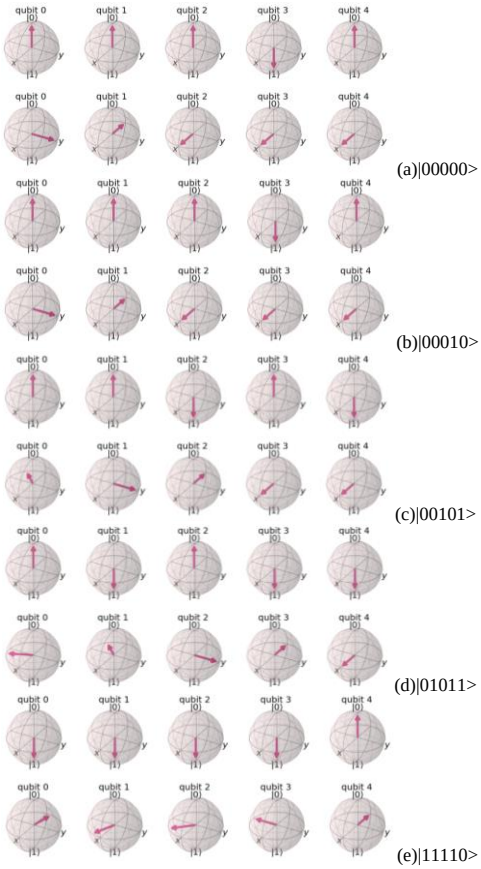


Figure 3. QFT of a 5-Qubit system

In Figure1, after measuring the first four qubits, the function "r" period can be easily calculated. See Appendix A for Qiskit code. In this Quantum Circuit, the function of the Inverse Quantum Fourier Transform is crucial. For more information about QFT see Appendix B.

Bernstein-Vazirani algorithm

Another algorithm showing the advantages of quantum computers over the classical one is the Bernstein-Vazirani algorithm [7], [8].

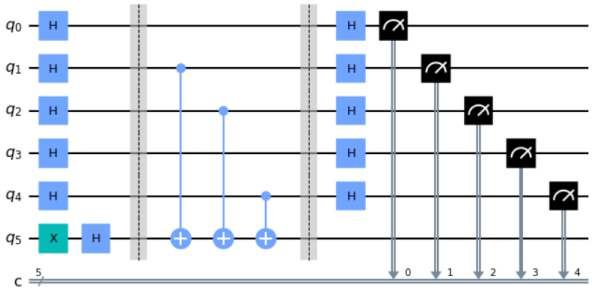


Figure 4. Bernstein-Vazirani algorithm

This algorithm is used to find a number in a black box. Consider a black box as hardware that can connect input and get the output out of it but not see the inside.

Consider that an “n” bit number is stored in that hardware. The goal is to find that number without looking into the hardware.

Classical scheme:

Consider we have a 5-bit number - - - - -. what we can do is to do the “AND” operation of the output with

{10000,01000,00100,00010,00001}. After five trials, a classical scheme can guess the number correctly.

Quantum scheme:

The difference here is that we can (in one shot) guess the number correctly, and we do that by considering all the possibilities of the result. If our inputs were in the state (|0> + |1>) /√2

then the output would be all the possible answers, including the correct number. Find the codes for Figure 4. in Appendix A. And the mathematical explanation in Appendix B.

So Quantum algorithms use Quantum properties like Quantum entanglement and Quantum superposition to solve complex problems in a smaller order of time. So that means a practical Quantum computer has more computational power in comparison to its classical counterparts.

QKD

As we discussed earlier, most security algorithms, including the RSA algorithm, uses complex mathematical problems that require computational power as a security advantage. However, if Quantum computers could reach better computational power, this means that today's security protocols are not safe enough. So if the messages want to be secure even with Quantum computers, the classical approach will fail, and a Quantum approach for key distribution should occur. QKD, which is short for Quantum Key Distribution, is the presented approach.

Stephen Wiesner first proposed quantum cryptography, and till now, researchers from all around the globe have tried to push boundaries for Quantum cryptography. One of the significant breakthroughs in Quantum Key Distribution was about Chinese satellite Micius in 2016. [19]

"The achievement brings the world one step closer to realizing truly unhackable global communications."

In this project, a solely secure Quantum Communication was established between Beijing and Vienna, separated by more than a hundred Kilometers. This Communication was completely secure, and even the satellite did not know what was going on. The researchers on this project used a satellite as a transmitter. They connected the satellite and two ground stations so that there could be no eavesdropping from the satellite.

So far, we saw that conditional security algorithms might not survive from Quantum computers, and by using QKD, we can have absolute security. However, Quantum communication is challenging to implement due to Quantum decoherence and the fragile nature of photons, which prevents the distance from going farther than 100 Kilometers.

Very properties that make light the ideal medium information, makes it hard to store the information[14]. So far Quantum Optical Channel is the ideal medium for Quantum information. But a single photon is too low in energy to be lost in a complete light background [15]. The fragile nature of Photons and the Noisy Quantum Channels makes it hard to reach high fidelity specially toward Long Distance Communication.

In classical telecommunication, the answer for increasing the signal-noise ratio is amplifiers. However, due to the "no-cloning" theorem [11], Quantum signals cannot be amplified.

In order to copy |κ> = λ_1 |0>+λ_2 |1> to another state, both $\lambda_1 \; and \; \lambda_2$ must be known. Consider a copy unitary Operator called C. That unitary operator is a cloning operator if and only if it exists for every state. This is not true for |k> = |1>. For mathematical explanation see Appendix B.

The post-process of amplifying is the measurement which, in a Quantum context, measuring a Quantum state will force the system to collapse into the post-measurement state and ruin the Quantum properties.

One of the best solutions for Long Distance Quantum Communication is Quantum Repeater.

The idea is to divide the distance into smaller lengths and, instead of having amplifiers in each link, do Bell state measurement to forward entanglement between nodes.

