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	$\vert 0\rangle$	$\vert 1\rangle$
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)

$$
\begin{aligned}
&(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \\
&= \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} \otimes \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1 \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \\ \beta_1 \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix} \\
&= \alpha_1\alpha_2 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_1\beta_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \beta_1\alpha_2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \beta_1\beta_2 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \\
&= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle,
\end{aligned}
$$

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
- $|00\rangle \rightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle \rightarrow \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |10\rangle \rightarrow \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |11\rangle \rightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

Entanglement

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

$$\begin{aligned} & \Pr(|0\rangle\,, |0\rangle) + \Pr(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \\ = {} & \Pr(|0\rangle) \Pr(M = |0\rangle \mid |0\rangle) + \Pr(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \Pr(M = |1\rangle \mid \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \\ = {} & \tfrac{1}{2}.1 + \tfrac{1}{2}.\tfrac{1}{2} \\ = {} & \tfrac{3}{4} = 0.75 \end{aligned}$$

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 $\frac{\sqrt{2}}{2(1+\sqrt{2})} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$
- $E_3 = I - E_1 - E_2, \quad \text{where } I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- 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.)

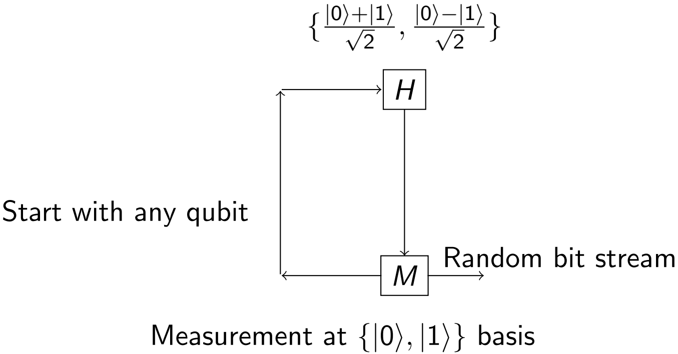
1 input, 1 output. Can be seen as $2^1 \times 2^1$ unitary matrices where the elements are complex numbers.

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



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

Start with any qubit

Random bit stream

Measurement at $\{|0\rangle, |1\rangle\}$ basis

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:

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

Preliminaries (circuit for entangled state)

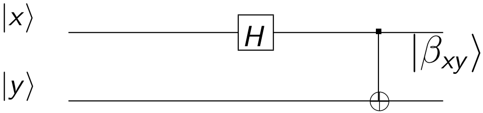


Figure: Quantum circuit for creating entangled state

Bell State	Description
$\|\beta_{00}\rangle$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
$\|\beta_{01}\rangle$	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$
$\|\beta_{10}\rangle$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
$\|\beta_{11}\rangle$	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}}$

Cloning: Possible in classical domain, not in quantum

- Possible to copy a classical bit
- Not possible for an unknown quantum bit
- A result of quantum mechanics
- Stated by Wootters, Zurek, and Dieks in 1982
- W. K. Wootters and W. H. Zurek. A Single Quantum Cannot be Cloned, Nature 299 (1982), pp. 802803.
- D. Dieks. Communication by EPR devices, Physics Letters A, vol. 92(6) (1982), pp. 271272.
- Huge implications in quantum computing, quantum information, quantum cryptography and related fields.

No cloning (contd.)

- It is not possible to copy an unknown Quantum state.
- Consider a quantum slot machine with two slots labeled A and B.
- A is the data slot set in a pure unknown quantum state $|\psi\rangle$ whereas B is target slot set in a pure state $|s\rangle$ where A will be copied.

No cloning (contd.)

- Let there exist a unitary operator which does the copying procedure. Mathematically it is written as $U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$.
- U: unitary operator, $UU^\dagger = I$.
  $(U^\dagger)_{ij} = \overline{U}_{ji}$, transpose and scalar complex conjugate.
- Let this copying procedure works for two particular pure states, $|\psi\rangle$ and $|\phi\rangle$. Then we have

$$U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle, U(|\phi\rangle|s\rangle) = |\phi\rangle|\phi\rangle$$

- Take the inner product: $\langle s|\langle\psi|U^\dagger U|\phi\rangle|s\rangle = \langle\psi|\langle\psi||\phi\rangle|\phi\rangle$.
  This implies $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$.

No Cloning (contd.)

