CONTENTS

Quantum Bitcoin and Cheque

ABSTRACT

The goal of the project is to explore the vulnerabilities of the current classical algorithm for encryption and hashing of crypto-currencies when subjected to quantum computing and to design more secure quantum algorithms.

I. INTRODUCTION

We shall start with a background of the classical computations and then develop quantum methods for the same.

A. Background

Blockchain is the method used at present for secure peer to peer transactions through decentralized currencies[1]. It comprises peers broadcasting transactions on a decentralized ledger, secured by a digital signature. The signature can be generated uniquely by the use of a private key held by the node generating the signature only. The other peers can verify the authenticity of the signature using a widely available public key. Since copies of ledgers are possessed by all the peers on the network, it is imperative to develop a form of authenticity check on the ledgers. This is doing by using a special string called the nonce, which is in turn dependent on the contents of the ledger, to generate a hash satisfying some conditions. Mathematics show that brute force search is the only method for generating such a nonce. The probability of success is of the order of $\frac{1}{2^N}$, where N is the number of bits used for hashing. For a standard 256-bit hash, the probability of finding a special nonce is too low for all practical purposes. Thus, "guessing" a nonce is nearly next to impossible at an individual level. To increase the security even further, blocks of transactions with a valid nonce are linked together in the form of a chain to prevent any fraudulent manipulation of previous transactions. This is called a block chain. Quantum computing is a form of computing that uses the quantum mechanical states of particles, called qubits, to store information, instead of storing them on classical switches. Two special properties of qubits are that they can undergo superposition and entanglement. These properties allow special quantum algorithms to be developed, which speed an otherwise slow classical process. Quantum computers are speculated to

posses serious threats to the classical computing algorithms[2], including those used in the security of bitcoins. Quantum algorithms like Grover's algorithm and a more generalized version of it can search for the nonce much faster than a classical computer.

B. Objectives And Applications

The aim of the project is to find loopholes in the present system of cryptocurrency[1] when subjected to quantum computation and to find methods to improve the security. The problem at hand involves understanding the current methods of encryption and hashing, following by designing a quantum algorithm to break the same. At the last leg of the project, we shall solve these problems by using quantum algorithms for hashing.

Our work may be used to develop and enhance secure quantum algorithms for crypto-currencies. The algorithms presented in our work can also be used to design a new crypto-currency system on a real quantum computer back-end.

C. System Requirements

The code for our work uses Qiskit on a Jupyter Notebook on Python. The following are the minimum system requirements to run our code.

Processors: Intel Atom processor or Intel Core™ i3 processor or higher

Disk space: 1 GB or higher

Operating systems: Windows 7 or later, macOS 10.12.6 or later, and Ubuntu 16.04 or later

Python: 3.6 or higher

Numpy: 1.20.0 or higher

Jupyter Lab/Notebook: 6.3.0 or higher

II. BLOCKCHAIN

In this section we shall discuss the main ideas of the blockchain system[1]. The basic unit of currency is defined as a block containing information about a transaction. The transaction is signed using an encrypted signature. The signature requires a private key to generate and a public key for verification. Details of some encryption methods are discussed later. Once a block signature has been verified, it is considered as a "legal block". To prevent peers from double spending, it is imperative to store all records of previous transactions in the block. This is made possible by storing some information of the previous block in the next block. Further, to ensure the correct chronology of these blocks, a timestamp (epoch) is used in the block, which marks the time of creation of the block. Since each block contains information about the previous block, the timestamp will be linear in the chain. Any discrepancies regarding this is indicative of a fraudulent block. Finally, we come to the main point that is relevant to our work. How does one ensure, in such a decentralized system, that there is no manipulation of information? This is achieved by hashing. Hashing the information in the block produces a 256-bit long hash. It is easy to verify a hash from a block but very difficult to generate a block that produces a given hash[3]. Also, changing even a single character can cause a huge change in the hash. Details of hashing are discussed in more detail later Whether a block should be trusted or not is governed by the concept of "Proof of Work". This involves finding an arbitrary string, called the nonce, by brute-force, to be appended at the end of the block so that its hash starts with a certain minimum number of zeroes. To prevent manipulation of previous transactions, each block starts with the hash of the previous block. Resources in terms of CPU and electricity are used in huge quantities to generate these nonce. Any fraudulent party working individually to manipulate information in the blockchain will be unable to compete in terms of resources to find a proof of work for successive chains. This will in turn ensure that the longest chain is the most trusted one in case of a fork and the other short chains are automatically rejected. Figure II.1 shows the contents of a block. Figure II.2 shows a pictorial representation of a blockchain.

The working of a blockchain system is summarized below.

1. New transactions are broadcast to all nodes.

2. Each node collects new transactions into a block.

3. Each node works on finding a difficult proof-of-work for its block.

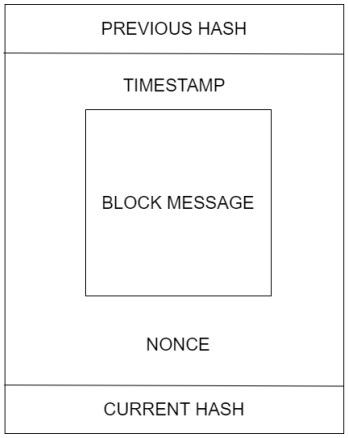

FIG. II.1. A typical block

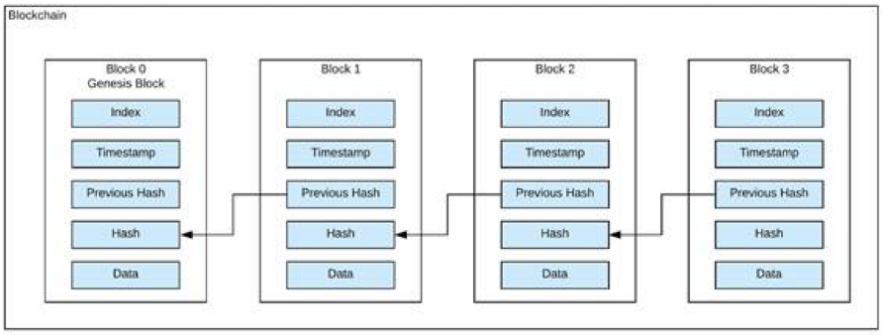

FIG. II.2. The structure of a block chain[4]

4. When a node finds a proof-of-work, it broadcasts the block to all nodes.

5. Nodes accept the block only if all transactions in it are valid and not already spent.

6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

III. CLASSICAL ALGORITHMS

In this section, we will take a look at each of the components of the blockchain implemented classically.

A. Encryption

Encryption is used to digitally sign transactions in a blockchain. Encryption is the process by which data is converted into a secure string of bits that can be uniquely decrypted. Encryption requires the use of a private key to decrypt an encrypted message and a public key to verify the encryption. Several encryption algorithms exists in the market, the most popular ones being the 3DES, AES and RSA[5].

B. Hashing

Hashing is the process by which a message of arbitrary lengths is converted to a bit string of fixed length. Unlike encryption, hashes are not unique. Several messages can have the same hash. Hashes must be easy to verify given a message. The reverse process, however, should be a hard one, i.e., given a hash, it should be practically impossible to find a message generating the hash. Hash collisions should also be rare, i.e., given a message and its hash, it should be practically impossible to find another message with the same hash. Finally, hashes must be distinctly different even for change of a single character in the message. Some commonly used hashing algorithms include SHA-1, Pearson Hash and SHA-256. In this paper, we will demonstrate the SHA-256. We will then design a surrogate hashing purpose that satisfies the aforementioned properties of hashes but is easy to simulate on a quantum computer.

SHA-256

This comprises using XOR and shift operators on registers pre-loaded with existing values. The code for the same is mentioned below. The code is written in python.

```
import math
import numpy as np
```

```
#The first 32 prime numbers are used to preset the hash registers by considering
    ↪ the fractional part of their square and cube roots
PRIMES=[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,
    ↪ 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149,
    ↪ 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229,
    ↪  233, 239, 241, 251, 257, 263, 269, 271,277,281,283,293,307,311]


#Right shift by n bits
def SHR_int(x,n):
    return x>>n
def SHR(s,n):
    x=int(s,2)
    return str(bin(x>>n))[2:].zfill(32)


#Right rotate by n bits
def ROTR_int(x,n):
    return (x>>n)|(x<<(32-n))&0xFFFFFFFF
def ROTR(s,n):
    x=int(s,2)
    return str(bin((x>>n)|(x<<(32-n))&0xFFFFFFFF))[2:].zfill(32)


#Linear combination in terms of XOR
def SIG0(x):
    return ROTR_int(x,2)^ROTR_int(x,13)^ROTR_int(x,22)
def SIG1(x):
    return ROTR_int(x,6)^ROTR_int(x,11)^ROTR_int(x,25)
    #return x
def sig0(s):
    x=int(s,2)
    return str(bin(ROTR_int(x,7)^ROTR_int(x,18)^SHR_int(x,3)))[2:].zfill(32)
def sig1(s):
    x=int(s,2)
```

```
    return str(bin(ROTR_int(x,17)^ROTR_int(x,19)^SHR_int(x,10)))[2:].zfill(32)
def che(x,y,z):
    return (x&y)|(~x&z)
def maj(x,y,z):
    return (x&y)^(y&z)^(z&x)

#Converts message to ASCII
def toAscii(message):
    return ''.join(str(bin(ord(c)))[2:].zfill(8) for c in message)

#Pads the message with zeroes till length is a multiple of 512 and then appends
    ↪ the length at the end
def padding(message_ascii):
    l=len(message_ascii)
    size=(l//512+1)*512
    pad=message_ascii+'1'
    for j in range(size-len(pad)-64):
        pad=pad+'0'
    pad=pad+str(bin(len(toAscii(message))))[2:].zfill(64)
    return pad,size

#Creates the message block
def message_block(message):
    padded_message=padding(toAscii(message))[0]
    nblocks=padding(toAscii(message))[1]//512
    w=[[None for _ in range(64)] for _ in range(nblocks)]
    for i in range(nblocks):
        for j in range(16):
            w[i][j]=padded_message[512*i+32*j:512*i+32*(j+1)]
        for j in range(16,64):
            w[i][j]=str(bin((int(sig1(w[i][j-2]),2)+int(w[i][j-7],2)+int(sig0(w[i
                ↪ ][j-15]),2)+int(w[i][j-16],2))%int(2**32)))[2:].zfill(32)
```

```
    return w


#Compression where registers are continuously updated with values of the linear
    ↪ functions above to generate the hash
def compress(w,H0):
    H=H0
    for j in range(len(w)):
        wj=int(w[j],2)
        T1=(K[j]+wj+SIG1(H[4])+che(H[4],H[5],H[6])+H[7])%int(2**32)
        T2=(SIG0(H[0])+maj(H[0],H[1],H[2]))%int(2**32)
        H=[(T1+T2)%int(2**32) ]+H[:-1]
        H[4]=(H[4]+T1)%int(2**32)
    return [(H0[i]+H[i])%int(2**32) for i in range(len(H))]


#Generates the hash in hexadecimal
def hashgen(message,H0):
    w=message_block(message)
    H=H0
    for i in range(len(w)):
        H=compress(w[i],H)
    return ''.join(str(hex(x))[2:].zfill(8) for x in H)


#Actually initializing the registers
K=[]
H=[]
for i in range(64):
    K.append(int(math.modf((PRIMES[i])**(1/3))[0]*(2**32)))
for i in range(8):
    H.append(int(math.modf((PRIMES[i])**(1/2))[0]*(2**32)))


#Inputiing the message from the user
message=input().rstrip()
```

```
#Printing the hash
print(hashgen(message,H))
```

Now we shall check the values of the hash for some sample strings. This can be done by running the code given above.