Chapter Two

Qubit & Quantum Measurement

Qubit, which is short for Quantum Bit, is a logical Quantum unit that enables Quantum Circuits to function. A Qubit can be in state |0> or |1> and even in a superposition state. There are two different ways to show a state of a Qubit. The first method is using Bra and Ket to represent the state. For instance, the state $|\varphi>$ is shown like $\alpha|0> + \beta|1>$. The other method is using matrices for representation, so the state $|\varphi>$ would be like

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

When a Qubit is in a superposition state, the probability of getting 0 when measuring the Qubit on the basis |0> will be $|\alpha^2|$, and the probability of getting 1 when measuring on the basis |1> is $|\beta^2|$.

Great attention must be taken here for the superposition concept. Before measuring a Qubit, one must not consider the state being whether |0> with probability $|\alpha^2|$ or |1> with probability $|\beta^2|$, but in a state $\alpha|0> + \beta|1>$.

Another crucial concept that needs to be explained is measurement. When measuring a classical state, the post-measurement state is independent of the measurement. In the case of bits, consider strings of one's has been transmitted to a station. If one calculated the number of ones in the strings and knew the total length of the strings, then finding the error rate would not be complicated. However, when dealing with

Qubits measuring a Quantum state will force the state to collapse into the post-measurement state, and then there will be no more than classical data. If the system's state is $|\varphi>$, the outer product can calculate the density matrix of that system. The post-measurement state and the probability of each outcome will be calculated as follow, where g is the degrees of degeneracy:

$$p(n) = tr(<\varphi|P_n) \,.\; P_n = \sum_{i=1}^{g} |\alpha_n^i \times \alpha_n^i|$$

$$|\varphi_2> = \frac{P_n\,|\varphi_1>}{\sqrt{p(n)}}$$

So, for example, in Quantum error correction, measuring the Qubits is not a good solution. Instead, the Qubit's states will be compared using the CNOT gate, and by analysing the results, error correction can be performed.

Quantum Entanglement

Quantum entanglement is one of the critical factors that make Quantum technology unique. Consider there is a secrete and very crucial letter written in two pages. Revealing even a paragraph or a sentence of that letter could mean a trophy for the enemy. In delivering the paper, it is a probability of an attempt to grab the papers from the hands of the delivery man. On the way, the spy tries to grab the letter, and a small piece of the letter is torn, falls into the enemy's hands. It is a great question why someone tries to deliver such an important letter by a delivery man but let us analyze this peculiar case.

There are two different kinds of paper for writing this letter, the classical papers and a Quantum Entangled pair of paper. If the letter were written in two classical papers, some percent of secret information was leaked. However, if the papers were Entangled, the unfaithful spy must grab the whole letter to get any information out of it. Having a piece of Entangled paper would mean nothing more than complete random letters.

When a Quantum state is entangled, the state cannot be divided into the tensor product of its subsystem. For instance, if the state is $|\varphi>$, then:

$$|\varphi> \neq |\alpha_1> \otimes |\alpha_2>$$

Entanglement is not limited to n-dimensional systems. There can be an entanglement between motion and spin of the same Qubit.

A famous entangled pair is known as EPR pair [9][10] – short for Einstein Podolsky Rosen – take the state as $|\varphi>$, then :

$$|\varphi> = \frac{1}{\sqrt{2}}\,(|0>\otimes|0> + |1>\otimes|1>)$$

which its short form is:

$$|\varphi> = \frac{1}{\sqrt{2}}\,(|00> + |11>)$$

$|\varphi>$ cannot be divided into the tensor product of two states.

Entanglement property brought absolute security between the pairs of entangled states.

There are two ways to assign the Entangled pairs between the nodes.

One way is to generate the entangled pairs and send one of them to another node.

The other way is to generate the pairs somewhere in between and transmit them to specific nodes.

The state of A and B are entangled, which means the data of both measurements would be correlated. By analyzing the data, both sides can be precise whether or not there was an eavesdropper.

There are two main factors:

Firstly, Every Quantum state is unique, and after measuring a system's state, it will collapse into a post-measurement state.

Secondly, Entangled states are unique. As long as the measurements data are correlated, there is Eavesdropper in the whole world.

So far, the concept of communication and its evolvement through time has been explained. The concept of Bit and Qubit (Quantum Bit) has been illustrated, and the nature of security in Quantum communication was understood.

Now that the role of Quantum Communication has been cleared let us step back to Quantum Repeaters. As discussed in Chapter One, a Quantum network must utilize Quantum Repeaters to use Quantum Key Distribution. The following are two crucial modules for Quantum Repeaters.

Quantum Teleportation

Quantum teleportation is a technique for transferring Quantum information from a sender to a receiver. Due to the fragile nature of photons and the noisy Quantum channels, Propagating Quantum information is hard to implement. Quantum teleportation [16] is a protocol that allows us to transport the state of one Qubit to the other Qubit. For a mathematical explanation, go to Appendix B.

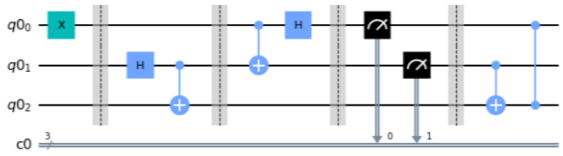


Figure 5. Quantum Teleportation

Linear Operators	They act within the vector space
Identity Operators	I
Unitary operator	SS^† = I
Hermitian operator	H = H^†
normal operator	T T^† = T^† T

Table 1. Operators

In this circuit, the Qubit zero is transported to Qubit two. All the Qubits are at state |0> in the initial time.