- $x = x^2$ has only two solutions: $x = 0$ and $x = 1$.
- Thus we get either $|\psi\rangle = |\phi\rangle$ or inner product of them equals to zero, i.e., $|\psi\rangle$ and $|\phi\rangle$ are orthogonal to each other.
- Thus a cloning device can only clone orthogonal states. Therefore a general quantum cloning device is impossible.
- Example: it is given that the unknown state is one of $|0\rangle$, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, two nonorthogonal states. Then it is not possible to clone the state without knowing which one it is.

Orthogonal quantum states: distinguishable

- Possible to distinguish two orthogonal states only
- Given two orthogonal states $\{|\psi\rangle, |\psi_\perp\rangle\}$, it is possible to distinguish them with certainty.
- For example,

$$\{|0\rangle, |1\rangle\};$$

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

$$\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

Distinguishability of Nonorthogonal quantum states

- Not possible to distinguish two nonorthogonal quantum states with certainty
- Given two nonorthogonal states $\{|\psi_0\rangle, |\psi_1\rangle\}$, it is not possible to distinguish them with probability 1.
- Example: it is given that the two states are $|0\rangle$, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, two nonorthogonal states. Then it is not possible to exactly identify each one.

Quantum Key Exchange Protocol: BB84

- Initiated by Charles Bennett and Gilles Brassard in 1979

  G. Brassard. Brief History of Quantum Cryptography: A Personal Perspective. [quant-ph/0604072]
- The paper was not getting accepted initially
- Finally published as Quantum Cryptography: Public key distribution and coin tossing, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)
- Citation: 5660 in August 2016, Google Scholar
- A scheme for quantum key distribution scheme
- The first protocol in the area of quantum cryptography
- The basics of this protocol comes from the seminal concept by Wiesner.

  S. Wiesner. Conjugate Coding. Manuscript 1970, subsequently published in SIGACT News 15:1, 78–88, 1983.

BB84: Basic Idea

- To transmit 0 or 1 securely.
- Choose some basis:

$$\{|0\rangle, |1\rangle\};$$
$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$
$$\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

- Take any basis. Encode 0 to one qubit and 1 to another qubit.
- If we use only a single basis, then anybody can measure in that basis, get the information and reproduce.
- Thus Alice needs to encode randomly with more than one bases.
- Bob will also measure in random basis.
- Basis will match in a proportion of cases and from that key will be prepared.

BB84 Algorithm (example)

$$+ : \{\uparrow = |0\rangle, \rightarrow = |1\rangle\}, \text{ i.e., } Z \text{ basis}$$

$$\times : \{\nearrow = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \nwarrow = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}, \text{ i.e., } X \text{ basis}$$

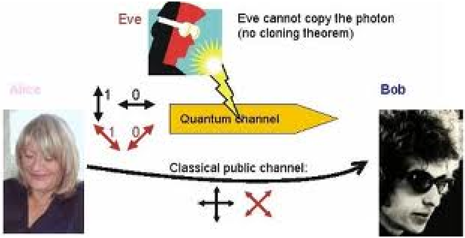
a	0	1	1	0	1	0	0	1
b	0	0	1	0	1	1	1	0
Basis	$+$	$+$	$\times$	$+$	$\times$	$\times$	$\times$	$+$
Polarization	$\uparrow$	$\rightarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\nearrow$	$\nearrow$	$\rightarrow$
Bob's Basis	$+$	$\times$	$\times$	$\times$	$+$	$\times$	$+$	$+$
Bob's measurement	$\uparrow$	$\nearrow$	$\nwarrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\rightarrow$
Public Discussion	M		M			M		M
Shared Key	0		1			0		1

BB84 (contd.)

- The protocol is provably secure (Theoretically)
- Based on no cloning theorem
- The proof comes from the quantum property that information gain is only possible at the expense of disturbing the signal
- If the two states we are trying to distinguish are not orthogonal, it is not possible to distinguish them with certainty
- The protocol is a method of securely communicating a private key from Alice to Bob

Attack Models (partial)

- Alice and Bob are communicating and Eve is sitting in between



- Intercept (measure) and resend: Choice of wrong basis in 50% cases and then out of them, measurement may be wrong in 50% cases. Thus the error rate will be 25%.
- Man in the middle attack: This attack is possible when the communication is being without any authentication. Weakness is same as any other classical protocol.
- Photon number splitting attack: Algorithm using single photon. In practice more than one photon may travel with a single laser pulse. Eve may get hold of the extra photon.