Message: `Hello World`

Hash: `a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e`

Making a slight change

Message: `Hello Workd`

Hash: `5ab45e33f10c8c9eb8005ba117fbd6e9d4ce3e61d5b199c08cbb7bbebf58cf68`

We see that the hash changes significantly.

Surrogate Hash Function: Pearson Hashes and LFSRs

The SHA-256 is a rather cumbersome method of hashing that requires significant amount of time and memory when simulating using qiskit. To overcome this difficulty, we will use a surrogate hash called the Pearson Hash[6]. The Pearson Hash makes use of a lookup table, which can be achieved using Linear Feedback Shift Registers (LFSR)[7]. These are easy to implement in qiskit[8], and the hash so generated satisfies the properties of a good hash. Since the purpose of our project is the search for nonce for a given hashing algorithm and not hashing, using a surrogate hashing algorithm will make no difference.

An LFSR comprises shift registers in which, at each iteration, the elements shift to the adjacent register (like in an ordinary shift register) and the first register takes the value of a linear function of some of the registers. Galois Theory of Fields dictates the working of these LFSRs (See VIII C). The values which are XORed are called taps. The LFSR structure is shown in Figure III.1 where $\oplus$ denotes XOR.

Pearson hashing uses two LFSRs. It works by taking the XOR of a character with the register and then performing two different sets of LFSRs. While LFSRs by themselves are reversible, it is impossible to extract the characters of a message from the hashing owing to the repeated XOR operations.

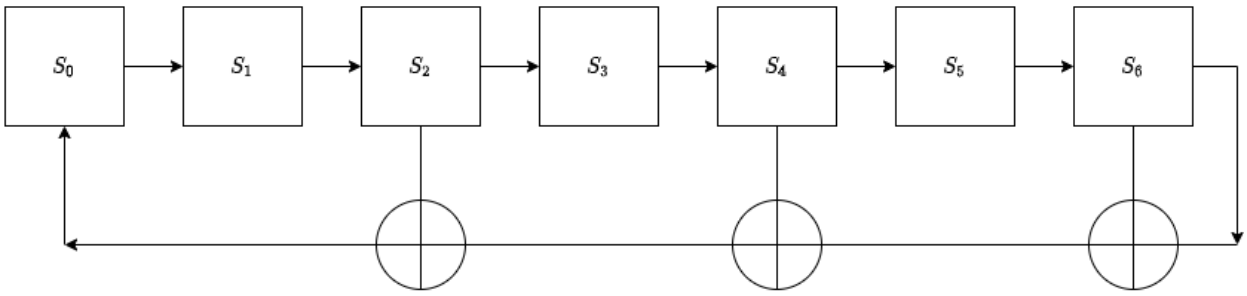

FIG. III.1. A sample LFSR with taps at 2,4 and 6

C. The Epoch, Nonce and Mining

The time stamp appended in a block (see II.1) is called an epoch. It is a 4-byte integer that represents the number of seconds passed from January 1, 1970 00:00 UTC.

The nonce is the arbitrary string that needs to be found by brute force algorithms to ensure the hash starts with a certain minimum number of zeroes. The process of finding the nonce is called "mining" in the language of crypto-currencies. Mining requires heavy use of resources like electricity and computing power. Bitcoin miners are often provided with incentives for the process. Since we have a 256-bit hash, mining success probability is of the order of 2^{-256}, a number that is astronomically small. Mining is a form of proof of work that ensures fraudulent individuals do not take advantage of a decentralized ledger. If the majority mines honest blocks, it becomes easy for someone or the other to get the nonce. In case of a fork in terms of two different blockchains with appropriate nonces, the longer blockchain gets accepted.

The hash function that we are using generates 8-bit long hashes. Our nonce can thus be 8-bit long, which can be represented by a single character.

IV. QUANTUM COMPUTING FOUNDATIONS

Before delving into quantum algorithms, it would be worthwhile to take a quick glance into the basics of quantum computing. Quantum computing uses the quantum state of a particle as the building block of information. Each such particle is called a qubit. These qubits follow the postulates of quantum mechanics[9], namely

1. The state of the particle is represented as a vector $|\psi(t)\rangle$ in a Hilbert Space.

2. The independent variables x and p of classical mechanics are represented by Hermitian operators X and P satisfying $\langle x|X|x\prime\rangle = x\delta(x - x\prime)$ and $\langle x|P|x\prime\rangle = -\iota\hbar\delta\prime(x - x\prime)$.

3. If a particle is in a state $|\psi\rangle$, measurement of the variable corresponding to the operator Ω will yield one of the eigenvalues ω with probability $P(\omega) \propto |\langle\omega|\psi\rangle|^2$. The state of the system will change from $|\psi\rangle$ to $|\omega\rangle$ as a result of the measurement.

4. The state vector $|\psi\rangle$ obeys the Schrödinger Equation $\iota\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle$, where $\hat{H}$ is the quantum Hamiltonian operator.

A. Qubits

As discussed before, qubits are the particles whose quantum states store the necessary information. To retrieve the information, we perform measurements using an unitary operator that has 2 eigenstates. These eigenstates are denoted as $|0\rangle$ and $|1\rangle$. Since the measurement operator is unitary, these eigenstates are orthonormal. The 2 eigenstates represents the two possible values of a classical bit, except that quantum mechanics allows **superposition** and **entanglement**, which are discussed subsequently.

B. Superposition

In general, quantum mechanics is probabilistic and not deterministic, i.e., the two eigenstates may not be the only possible states of a qubit. A qubit can be in a superposition of two states, in the form $|\psi\rangle = \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{2}}$ with the only requirement that $|\alpha|^2 + |\beta|^2 = 1$ (this is called normalization. When a measurement is performed on this state, the state collapses to either $|0\rangle$ with probability $|\alpha|^2$ or to $|1\rangle$ with probability $|\beta|^2$.

Since $|0\rangle$ and $|1\rangle$ are orthonormal, they form an orthonormal basis for the states. Each state can then be represented in the form of a vector as

$$|\psi\rangle = \frac{\alpha\,|0\rangle + \beta\,|1\rangle}{\sqrt{2}} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{IV.1}$$

This immediately yields

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

Any state can now be written as the linear combination of these two states. Upon measurement, however, the superposition is lost and the system collapses to either of the eigenstates.

Since an operator operates on one state to produce another state, they can be viewed as transforming one vector to another. Thus, they can be expressed as matrices. The postulates of quantum mechanics dictate that these operators must be unitary to yield compatible, real-valued measurement.

C. Multiple Qubits

Often we encounter multiple qubit systems. The state of such a system is decided by the states of the individual qubits. The direct product of the basis states form the basis (also called pure states) for the multi-qubit system.

As an example, consider the 2-qubit system. The basis set for such a system will be formed by the 4 basis states : $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$. These are notationally written as

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Any two-qubit system is a superposition of the 4 states mentioned above. However, not all two-qubit states are expressible as a direct product of two one-qubit states. This is called **entanglement**, which forms the basis for quantum teleportation, and spooky action at a distance.
For a multi-qubit system, we often use the decimal equivalent of a binary number to express the basis. For example, in a 4-qubit system, $|12\rangle = |1100\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |0\rangle$.

D. Quantum Gates

Any logical circuit requires the use of gates. A classical circuit uses AND, NOT, OR etc. as gates. Likewise, a quantum circuit uses unitary operators as gates. A gate can be expressed as a matrix. Some of the useful gates are presented below.

Hadamard Gate

The Hadamard gate is a **one-qubit** gate that is denoted by H. It performs the operation of transforming the standard basis of $|0\rangle$ and $|1\rangle$ into the Hadamard basis of $|+\rangle$ and $|-\rangle$ respectively as follows.

$$H|0\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$H|1\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

The matrix representation is

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The corresponding circuit diagram is given in figure IV.1

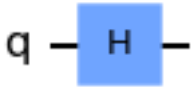

FIG. IV.1. Hadamard gate

X Gate

The Pauli-X gate is a **one-qubit** gate that is denoted by X (See VIII C for more details about Pauli Gates). It performs the operation of a classical NOT, i.e., it operates like the Pauli matrix σ_x as follows.

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

The matrix representation is

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The corresponding circuit diagram is given in figure IV.2

FIG. IV.2. X gate

Y Gate

The Pauli-Y gate is a **one-qubit** gate that is denoted by Y. It operates like the Pauli matrix σ_y as follows.

$$Y|0\rangle = -\iota|1\rangle = \begin{pmatrix} 0 \\ -\iota \end{pmatrix}$$
$$Y|1\rangle = \iota|0\rangle = \begin{pmatrix} \iota \\ 0 \end{pmatrix}$$

The matrix representation is

$$Y = \begin{pmatrix} 0 & -\iota \\ \iota & 0 \end{pmatrix}$$

The corresponding circuit diagram is given in figure IV.3

FIG. IV.3. Y gate

Z Gate

The Pauli-Z gate is a **one-qubit** gate that is denoted by Z. It operates like the Pauli matrix σ_z as follows.