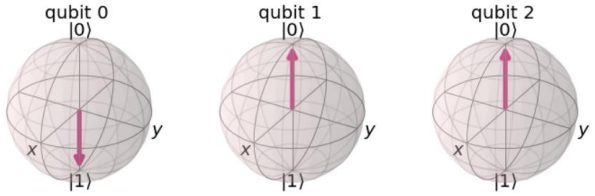


Figure 6. The state after the first barrier

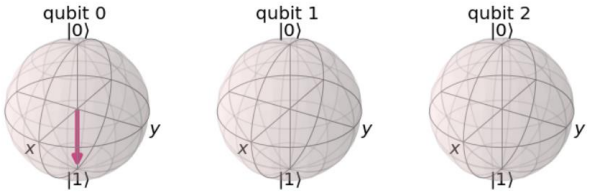


Figure 7. The state after the second barrier

As we can see, the state |1> must be transported to Qubit two. In Figure 7. Qubit 1 and Qubit 2 are entangled, and that is why their state vectors are hidden. By using a Histogram plot in 1024 trials, the results are the following.

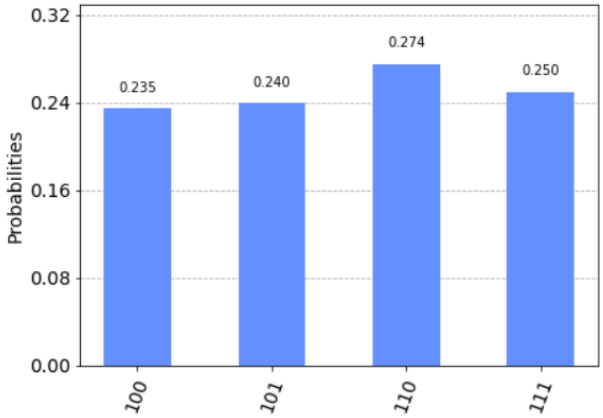


Figure 8. Histogram plot for Teleportation
(Read the results from the left to the right, C2, C1, C0.)

As we can see, C2 is 1, which means the circuit successfully transported the state |1> from the first Qubit to the third Qubit. Find the codes for this circuit in Appendix A.

After measuring the first two Qubits, there is a final state which depends on the measurement result. If the measurement results showed correlation, then the state of the third Qubit is the correct result. Nevertheless, if the measurement results were not correlated, the final state must pass through a phase shift Gate (after the fourth barrier). For mathematical details, go to Appendix B.

SDC: Super Dense Coding

Dense Coding and Quantum Teleportation are closely related. So let us first examine the differences between these two protocols.

Quantum Teleportation transmits the state of a Qubit to the other Qubit using two classical bits, while super dense coding sends two classical bits using a single Qubit.

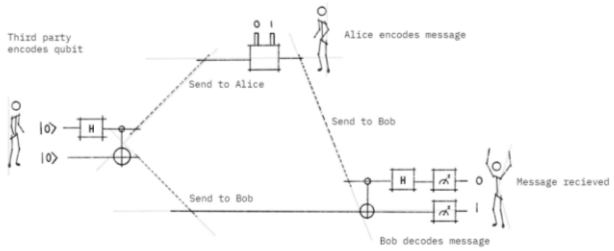


Figure 9. Dense Coding

Here the primary purpose is to transmit Alice's bits to Bob using a single Qubit. A Third side is needed to share Entangled states between Alice and Bob. After sending Entangled Qubits, Alice must encode her Qubit in order to store her classical bits' information. X and Z Multiplexer will act on the Qubit dependent on the classical control bit. For instance, If the classical bits are 00, the operator will be Identity, but if they are 01, X operator will act on the Qubit.

Classical Bits	Operator
00	I
01	X
10	Z
11	ZX

Table 2. Encoding Classical information into Qubit

When Bob does the reverse operation for entanglement, he will get a Qubit in the same state as Alice's Classical Bit. For mathematical explanation and Codes, see Appendix A & B.

Chapter Three

Quantum Purification

Quantum purification is a vital module in a Quantum network. Every n-dimensional entangled system has a maximum entanglement. Remember the example of the secret letter earlier; the more the system is entangled, the more randomness that piece of torn paper has. Due to the noisy hardware and environment, the entanglement between the system might decrease, so repeaters must have a purification module to gain the information.

Consider there is an ancient book that some parts of it are faded and impossible to read. If there was more than one copy of that book, so by comparing them, one could understand the book better. In other words, the entanglement between the topics of the book will improve. In purification protocol, instead of having one pair of entangled qubits, there will be more pairs of entangled qubits. Measuring the other pairs will increase the entanglement in the first entangled qubits.

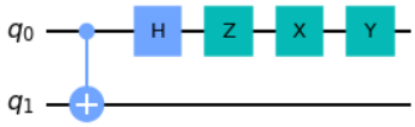
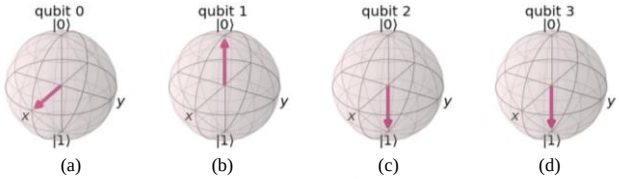


Figure 10. Universal Gates



(a) (b) (c) (d)

Figure 11. From right to left H, Z, X and Y Gate

Here there will be two approaches for Quantum Purification. One approach is the ideal Quantum Simulators, and the second one is the NISQ simulation using the 'Qasm' simulator with noise.