Eavesdropping in Quantum Channel

- The security in the protocol is based on the fact that if one wants to distinguish two non-orthogonal quantum states, then obtaining any information is only possible at the expense of introducing disturbance in the state(s).
- There are several works in the literature, that studied the relationship between "the amount of information obtained by Eve" and "the amount of disturbance created on the qubits that Bob receives from Alice".

Eavesdropping (contd.)

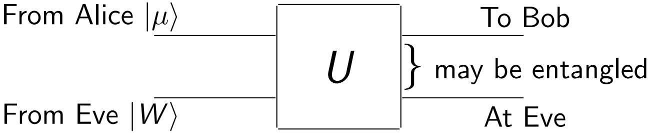
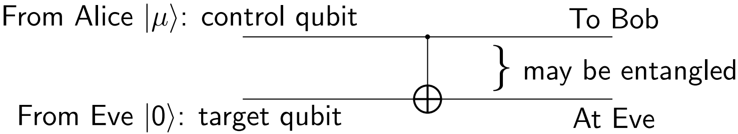


Figure: The model of Eavesdropping

Eve introduces additional qubit(s) to interact with the qubit communicated between Alice and Bob. Through interaction, $|W\rangle$ gets updated extracting some information from $|\mu\rangle$ and in the process $|\mu\rangle$ also gets modified. Thus error appears in the channel.

Simple Example: CNOT attack



From Alice $|\mu\rangle$: control qubit

To Bob

} may be entangled

From Eve $|0\rangle$: target qubit

At Eve

- Alice communicates in Z basis, i.e., $|\mu\rangle$ is either $|0\rangle$ or $|1\rangle$.
- Then Eve can copy that perfectly without creating any disturbance to $|\mu\rangle$.
- Thus the bit error rate in this case will be 0 between Alice and Bob and Eve's success probability in guessing the correct bit will be 1.

CNOT attack (contd.)

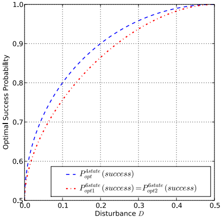
- Alice communicates in X basis, i.e., $|\mu\rangle$ is either $|+\rangle$ or $|-\rangle$.
- Then the output of the CNOT gate is an entangled state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ or $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$ (respectively).
- Consider the $|+\rangle$ case.
- $\frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{|++\rangle+|--\rangle}{\sqrt{2}}$
- If Bob measures in X basis, then he will observe $|+\rangle$ with probability $\frac{1}{2}$ and $|-\rangle$ with probability $\frac{1}{2}$.
- Thus the bit error rate in this case will be $\frac{1}{2}$ between Alice and Bob and Eve's success probability in guessing the correct bit will also be $\frac{1}{2}$.
- The eavesdropping is asymmetric.

Variants of BB84

Six-state protocol, 1997

D. Bruß. Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, 81 (1998) 3018–3021

- Exploiting an extra basis it would be possible to reduce the success probability of Eve to get the information about the raw key



Variants of BB84 (Contd.)

Semi quantum key distribution, 2007

M. Boyer, R. Gelles, D. Kenigsberg and T. Mor. Semi Quantum Key Distribution. Phys. Rev. A, 79:032341, Mar 2009

- Instead of $\{0, 1\}$ and $\{+, -\}$ basis, Bob measures the qubits in $\{0, 1\}$ basis only
- The authors call the $\{0, 1\}$ basis as the classical basis because of one-to-one correspondence with the classical bits
- Bob is called *classical*
- Alice is not classical, as she uses both the basis states like traditional BB84
- The protocol is called *semiquantum*

Other Variants of BB84

- Measurement device independent key distribution, 2012

  H. -K. Lo, M. Curty and B. Qi. Measurement-Device-Independent Quantum Key Distribution. Physical Review Letters, 108, 130503 (2012)

- Side channel free quantum key distribution, 2012

  S. L. Braunstein and S. Pirandola. Side-Channel-Free Quantum Key Distribution. Physical Review Letters, 108, 130502 (2012)

- Memory-assisted measurement-device-independent quantum key distribution, 2014

  C. Panayi, M. Razavi, X. Ma, N. Lütkenhaus. Memory-assisted measurement-device-independent quantum key distribution. New Journal of Physics, 16(4), (2014), 043005