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

$$Z|1\rangle = -|1\rangle = -\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The matrix representation is

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The corresponding circuit diagram is given in figure IV.4

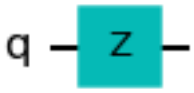

FIG. IV.4. Z gate

R_x Gate

The R_x gate is a **one-qubit** unitary gate that takes a parameter θ. It is given by the matrix

$$R_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\iota \sin\left(\frac{\theta}{2}\right) \\ -\iota \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

R_y Gate

The R_y gate is a **one-qubit** unitary gate that takes a parameter θ. It is given by the matrix

$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & \sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

R_z Gate

The R_z gate is a **one-qubit** unitary gate that takes a parameter θ. It is given by the matrix

$$R_z(\theta) = \begin{pmatrix} e^{-\iota\frac{\theta}{2}} & 0 \\ 0 & e^{\iota\frac{\theta}{2}} \end{pmatrix}$$

CX Gate

The CNOT (or CX) gate is a **two-qubit** gate that is denoted by CX. It operates a classical NOT, i.e., an X gate on the second qubit if the first qubit is $|1\rangle$. Its working is shown below.

$$CX\,|00\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$CX\,|01\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$CX\,|10\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$CX\,|11\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

The matrix representation is

$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Note that the order of the qubits is important here. The corresponding circuit diagram is given in figure IV.5

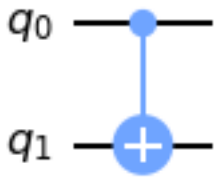

FIG. IV.5. CX gate

CZ Gate

The CZ gate is a **two-qubit** gate that is denoted by CZ. It is like a classical AND gate which flips the sign if and only if both qubits are $|1\rangle$. Its working is shown below.

$$CZ\,|00\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$CZ\,|01\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$CZ\,|10\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$CZ\,|11\rangle = -\,|11\rangle = - \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

The matrix representation is

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Note that the order of the qubits is unimportant here. The corresponding circuit diagram is given in figure IV.6

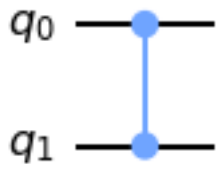

FIG. IV.6. CZ gate

SWAP Gate

The SWAP gate is a **two-qubit** gate that is denoted by $SWAP$. It swaps the two qubits. Its working is shown below.

$$SWAP\,|00\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$SWAP\,|01\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$SWAP\,|10\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$SWAP\,|11\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

The matrix representation is

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Note that the order of the qubits is unimportant here. The corresponding circuit diagram is given in figure IV.7

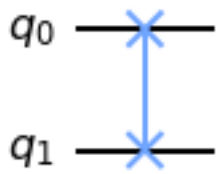

FIG. IV.7. *SWAP* gate

MCT Gate

The Multi Controlled Toffoli (MCT) gate is a **multi-qubit** gate that is denoted by MCT.It puts a negative sign on the target qubit if all the control qubits are $|1\rangle$. The matrix representation is

$$MCT = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix}$$

Note that the order of the qubits is unimportant here. The corresponding circuit diagram is given in figure IV.8

Note that gates can be cascaded. The order of operations of the gates is important. If we have gates G_1 and G_2, then $G_1G_2\,|\psi\rangle$ means G_2 is operated first on $|\psi\rangle$ and then G_1 is applied on the resulting states. Sometimes, cascading gates may result in an equivalent gate. As an example, cascading the operation of H followed by X is same as R_y since $XH = R_y$ (this is trivial and can be easily verified).

E. Entanglement

Entanglement is the is phenomenon where two or more quantum particles (qubits) are correlated and measurement of one particle collapses the wavefunction of the other particles. A simple example

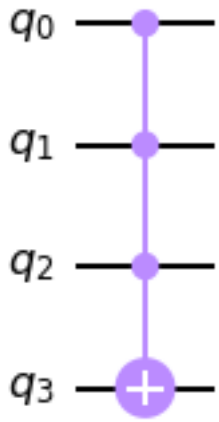

FIG. IV.8. *MCT* gate on 4 qubits

of an entangled state is

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

If the measurement of the first particle collapses to $|0\rangle$, the second particle collapses to $|0\rangle$ as well. Note that entangled states cannot be factored into a direct product of two single qubit states. This is a phenomenon that is purely quantum mechanical and is extremely useful in secure communication. This is because, since a measurement of any one particle collapses the wavefunction of the other particles as well, eavsdroppers will never go unnoticed, unlike in the classical case. To measure entanglement, we use the concepts of Bell's inequality. Entanglement has led to several paradoxes as well, the most famous of which is the EPR paradox presented in VIII C

V. GROVER'S ALGORITHM

Grover's search algorithm[10] is an important quantum algorithm that provides an edge over all classical algorithms in database search. Grover's algorithm shall form the backbone for our search for the nonce. The algorithm uses repeated iterations of a quantum oracle (an oracle stands for a special function) and a diffuser on a superposition of $|0\rangle$ and $|1\rangle$.

A. Oracle

The oracle is the function that "marks" the states which are the successful search results by applying a negative sign on it. Consider the state $|\omega\rangle$ to be successful. Denote the oracle by U_ω so that

$$U_\omega |x\rangle = \begin{cases} |x\rangle & x \neq \omega \\ -|x\rangle & x = \omega \end{cases} \tag{V.1}$$

The purpose of the oracle is to reflect the coefficient of "solution state ket" about 0, keeping the other coefficients intact. This will help the diffuser amplify amplitudes.

B. Diffuser

The diffuser is the key component of the Grover Search algorithm. The diffuser amplifies the amplitude of the solution states. It does this by reflecting the amplitudes of the states about the average amplitude. We denote the diffuser by U_s, so that

$$U_s = 2|s\rangle\langle s| - \mathbb{I} \tag{V.2}$$

where $|s\rangle$ is some arbitrary state. This is indeed a reflection about the state $|s\rangle$. This is because any arbitrary state $|\psi\rangle$ can be written as $|\psi\rangle = \cos\alpha\,|s\rangle + \sin\alpha\,|s_\perp\rangle$ where $|s_\perp\rangle$ is orthogonal to

$|s\rangle$. Then we have

$$\begin{aligned} U_s|\psi\rangle &= U_s\left(\cos\alpha|s\rangle + \sin\alpha|s_\perp\rangle\right) \\ &= \left(2|s\rangle\langle s| - \mathbb{I}\right)\left(\cos\alpha|s\rangle + \sin\alpha|s_\perp\rangle\right) \\ &= \cos\alpha\left(2|s\rangle\langle s||s\rangle - |s\rangle\right) + \sin\alpha\left(2|s_\perp\rangle\langle s_\perp||s_\perp\rangle - |s_\perp\rangle\right) \\ &= \cos\alpha\left(2|s\rangle - |s\rangle\right) + \sin\alpha\left(-|s_\perp\rangle\right) \\ &= \cos\alpha|s\rangle - \sin\alpha|s_\perp\rangle \end{aligned} \tag{V.3}$$

and we can clearly see that this is a reflection about the $|s\rangle$ axis.

Note that we can write $|s\rangle$ as a sum of two components, one linear function of $|\omega\rangle$ and the other a linear function of a state $|s\prime\rangle$ orthogonal to $|\omega\rangle$. Thus

$$|s\rangle = \sin\theta|\omega\rangle + \cos\theta|s\prime\rangle \tag{V.4}$$

Each iteration will comprise U_sU_ω, i.e., reflection of $|s\rangle$ about $|s\prime\rangle$ followed by reflection about $|s\rangle$. This results in amplitude amplification.

C. The Method

The method of applying Grover's Search is quite simple.

1. Initialize $|s\rangle = \dfrac{|0\rangle + |1\rangle}{2}$.

2. Perform U_ω on the state to reflect component along $|\omega\rangle$, keeping components orthogonal to $|\omega\rangle$ intact.

3. Apply U_s on this state to reflect the state about $|s\rangle$

4. Repeat steps 2 and 3 till search is complete.

The above steps are illustrated in Now will we actually implement the oracle and the diffuser using quantum logic gates. First let us take a look at the oracle.

Implementation of the Oracle

The oracle is implemented using a phase kickback mechanism. Consider the CNOT gate in V.1. The CNOT gate acts as shown below.

$$\begin{aligned} CX\,|00\rangle &= |00\rangle \\ CX\,|01\rangle &= |01\rangle \\ CX\,|10\rangle &= |11\rangle \\ CX\,|11\rangle &= |10\rangle \end{aligned} \tag{V.5}$$

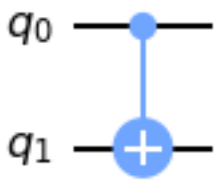

FIG. V.1. CNOT gate

Now, if we have our classical function f behaving as

$$\begin{aligned} f(\omega) &= 1 \\ f(s) &= 0 \quad \forall s \neq \omega \end{aligned} \tag{V.6}$$

Then we can set up an output qubit as

$$|out\rangle = |-\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

so that

$$CX\,|f(x)\ out\rangle = \begin{cases} |f(x)\ out\rangle & f(x) = 0 \\ -\,|f(x)\ out\rangle & f(x) = 1 \end{cases} \tag{V.7}$$

Thus we get our oracle. The oracle circuit is shown in V.2.

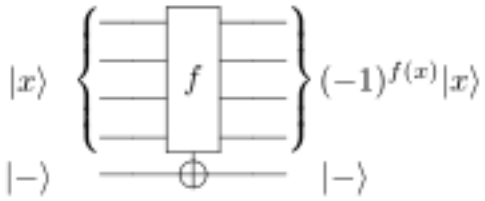

FIG. V.2. The Oracle

Implementation of the Diffuser

The diffuser has the equation as per equation V.3. To implement the diffuser on the state $|000\cdots0\rangle$, we just need to flip all qubits using X gates and then apply a multi-controlled Z-gate. Since we are starting with the state $|+++\cdots+\rangle$, we need to apply a H-gate in the beginning and at the end to got to $|000\cdots0\rangle$ and revert back. Figure V.3 shows the diffuser circuit for 8 qubits.

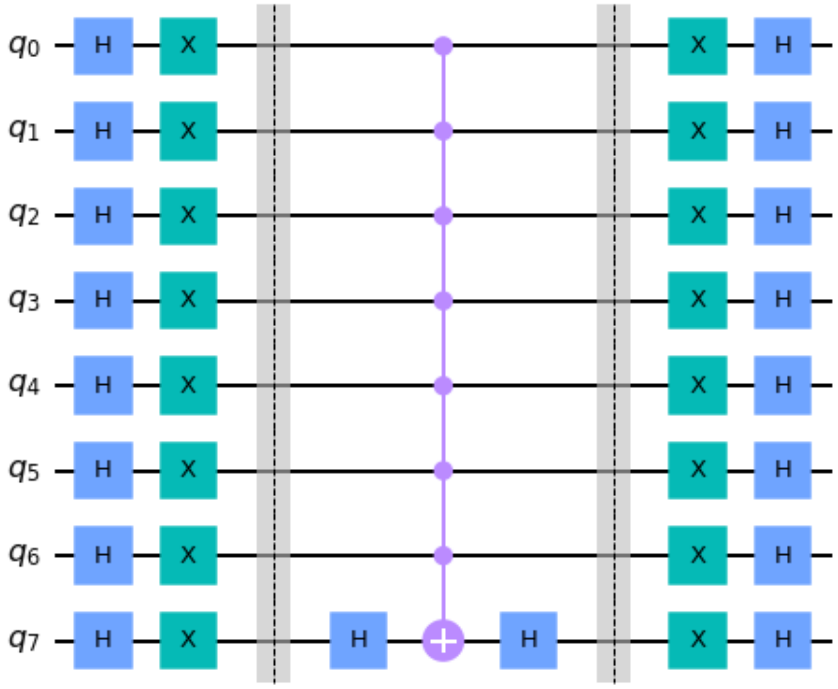

FIG. V.3. The Diffuser for 8 qubits

D. Number of Iterations

Let our register consist of n qubits. The number of pure states possible is then $2^n = N$. Consider the initial state of the system, where the system is initialized to $|+++\cdots+\rangle$. This is nothing but an equal superposition of the N pure states. Since $|\omega\rangle$ is one of these states and all states occur with equal probabilities, probability of finding $|\omega\rangle$ is $\frac{1}{N} = \frac{1}{2^n}$. Now, from equation V.4, the probability of measuring $|\omega\rangle$ is $\sin^2\theta$. Thus we have,

$$\begin{aligned} \sin^2\theta &= \frac{1}{2^n} \\ \Rightarrow \sin\theta &= \sqrt{\frac{1}{2^n}} \end{aligned} \tag{V.8}$$

At each iteration we reflect by 2θ. Thus, after k iterations, we arrive at angle $2k\theta$. For complete search, $2k\theta$ should be as close as possible to $\frac{\pi}{2}$ but less than that (to avoid overshoot). For small *theta*, $\sin\theta \approx \theta$. Thus, we have

$$\begin{aligned} 2k\theta &= \frac{\pi}{2} \\ \Rightarrow k\sqrt{\frac{1}{2^n}} &= \frac{\pi}{4} \\ \Rightarrow k &= \frac{\pi}{4}\sqrt{2^n} \\ \Rightarrow k &= \frac{\pi}{4}\sqrt{N} \end{aligned} \tag{V.9}$$

Thus, our complexity of search is $\mathcal{O}(\sqrt{N})$ as compared to $\mathcal{O}(N)$ for a classical brute force method. Further, if there are M solutions instead of one and we are interested in finding at least one solution, the complexity of Grover's algorithm is $\mathcal{O}\left(\sqrt{\frac{N}{M}}\right)$.