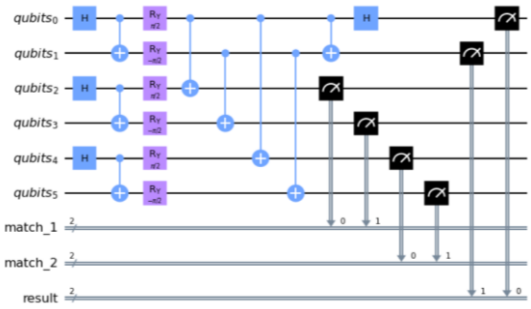
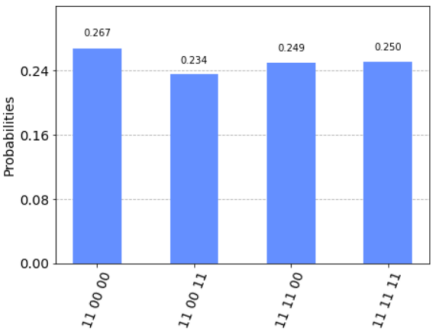
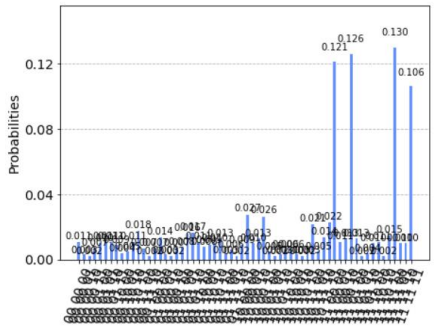


Figure 12. Quantum Circuit for Purification



(a) Ideal simulator



(b)Noisy simulator

Figure 13. Purification result

We can see here that for a low noise channel (0.01 error), only 40 percent of the results are reliable. However, the probability of each noisy answer is negligible compared to correct outcomes. See Appendix A for Qiskit codes.

After purification if the channel is safe enough to send Qubits, Alice can send one pair of her Entangled Qubits to the Bob using Swapping protocol [12]. Figure 14, shows the transmission of Qubit 1 over Quantum Channel to Bob.

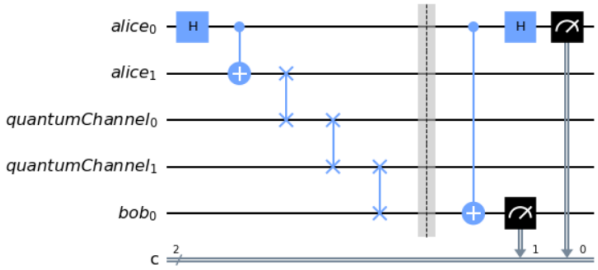
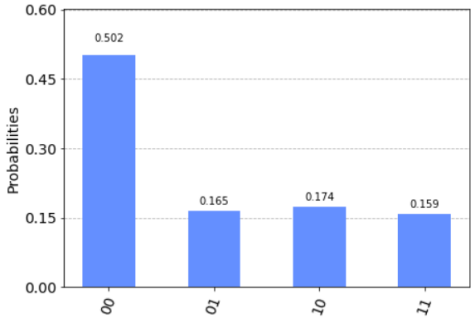


Figure 14. Entanglement transmission using swapping

The results from the measurement have been taken in two scenarios. The first one is with an ideal Quantum channel, and the second one is a noisy channel with 0.01 error for one port Quantum Gates. The error of multi-ports Quantum Gates can be derived respectively. Figure 15 shows the results of different measurements. For Qiskit codes of this part, see Appendix A.

(a)Qasm simulator with noise



(b) Ideal model

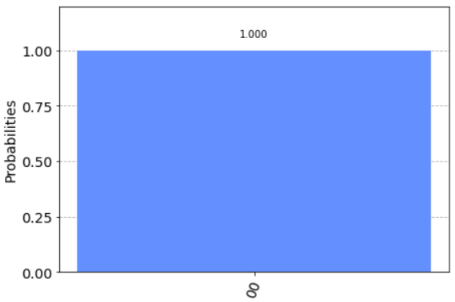


Figure 15. measurement results for Quantum Swapping

A repeater works like an amplifier with this difference that it is not amplifying anything but it is building a new link. So first thing is to divide that long path into shorter path and then

stablish a correlated link between them and then instead of amplifying the link and classically transfer it to another base station we can set another link with that station [13].

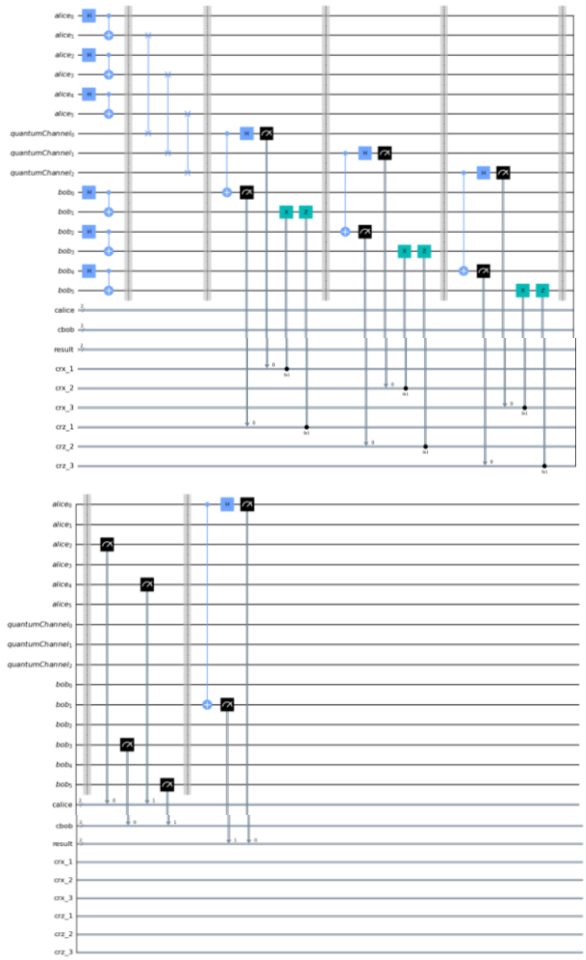


Figure 16. Quantum Repeater

This is the design of a Quantum-Repeater using Quantum-Circuits and Evaluating its Performance on an IBM software tool, Qiskit.

