Quantum Information and Quantum Cryptography: An Introductory Overview

Arpita Maitra

Indian Institute of Technology Kharagpur
[arpita76b@gmail.com]

18th June, 2018

Outline of the talk

- Preliminaries of Quantum Paradigm
  - What is a Qubit?
  - Entanglement
  - Quantum Gates
  - No Cloning
  - Indistinguishability of quantum states
- Quantum Key Exchange Protocol: BB84
  - Basic idea
  - Some Eavesdropping Strategies
  - State of the art: News and Industries

Introduction

- Basic model of classical computers: initially visualized by Alan Turing, Von Neumann and several other researchers in 1930's.
- Limited by classical physics and thus termed as classical computers
- In 1982: Richard Feynman presented the seminal idea of a universal quantum simulator or more informally, a quantum computer

Introduction (contd.)

- A quantum system of more than one particles: dimension is exponentially large in the number of particles
- A quantum system can efficiently solve a problem that may require exponential time on a classical computer
- 1980's: Deutsch-Jozsa and Grover's algorithms
- 1994: Shor, Factorization and Discrete Log Problems can be efficiently solved in quantum paradigm
- Major impact in Classical Cryptography

Introduction (contd.)

- While commercial quantum computers are still elusive(?), the recent developments in the area of experimental physics are gaining momentum
- Award of Nobel prize for Physics in 2012 to Wineland and Haroche for "ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems"
- The Nobel prize in Physics, 2016, is awarded to Thouless, Haldane and Kosterlitz for "theoretical discoveries of topological phase transitions and topological phases of matter"
- These works might have importance towards actual implementation of a quantum computer

NSA Statement

In August, 2015 the U.S. National Security Agency (NSA) released a major policy statement on the need for post-quantum cryptography (PQC)

National Security Agency, Cryptography today, August 2015, archived on 23 November 2015, `tinyurl.com/SuiteB`

"For those partners and vendors that have not yet made the transition to Suite B algorithms (Eliptic curve cryptography), we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition...."

NSA Statement (Cond.)

This announcement clearly states the following points.

- People who had not yet upgraded from RSA to ECC should not do so
- People should be ready for the future upgrades to post-quantum protocols

These are the signals of the following fact.....

Practical quantum computers might not be a distant dream

Quantum Cryptology: Motivation

- The pioneering developments in the domain of Classical cryptography in 1970's are:
  - Diffie-Hellman Key Exchange and
  - RSA (Rivest-Shamir-Adleman) Public Key Cryptosystem.
  - Elliptic Curve Cryptosystem is also extremely popular now.
- Diffie-Hellman Key Exchange: based on Discret Log Problem
- RSA (Rivest-Shamir-Adleman) Public Key Cryptosystem: based on factorization of a large number
- Security would be compromised in post quantum era

Solutions

- Lattice based and Code based Cryptosystems:
  - considerable Research
  - not as efficient as RSA/ECC,
  - may be used shortly in commercial domain in case quantum computers arrive
- Alternative solution: Quantum Crytography
- Warrants the security against quantum adversary; adversary with a unbounded power of computation

Preliminaries: Qubit and Its Different Representation

- Bit (0 or 1): basic element of a classical computer
- The quantum bit (called the qubit): the main mathematical object in the quantum paradigm (physical counterpart is a photon)

Physical support	Name	Information support	$\|0\rangle$	$\|1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photon	Fock state	Vacuum	Single photon state
	Time bin encoding	Time of arrival	Early	Late
Electrons	Electronic spin	Spin	Up	Down
	Electron number	Charge	No electron	One electron

Matrix Representation

Classical bits: $0, 1$. Quantum counterpart $|0\rangle, |1\rangle$.