E. Generalized Grover Search

Generalized Grover search[11] dwells on the main Grover Search algorithm, except that it reduces the number of gates required by using suitable alternate unitary gates. This further increases the efficiency of the algorithm.

The original grover iterate takes the form $G = OAM_0A^\dagger$, where A is any unitary operator (we have used the Hadamard) and O is the oracle. The M_0 represents the mirroring circuit. M_0 has the form $M_0 = X^{\otimes n}M_1X^{\otimes n}$, where M_1 is the mirror flip of the last bit implemented using the multi-controlled Z-gate. Thus, we have $G = OAM_0A^\dagger = OAX^{\otimes n}M_1X^{\otimes n}A^\dagger$. Setting $B = AX^{\otimes n}$

gives $B^\dagger = X^{\otimes n} A^\dagger$ since $X^{\otimes n\dagger} = X^{\otimes n}$.We can then write $G = OBM_1B^\dagger$, where M_1 is a single gate and B avoids the use of $= X^{\otimes n}$, thereby reducing the total number of gates.

VI. OUR WORK

In this section, we shall present our work. The code for the same can be found on Git hub[1]. Our work essentially includes designing a suitable hash function and then cracking it using Generalized Grover Search algorithm. We are working on **8-bit hashes**. Note that we will use the **little-endian system** throughout, i.e., S_0 represents the Most Significant Bit and S_7 the Least Significant Bit.

A. Classical Hashing Algorithm

The hashing algorithm followed is the 8-bit Pearson Hash generation using 2 LFSRs. The taps for the first LFSR are at indices 3, 4, 5 and 7. The taps for the second LFSR are at indices 1, 2, 4 and 7. The diagrams for the same are presented in figures VI.1 and VI.2 respectively. Characters

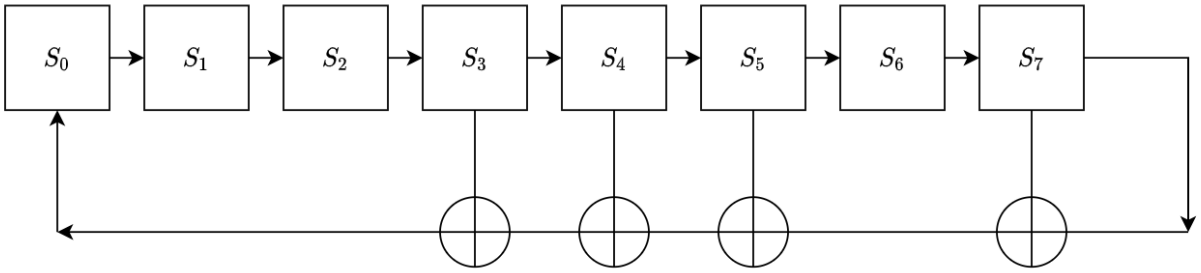

FIG. VI.1. The First LFSR

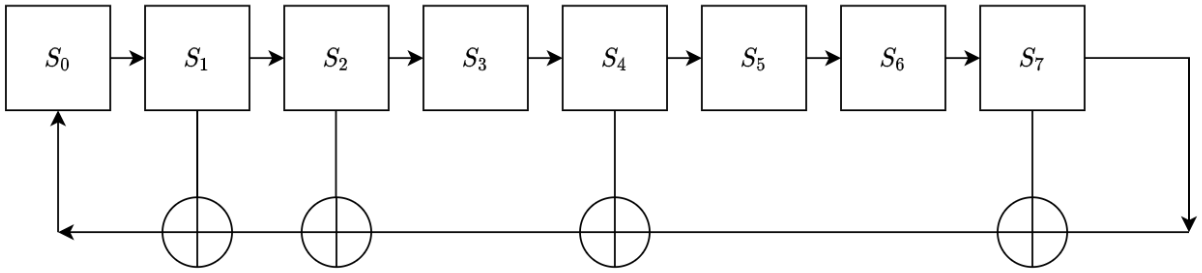

FIG. VI.2. The Second LFSR

are read from the message one at a time. The register is updates by taking its XOR with the ASCII of the character. The new value obtained is then passed through the first LFSR, followed by the second LFSR. The process is repeated for all characters till the end of the message. The code for the same is shown below.

[1] `https://github.com/Ankan-Mukherjee/NIUS.git`

```
def LFSR1_Classical(x):
    bit = ((x >> 0) ^ (x >> 2) ^ (x >> 3) ^ (x >> 4)) & 1
    x = ((x >> 1)|(bit<<7))%256;
    return x
def LFSR2_Classical(x):
    bit = ((x >> 0) ^ (x >> 3) ^ (x >> 5) ^ (x >> 6)) & 1
    x = ((x >> 1)|(bit<<7))%256;
    return x
def hash_Classical(message):
    x=0
    for i in message:
        x=x^ord(i)
        x=LFSR1_Classical(x)
        x=LFSR2_Classical(x)
    return x

message=input().rstrip()
print(hash_Classical(message))
```

Now we shall check the values of the hash for some sample strings. This can be done by running the code given above.

Message: `Hello World`

Hash: `15`

Making a slight change

Message: `Hello Workd`

Hash: `239`

We see that the hash changes significantly.

B. Quantum Hashing Algorithm

Now we will implement the same hashing algorithm on a quantum computer. This will make use of one quantum register comprising 8 qubits. The nonce itself will be stored on a register of 8 qubits. One qubit will be the output qubit that decides if a given hash is valid or not. Thus, our

circuit will make use of 17 qubits in total, along with some classical bits.

The Two LFSRs and Their Inverses

Let us first take a look at the two LFSR circuits, given in figures VI.3 and VI.4 respectively. These LFSRs perform the same function as the classical LFSRs, except that they do it on qubits.

For a quantum computer, it is imperative that after each iteration, the registers are restored to the original state for the next iteration to take place successfully. We need to design the circuits for inverting the LFSRs as well. These circuits are shown in figures VI.5 and VI.6 respectively.

The Hashing Operation

The hashing is performed in the following steps.

1. The classical algorithm is used to compute the hash till the end of the message block, just before the nonce.
2. The quantum hash register of 8 qubits is initialized with the hash generated.
3. The nonce is XORed with the hash register using CX gates.
4. The first LFSR with taps at 3, 4, 5 and 7 is operated once on the hash register.
5. The second LFSR with taps at 1, 2, 4 and 7 is operated once on the hash register.

The circuit for the entire hashing operator is shown in figure VI.7.

The Oracle

It is now time to put everything together. We shall assume that a valid nonce is one that starts with 5 zeroes. For this, we need to check if the registers at indices 0, 1, 2, 3 and 4 are $|0\rangle$. A multi-controlled Toffoli gate from these register qubits to the output will flip the qubits of the output if and only if all of the 5 qubits were $|1\rangle$. Further, if the output is initialized to $|out\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, we will get the output to flip sign only when all of the 5 qubits are $|1\rangle$ or else output stays the same. Since we are interested in checking if all the 5 qubits are $|0\rangle$, we must use X gates on them before passing them through the multi-controlled Toffoli gate. After the check, we must restore the registers by inverting the operations applied. This invovles taking an X gate on qubits 0, 1,