Conclusion

In the decades ahead, Quantum computation will improve, which could threaten classical cryptographic protocols. QKD has obstacles in its way to being a practical protocol. Quantum Repeaters are a feasible solution for Long-Distance Quantum Communication so far. Quantum repeaters cannot solely solve the noise and decoherence, so other protocols and technologies like Quantum purification, Quantum Memories, and Quantum Error Correction need to grow to have an efficient Quantum network.

Reference

[1] Wikipedia contributors. (2021, August 18). Samuel Morse. In Wikipedia, The Free Encyclopaedia. Retrieved 10:24, August19,2021,from:https://en.wikipedia.org/w/index.php?title=Samuel_Morse&oldid=1039331217

[2] Shannon, C. E., & Weaver, W. (1949). The mathematical theory of communication. Urbana: University of Illinois Press.

[3] Scott Aaronson. (January 2008).” The limits of quantum”. Journal: Scientific American. Volume: 298.Issue:3. Pages:62-69. Publisher: Scientific American, a division of Nature America, Inc.

[4] Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). Communications of the ACM. 21 (2): 120126.CiteSeerX10.1.1.607.2677.doi:10.1145/359340.359342. S2CID 2873616.

[5] Stephane Beauregard, Circuit for Shor's algorithm using 2n+3 qubits, arXiv: quant-ph/0205095

[6] Qiskit textbook. (2021, June 17). Shor’s Algorithm. From: https://qiskit.org/textbook/ch-algorithms/shor.html.

[7] Ethan Bernstein and Umesh Vazirani (1997) "Quantum Complexity Theory" SIAM Journal on Computing, Vol. 26, No. 5: 1411-1473, doi:10.1137/S0097539796300921.

[8] Jiangfeng Du, Mingjun Shi, Jihui Wu, Xianyi Zhou, Yangmei Fan, BangJiao Ye, Rongdian Han (2001) "Implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement on an ensemble quantum computer", Phys. Rev. A 64, 042306, 10.1103/PhysRevA.64.042306, arXiv: quant-ph/0012114.

[9] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. “Can Quantum-Mechanical Description of Physical Reality be Considered Complete? “.47, 777 (1935).

[10] N. Bohr.Phys. Rev. “Can Quantum-Mechanical Description of Physical Reality be Considered Complete? “.48, 696 – Published 15 October 1935

[11] Wootters, William; Zurek, Wojciech (1982). "A Single Quantum Cannot Be Cloned". Nature. 299 (5886): 802–803. Bibcode:1982Natur. 299..802W. doi:10.1038/299802a0.

[12] Sowmitra Das∗, Md. Saifur Rahman†and Mahbub Alam Majumdar. “Design of a Quantum-Repeater using Quantum-Circuits and Benchmarking its Performance on an IBM Quantum-Computer”. arXiv: 2009. 04584v1 [quant-ph] 9 Sep 2020.

[13] A Rastogi, E Saglamyurek, T Hrushevskyi, B Smith… “Towards a high-performance photonic quantum memory using Bose-Einstein condensate”- Bulletin of the American Physical Society, 2021

[14] Broadband Quantum Memories | University of Oxford Department of Physics. From: https://www.physics.ox.ac.uk/research/group/quantum-and-optical-technology

[15] Wikipedia contributors. (2021, June 14). Quantum Memory. In Wikipedia, The Free Encyclopaedia. last edited on 24 June 2021, at 08:26 (UTC)

[16] Qiskit textbook. (2021, June 17). Quantum Teleportation. From: https://qiskit.org/textbook/ch-algorithms/teleportation.html

[17] Heideman, M.T.; Johnson, D. H.; Burrus, C. S. (1984). "Gauss and the history of the fast Fourier transform". IEEE ASSP Magazine. 1 (4): 14–21. doi:10.1109/MASSP.1984.1162257. S2CID 10032502.

[18] Qiskit textbook. (2021, June 17). Quantum Fourier Transform. From: https://qiskit.org/textbook/ch-algorithms/quantum-fourier-transform.html

[19] Bedington, R., Arrazola, J.M. & Ling, A. Progress in satellite quantum key distribution. *npj Quantum Inf* **3,** 30 (2017). https://doi.org/10.1038/s41534-017-0031-5

Appendix

Appendix A

Bernstein-Vazirani algorithm:

```
#import libraries
from qiskit import *
from qiskit.tools.visualization import plot_histogram
number = 'number'

#Creating Quantum Circuit
Circuit = QuantumCircuit(len(number)+1,len(number))
%matplotlib inline

#Implementing Quantum Gate
Circuit.h(range(len(number)))
Circuit.x(len(number))
Circuit.h(len(number))
Circuit.barrier()

for i,k in enumerate(reversed(number)):
    if k == '1':
        Circuit.cx(i,len(number))

Circuit.barrier()

Circuit.h(range(len(number)))
#measuring the result
Circuit.measure(range(len(number)),range(len(number)))

simulator = Aer.get_backend('qasm_simulator')
result = execute(Circuit, backend=simulator, shots=1).result()
counts = result.get_counts()
Circuit.draw(output = 'mpl')
#print the result
print(counts)
```

Quantum Teleportation:

```
from qiskit import * #importing library
Qb = QuantumRegister(3)
Cb = ClassicalRegister(3)
circuit = QuantumCircuit(Qb,Cb)
%matplotlib inline  #here Q0 form Quantum Register
circuit.x(Qb[0])    #now we want to apply X operator to our first Qubit
from qiskit.tools.visualization import plot_bloch_multivector
circuit.barrier()   #we can put a barrier in our draw plot so that we can divide different stages
circuit.h(Qb[1])
circuit.cx(1,2)     # first we need to make the control qubit (|0> + |1>)/sqrt(2)
circuit.barrier()   #Q[1] and Q[2] are now entangled
circuit.cx(0,1)
circuit.h(Qb[0])
circuit.barrier()
circuit.measure(Qb[0],Cb[0])
circuit.measure(Qb[1],Cb[1])
circuit.barrier()
circuit.cx(1,2) #flip
circuit.cz(0,2) #phase - shift
simulator = Aer.get_backend('statevector_simulator')
result = execute(circuit,backend=simulator).result()
statevector =result.get_statevector()  #plot_bloch_multivector(statevector)
circuit.measure(Qb[2],Cb[2])
circuit.measure(Qb[1],Cb[1])
circuit.measure(Qb[0],Cb[0])
simulator = Aer.get_backend('qasm_simulator')
result = execute(circuit,backend = simulator, shots= 1024).result()
counts = result.get_counts()
from qiskit.tools.visualization import plot_histogram   #plot_histogram(counts)
```