$|0\rangle$ can be written as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle$ can be written as $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Superposition of $|0\rangle, |1\rangle$: $\alpha|0\rangle + \beta|1\rangle$ can be written as

$$\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

Basic Algebra (tensor product)

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$$

$$= \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} \otimes \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1 \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \\ \beta_1 \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix}$$

$$= \alpha_1\alpha_2 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_1\beta_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \beta_1\alpha_2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \beta_1\beta_2 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle,$$

can be seen as tensor product.

n Qubits State

***n* qubit state:**

$$|x_0\rangle \otimes |x_1\rangle \otimes \ldots \otimes |x_{n-2}\rangle \otimes |x_{n-1}\rangle = |x_0, x_1, \ldots, x_{n-2}, x_{n-1}\rangle,$$

with $x_i \in \{0, 1\}$

- Can be written as a $2^n \times 1$ matrix
- All values are 0 except 1 at the row indexed by the integer $x_0, x_1, \ldots, x_{n-2}, x_{n-1}$ in binary
- $|00\rangle \rightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, $|01\rangle \rightarrow \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$, $|10\rangle \rightarrow \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$, $|11\rangle \rightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

Any 2-qubit state may not be decomposed as above.

Consider the state

$$\gamma_1|00\rangle + \gamma_2|11\rangle$$

with $\gamma_1 \neq 0, \gamma_2 \neq 0$. This cannot be written as

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle).$$

This is called entanglement. Known as Bell states or EPR pairs. An example of maximally entangled state is

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

Qubits and Measurement

- Two types of measurement; Projective and POVM (Positive Operator Valued Measure)
- A simple and important example of measurement is the measurement in *computational basis* i.e., in $\{|0\rangle, |1\rangle\}$ basis
- Two measurement operators are available; $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$
- Matrix representation; $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
- Note that $\sum_{i=0}^{1} M_i^\dagger M_i = I$ (Completeness condition), where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Measurement

- Consider the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.
- If we choose M_0, the state after measurement becomes $|\phi_0\rangle = \frac{M_0|\psi\rangle}{\sqrt{\langle\psi|M_0^\dagger M_0|\psi\rangle}}$
- Matrix representation of

$$M_0\,|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

- Matrix representation of

$$\langle\psi|M_0^\dagger M_0|\psi\rangle = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\alpha|^2$$

Measurement (Contd.)

- We get

$$\begin{aligned} |\phi_0\rangle &= \frac{M_0 |\psi\rangle}{\sqrt{\langle\psi| M_0^\dagger M_0 |\psi\rangle}} \\ &= \frac{\alpha}{|\alpha|} |0\rangle \\ &= \exp\{j\theta\} |0\rangle \rightarrow |0\rangle \end{aligned}$$

  (We neglect the phase here)

- Similarly, if we choose M_1, we get $|\phi_1\rangle = \frac{M_1|\psi\rangle}{\sqrt{\langle\psi| M_1^\dagger M_1 |\psi\rangle}} = |1\rangle$

Measurement (Contd.)

- The probability to get $|0\rangle$ is $p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = |\alpha|^2$
- Probability to get $|1\rangle$ is $p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = |\beta|^2$
- Example:

$$\frac{1+i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

- Measurement: $|0\rangle$ with probability $\frac{1}{2}$, and $|1\rangle$ with probability $\frac{1}{2}$.
- This is an example of Projective measurement

How to Distinguish $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

- Measurement (M):
  - $\Pr(M = |0\rangle \,|\, |0\rangle) = 1$
  - $\Pr(M = |1\rangle \,|\, |0\rangle) = 0$
  - $\Pr(M = |0\rangle \,|\, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{1}{2}$
  - $\Pr(M = |1\rangle \,|\, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{1}{2}$
- Strategy:
  - Measure $|0\rangle$, tell $|0\rangle$
  - Measure $|1\rangle$, tell $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Probability of success:

$$\Pr(|0\rangle, |0\rangle) + \Pr(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle))$$

$$= \Pr(|0\rangle) \Pr(M = |0\rangle \,|\, |0\rangle) + \Pr(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \Pr(M = |1\rangle \,|\, \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle))$$

$$= \tfrac{1}{2}.1 + \tfrac{1}{2}.\tfrac{1}{2}$$

$$= \tfrac{3}{4} = 0.75$$

Distinguishing $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (Contd.)