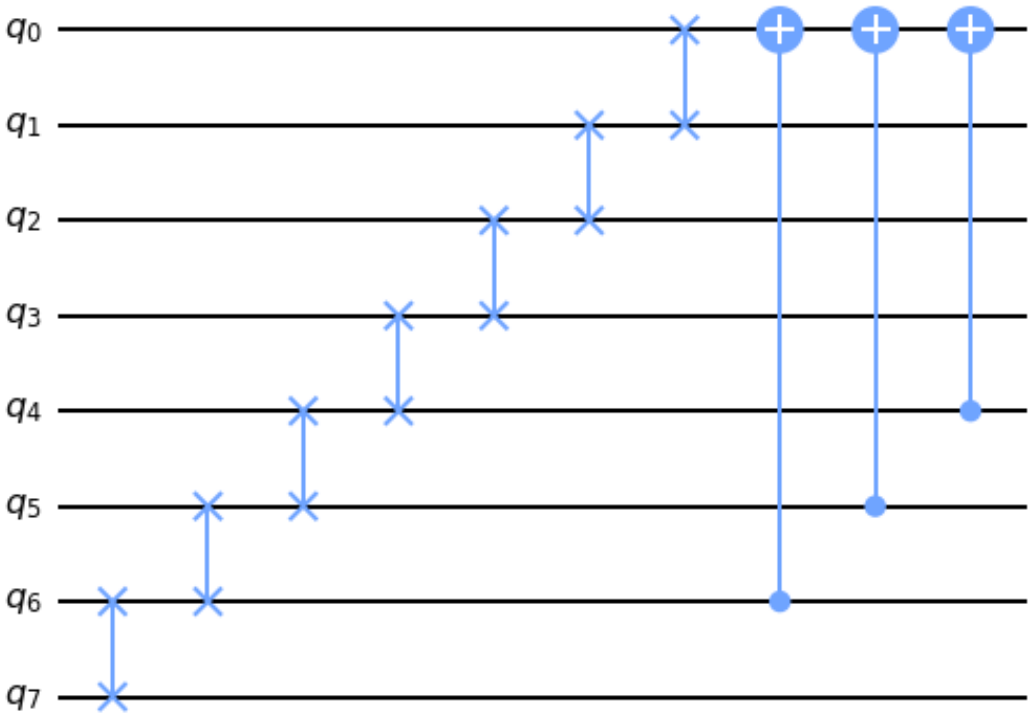

FIG. VI.3. The First LFSR

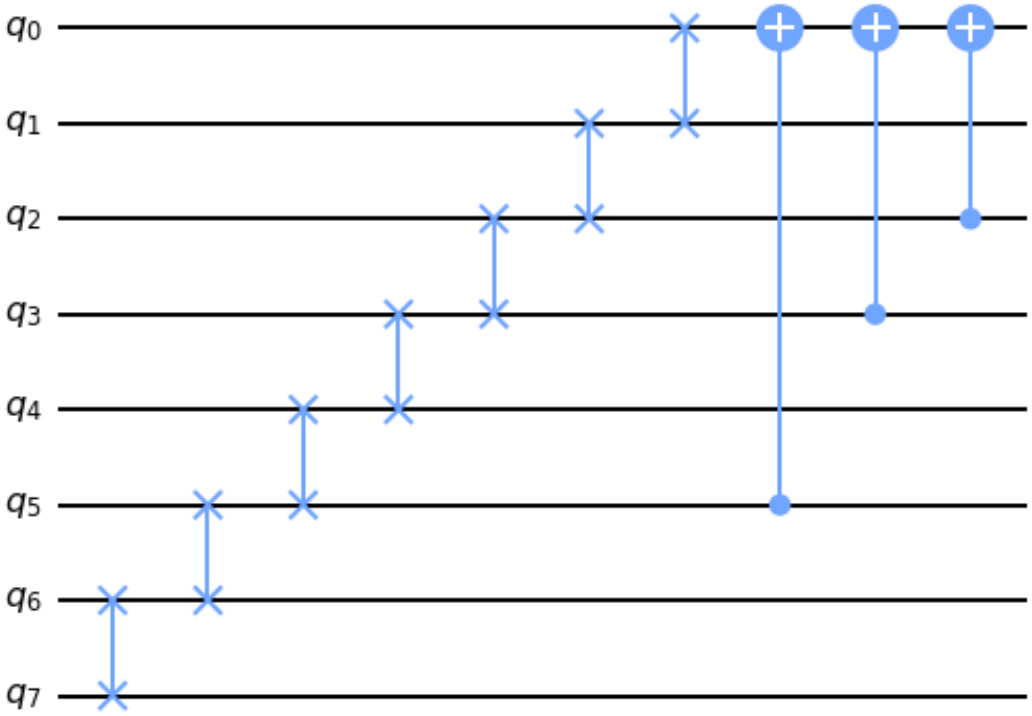

FIG. VI.4. The Second LFSR

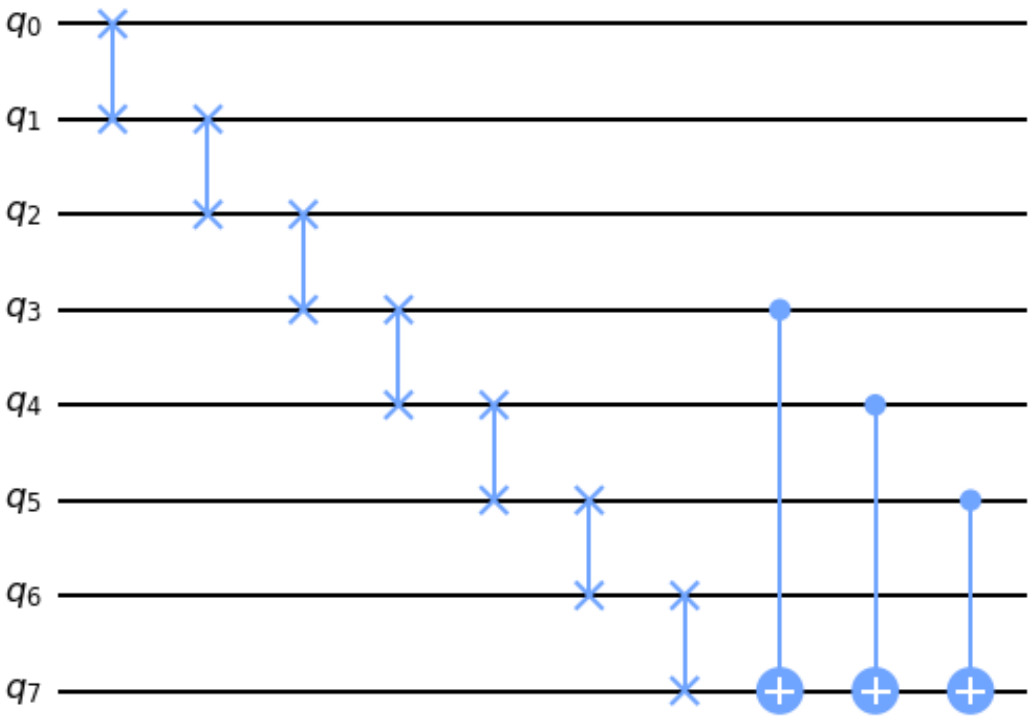

FIG. VI.5. Inverse of the First LFSR

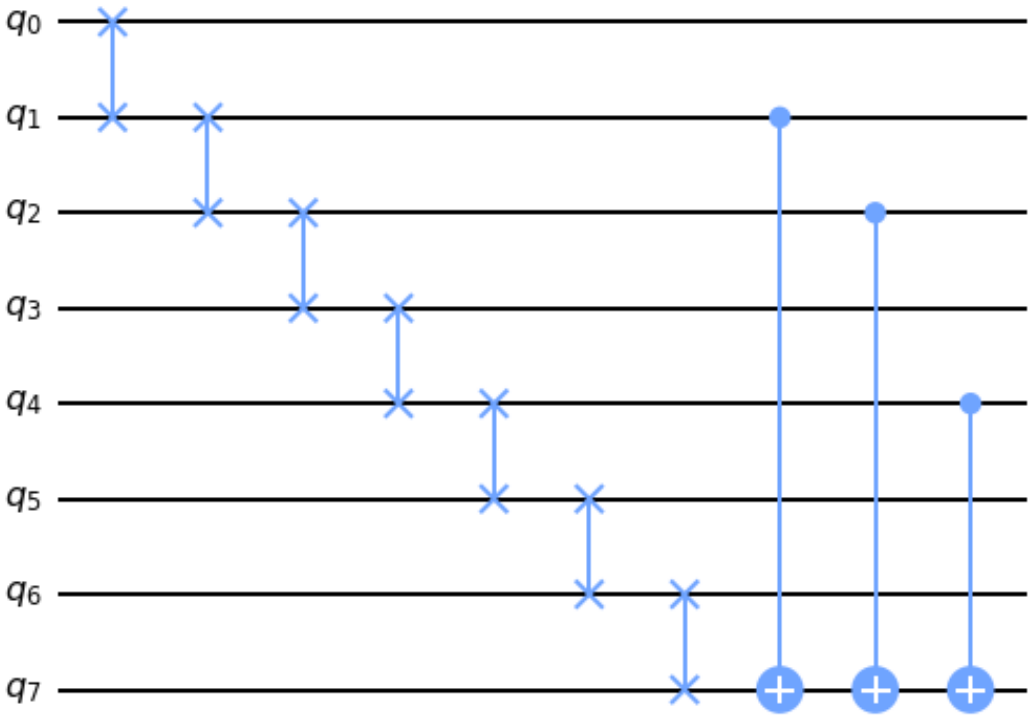

FIG. VI.6. Inverse of the Second LFSR

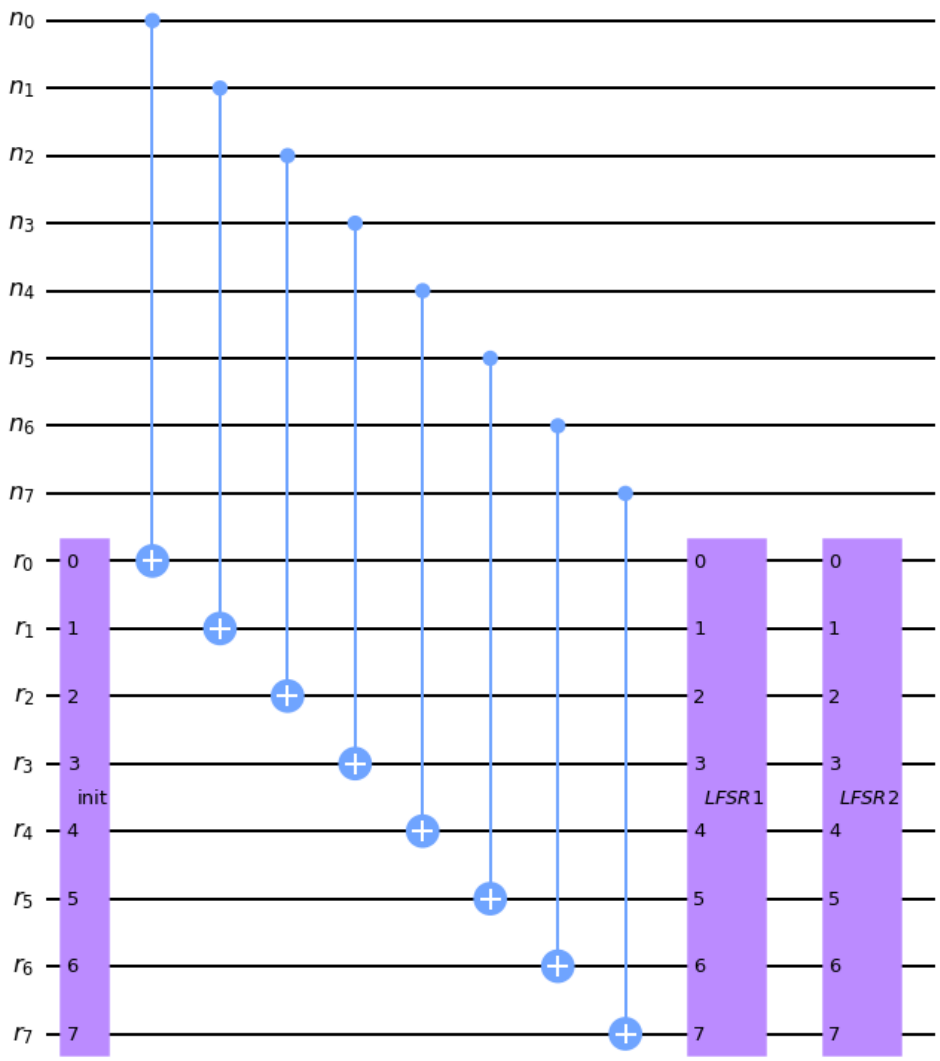

FIG. VI.7. Hashing Circuit

2, 3 and 4, followed by the inverse of the second LFSR, followed by the inverse of the first LFSR. Figure VI.8 shows the complete oracle circuit.