Purification, ideal

```
circuit = QuantumCircuit(4,2)
%matplotlib inline #circuit.draw(output = 'mpl')
circuit.h(0)
circuit.h(2)
circuit.cx(0,1)
circuit.cx(2,3)
simulator = Aer.get_backend('statevector_simulator')
result = execute(circuit,backend=simulator).result()
statevector =result.get_statevector() #plot_bloch_multivector(statevector)
circuit.barrier()
circuit.cx(0,2)
circuit.cx(1,3)
circuit.barrier()
circuit.measure(2,0)
circuit.measure(3,1)
circuit.measure(2,0)
simulator = Aer.get_backend('qasm_simulator')
result = execute(circuit,backend = simulator, shots= 1024).result()
counts = result.get_counts()
from qiskit.tools.visualization import plot_histogram #plot_histogram(counts)
```

Purification, with noise

```
import qiskit.providers.aer.noise as noise # Error probabilities
prob_1 = 0.01  # 1-qubit gate
prob_2 = 0.1   # 2-qubit gate
error_1 = noise.depolarizing_error(prob_1, 1) # Depolarizing quantum errors
error_2 = noise.depolarizing_error(prob_2, 2)
noise_model = noise.NoiseModel()  # Add errors to noise model
noise_model.add_all_qubit_quantum_error(error_1, ['u1', 'u2', 'u3'])
noise_model.add_all_qubit_quantum_error(error_2, ['cx'])
basis_gates = noise_model.basis_gates # Get basis gates from noise model
circuit = QuantumCircuit(4,2)
circuit.h(0)
circuit.h(2)
circuit.cx(0,1)
circuit.cx(2,3)
circuit.barrier()
circuit.cx(0,2)
circuit.cx(1,3)
circuit.barrier()
circuit.measure(2,0)
circuit.measure(3,1)
result = execute(circuit, Aer.get_backend('qasm_simulator'),  # Perform a noise simulation
                 basis_gates=basis_gates,
                 noise_model=noise_model,shots = 1024).result()
counts = result.get_counts()  #plot_histogram(counts)
```

Quantum Swapping with noise

```
#swapping with noise
A = QuantumRegister(2, 'alice')
C = QuantumRegister(2, 'quantumChannel')
B = QuantumRegister(1, 'bob')
cl = ClassicalRegister(2, 'c')
Circuit = QuantumCircuit(A, C, B, cl)
Circuit.h(A[0])   # perform entanglement algorithm
Circuit.cx(A[0],A[1])
Circuit.swap(A[1],C[0])
Circuit.swap(C[0],C[1])
Circuit.swap(C[1],B)
Circuit.barrier()  #Circuit.draw(output='mpl')
Circuit.cx(A[0],B) # measurement  # inverse entanglement
Circuit.h(A[0])
Circuit.measure(A[0],cl[0])
Circuit.measure(B,cl[1])   #Circuit.draw(output = 'mpl')
result = execute(Circuit, Aer.get_backend('qasm_simulator'),  # Perform a noise simulation
                 basis_gates=basis_gates,
                 noise_model=noise_model,shots = 1024).result()
counts = result.get_counts()  #plot_histogram(counts)
simulator = Aer.get_backend('statevector_simulator')
result = execute(Circuit,backend=simulator).result()
statevector =result.get_statevector()
```

Quantum Swapping without noise

```
A = QuantumRegister(2, 'alice')
C = QuantumRegister(2, 'quantumChannel')
B = QuantumRegister(1, 'bob')
cl = ClassicalRegister(2, 'c')
CircuitB = QuantumCircuit(A, C, B, cl)
CircuitB.h(A[0])  # perform entanglement algorithm
CircuitB.cx(A[0],A[1])
CircuitB.swap(A[1],C[0])
CircuitB.swap(C[0],C[1])
CircuitB.swap(C[1],B)
CircuitB.barrier()
CircuitB.cx(A[0],B) # measurement  # inverse entanglement
CircuitB.h(A[0])
CircuitB.measure(A[0],cl[0])
CircuitB.measure(B,cl[1])
CircuitB.measure(2,0)
simulatorB = Aer.get_backend('qasm_simulator')
resultB = execute(CircuitB,backend = simulatorB, shots= 1024).result()
countsB = resultB.get_counts()
simulatorB = Aer.get_backend('statevector_simulator')
resultB = execute(CircuitB,backend=simulatorB).result()
statevectorB =resultB.get_statevector()  #plot_histogram(countsB)
```

QFT

```
from qiskit.circuit.library import QFT
from qiskit.quantum_info import Statevector
from qiskit import QuantumCircuit
from qiskit.visualization import plot_bloch_multivector
import warnings
warnings.filterwarnings('ignore')
state = 'State'
FourierCircuit = QuantumCircuit(len(state))
FourierCircuit.initialize(Statevector.from_label(state).data,FourierCircuit.qubits[::-1])
display(plot_bloch_multivector(Statevector.from_instruction(FourierCircuit).data))
FourierCircuit.append(QFT(len(state),do_swaps=True),FourierCircuit.qubits)
display(plot_bloch_multivector(Statevector.from_instruction(FourierCircuit).data))
```