Consider the following operators;

- $E_1 = \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle \langle 1|$;
- Corresponding Matrix representation $\frac{\sqrt{2}}{1+\sqrt{2}} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
- $E_2 = \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}$;
- Corresponding Matrix representation $\frac{\sqrt{2}}{2(1+\sqrt{2})} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$
- $E_3 = I - E_1 - E_2$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- Note that $\sum_i E_i = I$, $i = \{1, 2, 3\}$; Hence $E_i = M_i^\dagger M_i$ in this case

Distinguishing $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (Contd.)

- Strategy:
  - Get E_1, conclude $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - Get E_2, conclude $|0\rangle$
  - Get E_3, inconclusive, random guess
- Measurement (M):
  - $\Pr(M = E_1 | \, |0\rangle) = 0$
  - $\Pr(M = E_1 | \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{\sqrt{2}}{2(1+\sqrt{2})}$
  - $\Pr(M = E_2 | \, |0\rangle) = \frac{\sqrt{2}}{2(1+\sqrt{2})}$
  - $\Pr(M = E_2 | \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = 0$
  - $\Pr(M = E_3 | \, |0\rangle) = (1 - \frac{\sqrt{2}}{2(1+\sqrt{2})})$
  - $\Pr(M = E_3 | \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = (1 - \frac{\sqrt{2}}{2(1+\sqrt{2})})$

Distinguishing $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (Contd.)

- Probability of success for state $|0\rangle$

$$\begin{aligned} & \Pr(E_2, |0\rangle) + \tfrac{1}{2}\Pr(E_3, |0\rangle) \\ = & \Pr(|0\rangle)\Pr(E_2|\,|0\rangle) + \tfrac{1}{2}\Pr(|0\rangle)\Pr(E_3|\,|0\rangle) \\ = & \tfrac{1}{2}.\tfrac{\sqrt{2}}{2(1+\sqrt{2})} + \tfrac{1}{4}.(1 - \tfrac{\sqrt{2}}{2(1+\sqrt{2})}) \\ = & \tfrac{1}{4}(1 + \tfrac{\sqrt{2}}{2(1+\sqrt{2})}) \end{aligned}$$

- Similarly, it can be shown that probability of success for state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is also $\frac{1}{4}(1 + \frac{\sqrt{2}}{2(1+\sqrt{2})})$
- Thus, the total success probability is

$$\begin{aligned} & 2.\frac{1}{4}(1 + \frac{\sqrt{2}}{2(1+\sqrt{2})}) \\ & \approx 0.64 \end{aligned}$$

- $\{E_1, E_2, E_3\}$ is an example of POVM
- POVM does not provide better success probability in this case than projective measurement

Distinguishing $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (Contd.)

POVM does not provide better success probability than projective measurement

Then why should we bother about POVM?

- In projective measurement, when we get $|0\rangle$ we cannot tell anything with certainty i.e., whether it is $|0\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- If we measure $|1\rangle$, we can tell with certainty that the state was $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- This is asymmetric.

Distinguishing $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (Contd.)

So what is the proportion I am sure?

- $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ comes with proportion 0.5 and then measure $|1\rangle$ with proportion 0.5
- The proportion for certainty telling is 0.25 only. Here proportion can be interpreted as probability.
- For $|0\rangle$ measurement , there is no certainty at all, it can be $|0\rangle$ or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- However, in POVM, the proportion of certainty is symmetric and also more than .25, which is .29

Quantum Gates

n inputs, n outputs, reversible. Can be seen as $2^n \times 2^n$ unitary matrices where the elements are complex numbers.

Single input single output quantum gates.

Quantum input	Quantum gate	Quantum Output
$\alpha\|0\rangle + \beta\|1\rangle$	X	$\beta\|0\rangle + \alpha\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	Z	$\alpha\|0\rangle - \beta\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	H	$\alpha\frac{\|0\rangle+\|1\rangle}{\sqrt{2}} + \beta\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$

Quantum Gates (contd.)