C. Searching the Nonce

Grover Search

The grover search involves setting up the nonce to a superposition of all states using a H gate on all the qubits followed by the repeated application of the oracle followed by the diffuser. The diffuser used has been discussed in the section preceding figure V.3. The number of iterations

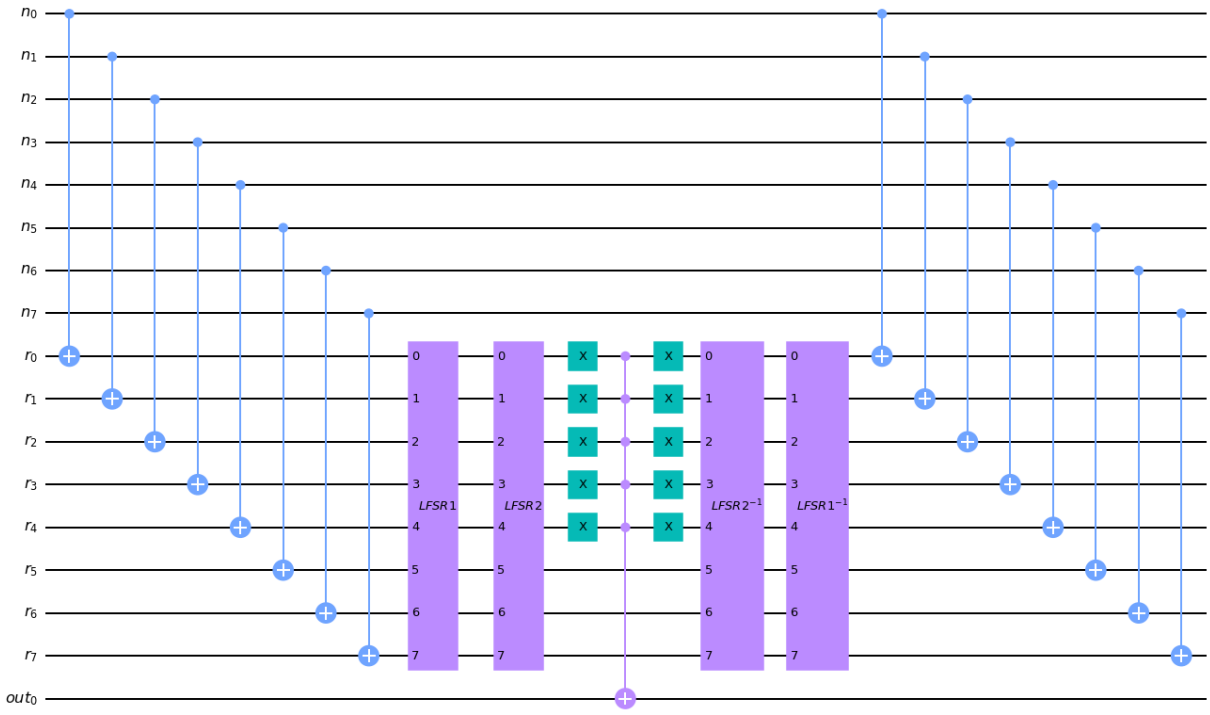

FIG. VI.8. Circuit for the Oracle

required is given by equation V.9, where, we now have $M = 8$ solutions instead of 1. Thus, number of iterations, k, is

$$k = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor = \left\lfloor \frac{\pi}{4}\sqrt{\frac{256}{8}} \right\rfloor = 4 \tag{VI.1}$$

Finally, we perform a measurement of the nonce. Figure VI.9 shows the entire circuit.

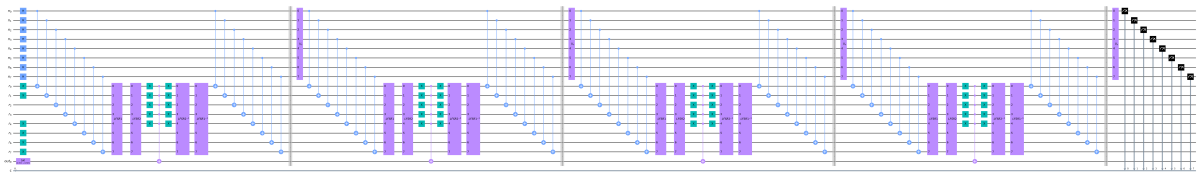

FIG. VI.9. Grover Search Circuit

Generalized Grover Search

Here, we replace the H gate followed by X gate by a single unitary gate. $R_y\left(\frac{\pi}{2}\right)$ is a suitable unitary transformation substitute for HX. Its inverse is $R_y\left(-\frac{\pi}{2}\right)$. We can then simplify our

diffuser to the one given in figure VI.10 thereby reducing 16 gates per iteration. This reduction in

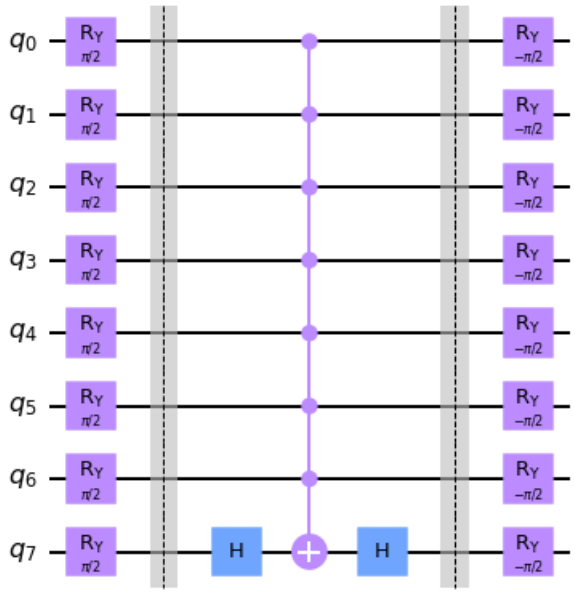

FIG. VI.10. Generalised Grover Diffuser

the number of gates is very helpful. We will do an analysis of the same in the next section.

VII. RESULTS

In this section, we shall see the results obtained after performing the Grover Search. Since we are using the **little-endian** system, the output qubits obtained must be read from right to left to get the ASCII value of the nonce-character. We will then append the nonce to the message and check if its classical hash indeed starts with 5 zeroes when written in binary.

Number of Gates

First we observe the difference in the number of gates used in the Grover and the Generalized Grover Search algorithms. To count the gates, we split them as follows

Each LFSR (or LFSR inverse) has
7 $SWAP$ gates
3 CX gates

Each Diffuser has
18 H gates
16 X gates
1 MCT gate

Each Generalized Diffuser has
16 R_y gates
2 H gates
1 MCT gate

Each iteration has
2 LFSRs
2 Inverse LFSRs
1 Diffuser (or Generalized Diffuser)
16 CX gates
10 X gates
1 MCT gate

There are 8 H gates at the start followed by 4 iterations. Thus the total number of gates can be summarized by table I.

SUMMARY OF THE NUMBER OF GATES USED							
Algorithm	**H**	**X**	**CX**	**SWAP**	**MCT**	**R_y**	**TOTAL**
Grover Search	80	104	112	112	8	0	416
Generalized Grover Search	16	40	112	112	8	64	352

TABLE I. Table summarizing the number of gates required

We observe that the Generalized Grover Search algorithm uses significantly less number of gates.

Qiskit Simulation

Here, we will use the **aer_simulator** provided by qiskit to run our code. For testing purposes our message is

Message: `Hello World`

This is then passed on to our program. A simulation of 1024 measurements is done. The result is shown in figure VII.1. Note that since all since we are using the **little-endian** system, output must be read from right to left. Converting the binary to decimal, we get the ASCII of the nonce to be appended as

```
28
3
21
25
15
6
10
16
```

We append the nonce and test the output hashes. The output hashes are (in the same order as the nonce values)

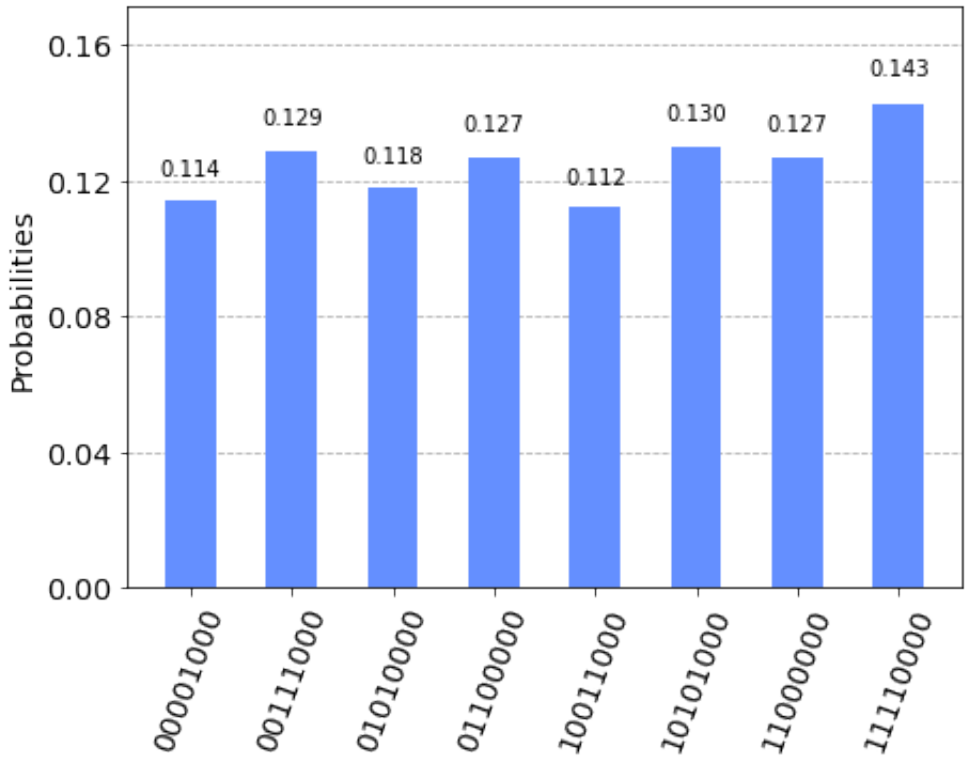

FIG. VII.1. Nonce values obtained and their probabilities

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

Thus, we conclude that our algorithm works successfully.

VIII. FUTURE WORK TO BE DONE

This section highlights the work left to be done in the subsequent interactions.

A. Testing on Real Quantum Hardware

So far all the results obtained are the outputs of simulations of the quantum circuits on a classical computer. The next phase will deal with actually using an IBM quantum system to execute the circuit. The circuit is quite heavy (17 qubits) and requires significant amount of quantum computing resources to execute. We will figure this out and check the probability distributions from a real quantum computer[12].

B. Developing a Secure Blockchain Using Entanglement

We will use the Bell's Measure and the CHSH inequality to develop a secure blockchain[13][14] (See VIII C).

C. Quantum Hashing

We will develop some novel hashing algorithms that are purely quantum mechanical and cannot be implemented on a classical computer.

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"

[2] V. M. et. al., "The impact of quantum computing on present cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018.