Shor's algorithm

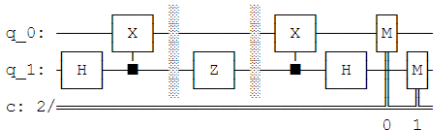
```
def a_x_mod15(a, x):
    if a not in [2,7,8,11,13]:
        raise ValueError("'a' must be 2,7,8,11 or 13")
    U = QuantumCircuit(4)
    for iteration in range(x):
        if a in [2,13]:
            U.swap(0,1)
            U.swap(1,2)
            U.swap(2,3)
        if a in [7,8]:
            U.swap(2,3)
            U.swap(1,2)
            U.swap(0,1)
        if a == 11:
            U.swap(1,3)
            U.swap(0,2)
        if a in [7,11,13]:
            for q in range(4):
                U.x(q)
    U = U.to_gate()
    U.name = "%i^%i mod 15" % (a, x)
    c_U = U.control()
    return c_U
#####End of Function#####
```

```
n = 4; m = 4; a = 7
# set up quantum circuit
shor = QuantumCircuit(n+m, n)
shor.draw()
# initialize the qubits
shor.h(range(n))
shor.x(m+n-1)
shor.barrier()
shor.draw()
# apply modular exponentiation
for x in range(n):
    exponent = 2**x
    shor.append(a_x_mod15(a, exponent),
        [x] + list(range(n, n+m)))

shor.barrier()
shor.draw()
# apply inverse QFT
from qiskit.circuit.library import QFT
shor.append(QFT(n).inverse(),range(n))
shor.barrier()
shor.draw()
# measure the first n qubits
shor.measure(range(n), range(n))
shor.draw()
```

Dense Coding

```
# Importing everything
from qiskit import QuantumCircuit
from qiskit import IBMQ, Aer, transpile, assemble
from qiskit.visualization import plot_histogram
##############################################################################
def create_bell_pair():
    """
    Returns:
        QuantumCircuit: Circuit that produces a Bell pair
    """
    qc = QuantumCircuit(2,2)    #Creating two Qubits at C
    qc.h(1)
    qc.cx(1, 0)               #Entangled Qubits
    return qc
##############################################################################
def encode_message(qc, qubit, msg):
    """Encodes a two-bit message on qc using the superdense coding protocol
    Args:
        qc (QuantumCircuit): Circuit to encode message on
        qubit (int): Which qubit to add the gate to
        msg (str): Two-bit message to send
    Returns:
        QuantumCircuit: Circuit that, when decoded, will produce msg
    Raises:
        ValueError if msg is wrong length or contains invalid characters
    """
    if len(msg) != 2 or not set([0,1]).issubset({0,1}):
        raise ValueError(f"message '{msg}' is invalid")
    if msg[1] == "1":
        qc.x(qubit)
    if msg[0] == "1":
        qc.z(qubit)
    return qc
##############################################################################
# Charlie creates the entangled pair between Alice and Bob
qc = create_bell_pair()

# We'll add a barrier for visual separation
qc.barrier()

# At this point, qubit 0 goes to Alice and qubit 1 goes to Bob

# Next, Alice encodes her message onto qubit 1. In this case,
# we want to send the message '10'. You can try changing this
# value and see how it affects the circuit
message = '10'
qc = encode_message(qc, 1, message)
qc.barrier()
# Alice then sends her qubit to Bob.

# After recieving qubit 0, Bob applies the recovery protocol:
qc = decode_message(qc)

# Finally, Bob measures his qubits to read Alice's message
qc.measure(0,0)
qc.measure(1,1)
# Draw our output
qc.draw()
##############################################################################
simulator = Aer.get_backend('qasm_simulator')
result = execute(qc, backend=simulator, shots=1).result()
counts = result.get_counts()
print(counts)
```

Out[7]:



In [8]:

```
simulator = Aer.get_backend('qasm_simulator')
result = execute(qc, backend=simulator, shots=1).result()
counts = result.get_counts()
print(counts)
```

```
{'10': 1}
```

Repeater

```
from qiskit import *
from qiskit.tools.visualization import plot_bloch_multivector
from qiskit.tools.visualization import plot_histogram
```

```
def swap(qc, qubit_1, qubit_2, qubit_3,crx,crz):
    qc.cx(qubit_1,qubit_2)
    qc.h(qubit_1)
    qc.measure(qubit_2,crz)
    qc.measure(qubit_1,crx)
    qc.x(qubit_3).c_if(crx, 1) # Apply gates if the registers
    qc.z(qubit_3).c_if(crz, 1) # are in the state '1'
    Circuit.barrier()
```

```
A = QuantumRegister(6, 'alice')
C = QuantumRegister(3, 'quantumChannel')
B = QuantumRegister(6, 'bob')
ca = ClassicalRegister(2, 'calice')
cb = ClassicalRegister(2, 'cbob')
cc = ClassicalRegister(2, 'result')
crz_1, crx_1 = ClassicalRegister(1, name="crz_1"), ClassicalRegister(1, name="crx_1")
crz_2, crx_2 = ClassicalRegister(1, name="crz_2"), ClassicalRegister(1, name="crx_2")
crz_3, crx_3 = ClassicalRegister(1, name="crz_3"), ClassicalRegister(1, name="crx_3")
Circuit = QuantumCircuit(A, C, B, ca,cb,cc,crx_1,crx_2,crx_3,crz_1,crz_2,crz_3)
#Entanglement
#H
#Alice
Circuit.h(A[0])
Circuit.h(A[2])
Circuit.h(A[4])
#Bob
Circuit.h(B[0])
Circuit.h(B[2])
Circuit.h(B[4])
#CNOT
#Alice
Circuit.cx(A[0],A[1])
Circuit.cx(A[2],A[3])
Circuit.cx(A[4],A[5])
#Bob
Circuit.cx(B[0],B[1])
Circuit.cx(B[2],B[3])
Circuit.cx(B[4],B[5])
Circuit.barrier()
##############################################################
swap(Circuit,C[0],B[0],B[1],crx_1,crz_1)
swap(Circuit,C[1],B[2],B[3],crx_2,crz_2)
swap(Circuit,C[2],B[4],B[5],crx_3,crz_3)
##############################################################
```

```
from math import pi
#Alice
Circuit.ry(pi/2,A[0])
Circuit.ry(pi/2,A[2])
Circuit.ry(pi/2,A[4])
#Bob
Circuit.ry(-pi/2,B[1])
Circuit.ry(-pi/2,B[3])
Circuit.ry(-pi/2,B[5])
Circuit.barrier()
##############################################################################
#Alice
Circuit.cx(A[0],A[2])
Circuit.cx(A[0],A[4])
#Bob
Circuit.cx(B[1],B[3])
Circuit.cx(B[1],B[5])
Circuit.barrier()
##############################################################################
Circuit.measure(A[2],ca[0])
Circuit.measure(B[3],cb[0])
Circuit.measure(A[4],ca[1])
Circuit.measure(B[5],cb[1])
Circuit.barrier()
##############################################################################
Circuit.cx(A[0],B[1])
Circuit.h(A[0])
Circuit.measure(B[1],cc[1])
Circuit.measure(A[0],cc[0])
Circuit.draw(output='mpl')
```