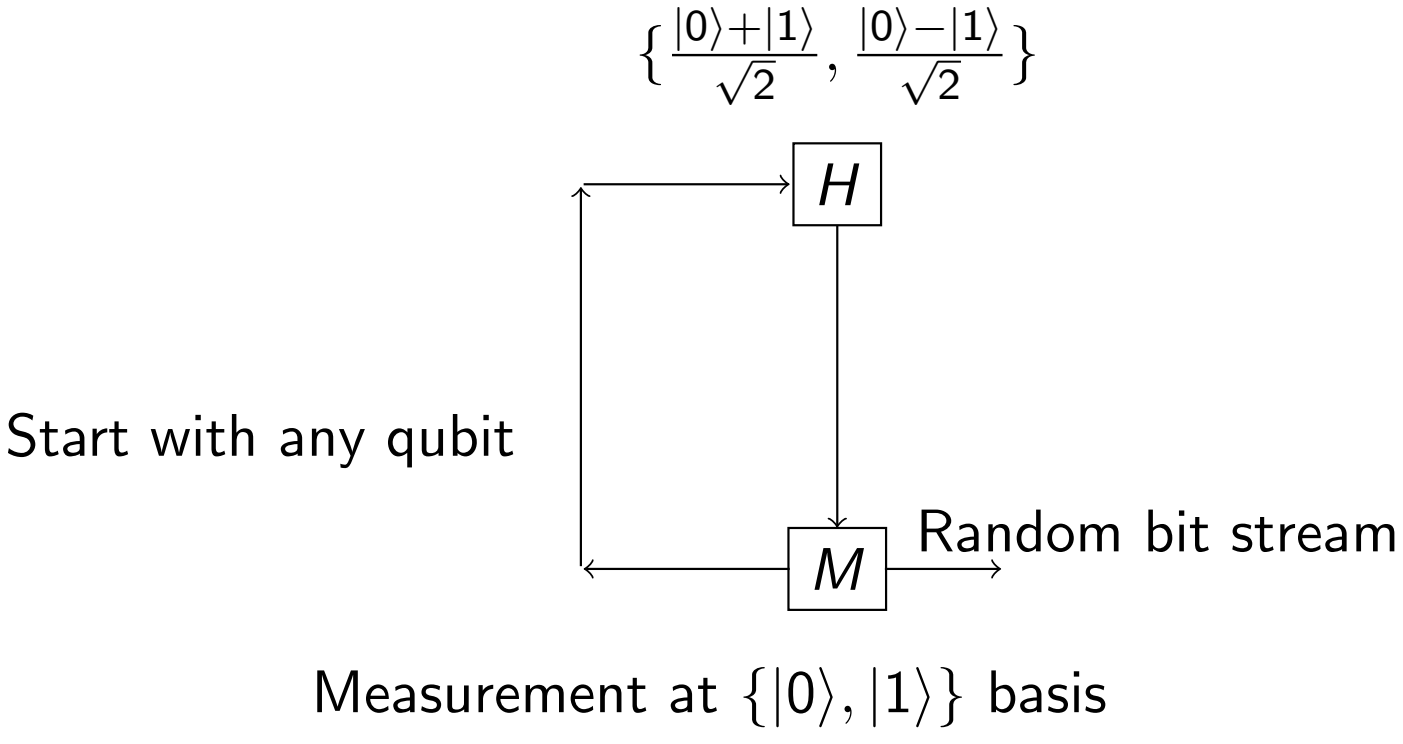
1 input, 1 output. Can be seen as $2^1 \times 2^1$ unitary matrices where the elements are complex numbers.

The X gate: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$

The Z gate: $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$

The H gate: $\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{\alpha+\beta}{\sqrt{2}} \\ \frac{\alpha-\beta}{\sqrt{2}} \end{bmatrix}$

A True Random Number Generator



Quantum Gates (contd.)

2-input 2-output quantum gates. Can be seen as $2^2 \times 2^2$ unitary matrices where the elements are complex numbers.

These are basically 4×4 unitary matrices. An example is the CNOT gate.

$$
\begin{aligned}
|00\rangle &\rightarrow |00\rangle, \\
|01\rangle &\rightarrow |01\rangle, \\
|10\rangle &\rightarrow |11\rangle, \\
|11\rangle &\rightarrow |10\rangle.
\end{aligned}
$$

The matrix is as follows:

$$
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
$$