[3] A. L. Selvakumar and C. S. Ganadhas, "The evaluation report of sha-256 crypt analysis hash function," in *2009 International Conference on Communication Software and Networks*, pp. 588–592, 2009.

[4] "Blockchain technology basics." `https://www.spheregen.com/blockchain-technology-basics/`. Accessed: 2021-09-10.

[5] R. R. A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems,"

[6] P. K. Pearson, "Fast hashing of variablelength text strings,"

[7] H. Krawczyk, "Lfsr-based hashing and authentication," in *Advances in Cryptology — CRYPTO '94* (Y. G. Desmedt, ed.), (Berlin, Heidelberg), pp. 129–139, Springer Berlin Heidelberg, 1994.

[8] R. Khalaf and A. Abdullah, "Generate quantum key by using quantum shift register," *International Journal of Computer Networks and Communications Security*, vol. 3, pp. 248–252, 06 2015.

[9] R. Shankar, *Principles of quantum mechanics*. New York, NY: Plenum, 2 ed., 1980.

[10] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, (New York, NY, USA), p. 212–219, Association for Computing Machinery, 1996.

[11] A. Gilliam, M. Pistoia, and C. Gonciulea, "Optimizing quantum search using a generalized version of grover's algorithm," 2020.

[12] "Ibm quantum computing systems." `https://www.ibm.com/quantum-computing/systems/`. Accessed: 2021-09-10.

[13] D. Rajan and M. Visser, "Quantum blockchain using entanglement in time," *Quantum Reports*, vol. 1, no. 1, pp. 3–11, 2019.

[14] K. Sarkar, B. Behera, and P. Panigrahi, "A robust tripartite quantum key distribution using mutually shared bell states and classical hash values using a complete-graph network architecture," 05 2019.

[15] Smite-Meister, "Bloch sphere." `https://creativecommons.org/licenses/by-sa/3.0`. Accessed: 2021-09-10.

[16] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Phys. Rev.*, vol. 47, pp. 777–780, May 1935.

[17] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov 1964.

[18] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969.

APPENDIX A: FIELD THEORY AND LFSR

We start with group theory. A group is a set of elements G with a binary operator $\oplus$ satisfying the following axioms:

1. Closure: $a \oplus b \in G \ \forall a, b \in G$.
2. Associativity: $\forall a, b, c \in G,\ a \oplus (b \oplus c) = (a \oplus b) \oplus c$.
3. Existence of identity: $\exists e \in G :\ \forall a \in G, e \oplus a = a \oplus e = a$.
4. Existence of Inverse: $\forall a \in G\ \exists b \in G :\ a \oplus b = e$.

A group is said to be Abelian if it is commutative, i.e., $a \oplus b = b \oplus a\ \forall a, b \in G$.
We will now define a field. A field $\mathbb{F}$ is a set of atleast two elements, with two operations, $\oplus$ and $\otimes$ such that the following conditions hold:

1. Addition axioms: $\mathbb{F}$ forms an Abelian group under $\oplus$ with identity 0.
2. Multiplication axioms: $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ forms an Abelian group under $\otimes$ with identity 1.
3. Distributive Law: $\forall a, b, c \in G,\ a \otimes (b \oplus c) = (a \otimes b) \oplus c$.

A field is called a finite field or a Galois field if and only if it has finitely many elements. An example of such a field is the residue class modulo a prime p given as $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ under $\oplus$ = addition mod p and $\otimes$ = multiplication mod p. Note that the residue classes of composite numbers do not form a field since they contain non zero elements that do not have an inverse. One such example is the residue class of 6, which contains 2 which has no inverse.
The field $\mathbb{F}_{p^k}$ is defined as the set of polynomials $P(x)$ of degree $k-1$ whose coefficients are taken modulo p. The operators are deined as $\oplus$ = usual polynomial addition with coeffecients mod p and $\otimes$ = usual polynomial multiplication with coeffecients mod p modulo another polynomial $Q(x)$ of degree k. To ensure that $\mathbb{F}_{p^k}$ is indeed a field, $Q(x)$ must not be factorizable into polynomials of degree lower than k, otherwise elements in $\mathbb{F}_{p^k}$ may not have an inverse. Such $Q(x)$ which are non factorizable are called **primitive polynomials**.

An LFSR of n bits can be represented using $\mathbb{F}_{2^k}$. The coefficient of each polynomial can thus be only 0 or 1, which represents the state of that bit. Shifting registers is like multiplying the polynomial by x and using taps is choosing the $Q(x)$. We have chosen taps at 3, 4, 5 and 7 for the first LFSR and at 1, 2, 4 and 7 for the second register. Since we are using the little endian system,

the corresponding polynomials are $1+x^3+x^5+x^6$ and $1+x^2+x^3+x^4$ respectively, both of which are primitive.

APPENDIX B: PAULI MATRICES AND BLOCH SPHERE

The most common operator used when it comes to requiring two eigenstates is the spin operator. The Pauli matrices form the basis for the spin operators. Here we discuss them in some more detail.

We start with the representation of a single qubit in the $|0\rangle$, $|1\rangle$ basis. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. Thus, the state can be represented as $|\psi\rangle = \binom{\alpha}{\beta}$. Now we can write $|\alpha| = \cos\left(\frac{\theta}{2}\right)$ and $|\beta| = \sin\left(\frac{\theta}{2}\right)$. The factor of half is a matter of convention. This means $\alpha = \cos\left(\frac{\theta}{2}\right)e^{\iota\phi_1}$ and $\beta = \sin\left(\frac{\theta}{2}\right)e^{\iota\phi_2}$. Since global phase does not affect observables of the system, we can factor out ϕ_1 and set $\phi_2 - \phi_1 = \phi$ so that $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = \sin\left(\frac{\theta}{2}\right)e^{\iota\phi}$. Thus, we can use two angular parameters, θ and ϕ to represent a state uniquely. These two parameters correspond to a point on a unit sphere. This sphere is called the bloch sphere, as is shown in figure VIII.1. Note that $\theta = 0$ corresponds to $|0\rangle$ and $\theta = \pi$ corresponds to $|1\rangle$.

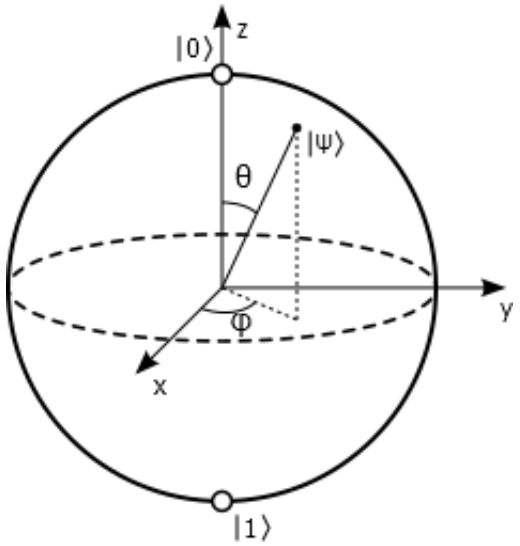

FIG. VIII.1. Bloch Sphere[15]

Now we note that the density matrix of a state $|\psi\rangle$ in quantum mechanics can be given by

$|\psi\rangle\langle\psi|$. Thus, we write

$$\begin{aligned}\rho = |\psi\rangle \otimes \langle\psi| &= \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{\iota\phi}\sin\left(\frac{\theta}{2}\right)\end{pmatrix} \otimes \begin{pmatrix}\cos\left(\frac{\theta}{2}\right) & e^{-\iota\phi}\sin\left(\frac{\theta}{2}\right)\end{pmatrix} \\ &= \begin{pmatrix} \cos^2\left(\frac{\theta}{2}\right) & e^{-\iota\phi}\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right) \\ e^{\iota\phi}\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right) & \sin^2\left(\frac{\theta}{2}\right)\end{pmatrix} \\ &= \begin{pmatrix} 1+\cos\theta & \cos\phi\sin\theta - \iota\sin\phi\sin\theta \\ \cos\phi\sin\theta + \iota\sin\phi\sin\theta & 1-\cos\theta\end{pmatrix} \\ &= \frac{1}{2}\left(\mathbb{I} + \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\sin\theta\cos\phi + \begin{pmatrix}0 & -\iota\\ \iota & 0\end{pmatrix}\sin\theta\sin\phi + \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\cos\theta\right)\end{aligned} \tag{VIII.1}$$

Now note that a unit vector on the sphere can be written, in spherical polar coordinates as $\hat{\mathbf{n}} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$. If we write $\sigma = (\sigma_x, \sigma_x, \sigma_z)$, with

$$\begin{aligned}\sigma_x &= \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \\ \sigma_y &= \begin{pmatrix}0 & -\iota\\ \iota & 0\end{pmatrix} \\ \sigma_z &= \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\end{aligned} \tag{VIII.2}$$

then we can modify equation VIII.1 to

$$\rho = \frac{1}{2}\left(\mathbb{I} + \hat{\mathbf{n}}.\sigma\right)$$

The 3 matrices in VIII.2 are the Pauli matrices, which are used as gates. These matrices have some interesting properties which makes solving problems easier using them, but they are not very relevant to our work and hence, we shall not discuss them here. They can be looked up from any standard textbook on quantum mechanics[9].

APPENDIX C: BELL'S MEASURE AND THE EPR PARADOX

Before talking about the bell's measure let us first dive into why it was made and for this we must look at the EPR experiment[16]. We will discuss Bohm's variant since Bell's response was

made in a way to that. Say we have prepared a electron-positron pair coming from a single source. These would be entangled in a way where if we measure the spin of one of the particles, the other particle will simultaneously collapse to the opposite spin.

$$|\psi\rangle = \frac{|\uparrow_e\downarrow_p\rangle + |\downarrow_e\uparrow_p\rangle}{\sqrt{2}}$$

So the main issue which Einstein had was that this means that measurement on one particle directly affects the other no matter how far it is. This makes it a non local effect which clearly does not make sense in a world which was believed to follow local realism. It can be proven that the two agents have no way to communicate using this pair hence showing that there actually is no faster than light communication. While one may think choosing basis in a certain manner can change measurement probabilities and essentially have some "information" change, no matter how much measurements are done, since this is probabilistic the other agent cannot conclude anything from that.