Appendix B

Bernstein-Vazirani algorithm:

Consider the case of a number with n=2

$step\ 1$:
$|\varphi> = |00>$
$step\ 2$:
$|\emptyset> = H\,|\varphi> = \frac{|00>+|01>+|10>+|11>}{\sqrt{2}}$
$step\ 3$:
$|\emptyset> = \frac{(-1)^{00\cdot number}|00>+(-1)^{01\cdot number}|01>+(-1)^{10\cdot number}|10>+(-1)^{11\cdot number}|1}{\sqrt{2}}$
$step\ 4$:
$number = 10$
$|\emptyset> = \frac{-|00>+|01>+|10>-|11>}{\sqrt{2}}$
$H\,|\emptyset> = |10>$

Teleportation Protocol:

Alice ***Bob***

$A' = |m> = \alpha|0> + \beta|1>$

$A \leftrightarrow B$ $B \leftrightarrow A$

Total Quantum System : $|m> \otimes |\Psi>_{AB}$

$[\alpha|0> + \beta|1>] \otimes \left[\frac{|00>+|11>}{\sqrt{2}}\right]$

$\frac{1}{2\sqrt{2}}\alpha|000> + \frac{1}{2\sqrt{2}}\beta|001> + \frac{1}{2\sqrt{2}}\alpha|110> + \frac{1}{2\sqrt{2}}\beta|111> +$

$\frac{1}{2\sqrt{2}}\alpha|000> - \frac{1}{2\sqrt{2}}\beta|001> - \frac{1}{2\sqrt{2}}\alpha|110> + \frac{1}{2\sqrt{2}}\beta|111> +$

$\frac{1}{2\sqrt{2}}\alpha|011> + \frac{1}{2\sqrt{2}}\beta|010> + \frac{1}{2\sqrt{2}}\alpha|101> + \frac{1}{2\sqrt{2}}\beta|100> +$

$\frac{1}{2\sqrt{2}}\alpha|011> - \frac{1}{2\sqrt{2}}\beta|010> - \frac{1}{2\sqrt{2}}\alpha|101> + \frac{1}{2\sqrt{2}}\beta|100>$

$\frac{1}{2}|\Psi_1> \otimes |m_1> + \frac{1}{2}|\Psi_2> \otimes |m_2> + \frac{1}{2}|\Psi_3> \otimes |m_3> + \frac{1}{2}|\Psi_4> \otimes |m_4>$

$|\Psi_1> = \frac{|00>+|11>}{\sqrt{2}}$, $|\Psi_2> = \frac{|00>-|11>}{\sqrt{2}}$, $|\Psi_3> = \frac{|01>+|10>}{\sqrt{2}}$, $|\Psi_4> = \frac{|01>-|10>}{\sqrt{2}}$

$|m_1> = \alpha|0> + \beta|1>$, $|m_1> = \alpha|0> - \beta|1>$, $|m_1> = \beta|0> + \alpha|1>$, $|m_1> = \beta|0> - \alpha|1>$

Shor's algorithm:

Begin algorithm:

(1) Pick "a" coprime with N=pq ≡ gcd(a,N) = 1

(2) Find the "order" r of the function
$a^r\ (mod\ N)\ \equiv smallest\ r\ such\ that\ a^r \equiv 1\ (mod\ N)$

(3) If r is even,
$x \equiv a^{\frac{r}{2}}\ (mod\ N)$
If $x + 1 \neq 0\ (mod\ N)\ then$
$\{p.q\} = \{\gcd(x+1.N)\ .\ \gcd(x-1.N)\}$
Else: find another "a"

$If\ the\ Classical\ bits\ are$: 10

$\frac{1}{\sqrt{2}}(|00> + |11>)$

$Z\ Gate$:

$\frac{1}{\sqrt{2}}(|00> - |11>)$

$Alice's\ bits\ are\ the\ controled\ bits\ \_\ CNOT$

$\frac{1}{\sqrt{2}}(|00> - |10>)$

$H\ Gate$:

$\frac{1}{\sqrt{2}}(|+0> - |-0>)$

$\frac{1}{2}(|00> + |10> - |00> + |10>) = |10>$

University of Tehran

College of Engineering

School of Electrical and Computer Engineering

Long Distance Quantum Communication Using Repeaters

A thesis submitted to the Undergraduate Studies Office

In partial fulfilment of the requirements for

The degree of Undergraduate in

Electrical Engineering

By:

Mohadeseh Azari

Supervisor:

Dr. Saleh Rahimi-Keshari (Faculty of Physics) / Dr. Leila Yousefi (Faculty of Electrical and Computer Engineering)