While there have been multiple responses to this, the most important one is the one discussed in Bell's paper [17]. First we will start by considering the EPR argument using spin particles. Consider a pair of spin one-half particles formed somehow in the singlet spin state and moving freely in opposite directions. Measurements can be made, say by Stern-Gerlach magnets, on selected components of the spins $\vec{\sigma_1}$ and $\vec{\sigma_2}$, If measurement of the component $\vec{\sigma_1} \cdot a$, where a is some unit vector, yields the value $+1$ then, according to quantum mechanics, measurement of $\vec{\sigma_2} \cdot a$ must yield the value -1 and vice versa. We now define some set of parameters λ which is taken as continuous which give us a complete description of the state. The result A of measuring $\vec{\sigma_1} \cdot a$ is then determined by a and λ, and the result B of measuring $\vec{\sigma_2} \cdot b$ in the same instance is determined by b and λ.

$$A(\vec{a}, \lambda) = \pm 1, B(\vec{b}, \lambda) = \pm 1 \tag{VIII.3}$$

We now take $\rho(\lambda)$ as the probability distribution of λ and we will now try to find the expectation value of of the product of the two components $\vec{\sigma_1} \cdot a$ and $\vec{\sigma_2} \cdot b$.

$$P(\vec{a}\vec{b}) = \int d\lambda \rho(\lambda) A(\vec{a}, \lambda) B(\vec{b}, \lambda) \tag{VIII.4}$$

The quantum mechanical expectation value of this is the following

$$\langle \vec{\sigma_1} \cdot a\vec{\sigma_2} \cdot b \rangle = -\vec{a} \cdot \vec{b} \tag{VIII.5}$$

However it turns out that equation VIII.4 doesn't give us the same result as VIII.5. So first off we know that we have a normalized distribution.

$$\int d\lambda \rho(\lambda) = 1 \tag{VIII.6}$$

if we take $\vec{a} = \vec{b}$ the P in equation VIII.4 can reach -1.

$$A(\vec{a}, \lambda) = -B(\vec{a}, \lambda) \tag{VIII.7}$$

Knowing this we can rewrite equation VIII.4 into the following

$$P(\vec{a}\vec{b}) = -\int d\lambda \rho(\lambda) A(\vec{a}, \lambda) A(\vec{b}, \lambda) \tag{VIII.8}$$

$$P(\vec{a}, \vec{b}) - P(\vec{a}, \vec{c}) = \int d\lambda \rho(\lambda)[1 - A(\vec{b}, \lambda) A(\vec{c}, \lambda)] \tag{VIII.9}$$

from equation VIII.3 we can write this

$$|P(\vec{a}, \vec{b}) - P(\vec{a}, \vec{c})| \leq \int d\lambda \rho(\lambda) A(\vec{a}, \lambda) A(\vec{b}, \lambda)[A(\vec{b}, \lambda) A(\vec{c}, \lambda) - 1] \tag{VIII.10}$$

The second term on the right is just $P(\vec{b}, \vec{c})$ so we get

$$1 + P(\vec{b}, \vec{c}) \geq |P(\vec{a}, \vec{b}) - P(\vec{a}, \vec{c})| \tag{VIII.11}$$

Now we define a $\overline{P}(\vec{a}, \vec{b})$ and a $\overline{-\vec{a} \cdot \vec{b}}$ which essentially are the averages over vectors differing from a small angle from $\vec{a}$ and $\vec{b}$ of the quantities under the bar. Let's suppose the following holds for some ϵ

$$|\overline{P}(\vec{a}, \vec{b}) + \overline{\vec{a} \cdot \vec{b}}| \leq \epsilon \tag{VIII.12}$$

We cannot make ϵ arbitrarily small and this can be proven by the following steps. Let us first

assume the following inequality holds for all $\vec{a}$ and $\vec{b}$

$$|\overline{\vec{a}\cdot\vec{b}} - \vec{a}\cdot\vec{b}| \leq \delta \tag{VIII.13}$$

Then using equation VIII.13 and equation VIII.12 we have

$$|\overline{P}(\vec{a},\vec{b}) + \vec{a}\cdot\vec{b}| \leq \epsilon + \delta \tag{VIII.14}$$

Now taking $\vec{a} = \vec{b}$ (hence their dot product is 1) we rewrite equation VIII.14 as the equation below while using the fact that $\overline{P(\vec{a},\vec{b})} = \int d\lambda\rho(\lambda)\overline{A}(\vec{a},\lambda)\overline{B}(\vec{b},\lambda))$.

$$\int d\lambda\rho(\lambda)[\overline{A}(\vec{b},\lambda)\overline{B}(\vec{b},\lambda)) + 1] \leq \epsilon + \delta \tag{VIII.15}$$

We can extend from VIII.3 that on averaging over a small range, $|\overline{A}(\vec{a},\lambda)| \leq 1$ and $|\overline{B}(\vec{b},\lambda)| \leq 1$. Now we can write the following

$$\overline{P}(\vec{a},\vec{b}) - \overline{P}(\vec{b},\vec{c}) = \int d\lambda\rho(\lambda)\overline{A}(\vec{a},\lambda)\overline{B}(\vec{b},\lambda)[\overline{A}(\vec{b},\lambda)\overline{B}(\vec{c},\lambda)+1] - \int d\lambda\rho(\lambda)\overline{A}(\vec{a},\lambda)\overline{B}(\vec{c},\lambda)[\overline{A}(\vec{b},\lambda)\overline{B}(\vec{b},\lambda)+1] \tag{VIII.16}$$

Using the inequalities on the averaged A and B we can write the following

$$|\overline{P}(\vec{a},\vec{b}) - \overline{P}(\vec{b},\vec{c})| \leq \int d\lambda\rho(\lambda)[\overline{A}(\vec{b},\lambda)\overline{B}(\vec{c},\lambda) + 1] - \int d\lambda\rho(\lambda)[\overline{A}(\vec{b},\lambda)\overline{B}(\vec{b},\lambda) + 1] \tag{VIII.17}$$

$$|\overline{P}(\vec{a},\vec{b}) - \overline{P}(\vec{b},\vec{c})| \leq 1 + \overline{P} + \epsilon + \delta \tag{VIII.18}$$

We write equation VIII.18 using equation VIII.17 and equation VIII.15. Finally using equation VIII.14 we rewrite the above equation as

$$|\vec{a}\cdot\vec{c} - \vec{a}\cdot\vec{b}| + \vec{b}\cdot\vec{c} - 1 \leq 4(\epsilon + \delta) \tag{VIII.19}$$

Now with the constraint coming from equation VIII.19 we can hand-pick values of $\vec{a},\vec{b},\vec{c}$ such that ϵ cannot be made arbitrarily small (take $\vec{a}\cdot\vec{b} = \vec{c}\cdot\vec{b} = 1/\sqrt{2}$ and $\vec{a}\cdot\vec{c} = 0$ this would show $4(\epsilon+\delta) \geq \sqrt{2} - 1$). The fact that ϵ cannot be made arbitrarily small implies that the quantum mechanical value cannot be approximated either accurately or arbitrarily close to this form using hidden variable. So this contradiction implies that some assumptions that we have taken happen

to not work together and that happen to be local determinism and hidden variables. So any hidden variable theory by nature itself is non local.

To get the form of the CSHS inequalities we essentially modify the form of equation VIII.16 and write it as follows

$$\overline{P}(\vec{a},\vec{b})-\overline{P}(\vec{a},\vec{b'}) = \int d\lambda\rho(\lambda)\overline{A}(\vec{a},\lambda)\overline{B}(\vec{b},\lambda)[1\pm\overline{A}(\vec{a'},\lambda)\overline{B}(\vec{b'},\lambda)]-\int d\lambda\rho(\lambda)\overline{A}(\vec{a},\lambda)\overline{B}(\vec{b'},\lambda)[1\pm\overline{A}(\vec{a'},\lambda)\overline{B}(\vec{b},\lambda)] \tag{VIII.20}$$

We now apply the triangle inequality and also note that the modulus of the averaged functions $\overline{A}$ and $\overline{B}$ are bounded above by 1 we will get

$$|\overline{P}(\vec{a},\vec{b}) - \overline{P}(\vec{a},\vec{b'})| \leq \left|\int d\lambda\rho(\lambda)[1 \pm \overline{A}(\vec{a'},\lambda)\overline{B}(\vec{b'},\lambda)]\right| + \left|\int d\lambda\rho(\lambda)[1 \pm \overline{A}(\vec{a'},\lambda)\overline{B}(\vec{b},\lambda)]\right| \tag{VIII.21}$$

We may as well remove the moduli brackets on the LHS since the quantities is non negative. Since $\int \rho(\lambda)d\lambda = 1$ and $\overline{P(\vec{a},\vec{b})} = \int d\lambda\rho(\lambda)\overline{A}(\vec{a},\lambda)\overline{B}(\vec{b},\lambda))$ we can rewrite equation VIII.21 as

$$|\overline{P}(\vec{a},\vec{b}) - \overline{P}(\vec{a},\vec{b'})| \leq 2 \pm (\overline{P}(\vec{a'},\vec{b'}) + \overline{P}(\vec{a'},\vec{b})) \leq 2 \pm |\overline{P}(\vec{a'},\vec{b'}) + \overline{P}(\vec{a'},\vec{b})| \tag{VIII.22}$$

The second inequality comes from the triangle inequality. Now we can choose the minus sign and we get

$$|\overline{P}(\vec{a},\vec{b}) - \overline{P}(\vec{a},\vec{b'})| + |\overline{P}(\vec{a'},\vec{b'}) + \overline{P}(\vec{a'},\vec{b})| \leq 2 \tag{VIII.23}$$

Finally we get the following equation by applying the triangle inequality on RHS of equation VIII.23

$$|\overline{P}(\vec{a},\vec{b}) - \overline{P}(\vec{a},\vec{b'}) + \overline{P}(\vec{a'},\vec{b'}) + \overline{P}(\vec{a'},\vec{b})| \leq 2 \tag{VIII.24}$$

The above inequality is the form of writing the CHSH inequalities [18]. The bound above is shown to be 2 which is satisfied for classical systems and is violated for quantum mechanical correlations. One can instead prove a different bound for quantum correlations as $2\sqrt{2}$. This is referred to as the Tsirelon's bound. To prove this we can suppose we have four hermitian operators A_0, A_1, B_0, B_1 where $[A_i, B_j] = 0$ but the $[A_0, A_1] \neq 0$ and $[B_0, B_1] \neq 0$. We define these A operators as being two different spin measurements on the same electron and B being the same on the positron where their results are either $+1$ or -1. We know that for a simple spin system $[\sigma\cdot\vec{a}, \sigma\cdot\vec{b}] = 2\iota\sigma\cdot(\vec{a}\times\vec{b})$.

Now we will define a new operator called $\mathcal{B}$

$$\mathcal{B} = A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1$$

This operator has been defined along the lines of the bell's measure where expectation value of the modulus of this operator would be the actual bells measure for a correlation function of $C_{ij} = \langle A_iB_j \rangle$. We can now square this operator and it would simpify as the equation below (since $A_i^2 = B_i^2 = I$)

$$\mathcal{B}^2 = 4I - [A_0, A_1][B_0, B_1]$$

Since these are spin operators we have $|[A_0, A_1][B_0, B_1]| \leq 4I$ using the commutation relation we had defined earlier. We would in fact have $\mathcal{B}^2$ reach it's maximum if A_0, B_0 measures along $\hat{x}$ and A_1, B_1 measures along $\hat{y}$ which would make $\mathcal{B}^2 = 8I$. This leads us to $\langle \mathcal{B} \rangle \leq 2\sqrt{2}$ which is the Tsirelon's bound.