Variants of BB84: The present trend

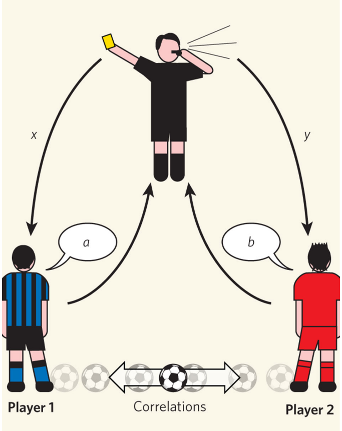
- Quantum Key Distribution: usually based on three main assumptions:
  - validity of Quantum Mechanics
  - assumption of no-information leakage from the honest parties' laboratories
  - fact that the honest parties have a sufficiently good knowledge of their devices
- All the three assumptions are necessary for the security of standard protocols, such as BB84 and its variants. For example, Alice and Bob may unknowingly use multi-photon source in BB84. It causes Photon Number Splitting (PNS) attack.
- Removing the third assumption is the motivation towards Device Independent Quantum Key Distribution.

Device Independent Quantum Key Distribution

- A QKD protocol whose security can then be proven without making any assumptions on the devices.
- These protocols, that are named Device Independent, offer a stronger form of security since they require the minimal assumptions.
- Security comes from some input-output statistics of devices, for example testing Bell inequality or CHSH inequality (John Clauser, Michael Horne, Abner Shimony, and Richard Holt)

CHSH Game

- CHSH game: Alice and Bob are allowed to share some correlation before the game starts
- Alice is given an input x and Bob is given an input y
- The rule of the game is that after receiving the input they can not communicate between themselves.
- Alice outputs a. Bob outputs b
- They win when $a \oplus b = x \wedge y$



CHSH Game (Contd.)

- Best classical strategy: Alice outputs 0, Bob outputs 0 (Same for 1)
- Probability of success: 0.75

(a, b)	(x, y)	$a \oplus b$	$x \wedge y$	$\Pr((a \oplus b = x \wedge y)\|(a, b))$	$\Pr((a \oplus b \neq x \wedge y)\|(a, b))$
(0, 0)	(0, 0)	0	0	$\frac{1}{4}$	0
	(0, 1)	0	0	$\frac{1}{4}$	0
	(1, 0)	0	0	$\frac{1}{4}$	0
	(1, 1)	0	1	0	$\frac{1}{4}$
(1, 1)	(0, 0)	0	0	$\frac{1}{4}$	0
	(0, 1)	0	0	$\frac{1}{4}$	0
	(1, 0)	0	0	$\frac{1}{4}$	0
	(1, 1)	0	1	0	$\frac{1}{4}$

CHSH Game (Contd.)

In quantum domain,

- Alice and Bob share a maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- If $x = 0$, Alice measures her qubit in $\{0, 1\}$ basis, if $x = 1$, she measures her qubit in $\{+, -\}$ basis
- If Alice gets $|0\rangle$ or $|+\rangle$, considers $a = 0$
- If she gets $|1\rangle$ or $|-\rangle$, considers $a = 1$
- If $y = 0$, Bob measures his qubit in $\{\pi/8, -\pi/8\}$ basis, if $y = 1$, he measures his qubit in $\{3\pi/8, -3\pi/8\}$
- If Bob gets $|\pi/8\rangle$ or $|3\pi/8\rangle$, considers $b = 0$
- If Bob gets $|-\pi/8\rangle$ or $|-3\pi/8\rangle$, considers $b = 1$

CHSH Game Contd.

(x, y)	(a, b)	$\mathrm{Pr}((a, b) \vert (x, y))$	$\mathrm{Pr}((a \oplus b = x \wedge y) \vert (x, y))$	$\mathrm{Pr}((a \oplus b \neq x \wedge y) \vert (x, y))$
$(0,\ 0)$	$(0,\ 0)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(0,\ 1)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1,\ 0)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1,\ 1)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
$(0,\ 1)$	$(0,\ 0)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(0,\ 1)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1,\ 0)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1,\ 1)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
$(1,\ 0)$	$(0,\ 0)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(0,\ 1)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1,\ 0)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(1,\ 1)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
$(1,\ 1)$	$(0,\ 0)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$
	$(0,\ 1)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(1,\ 0)$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	$\frac{1}{4}(1 + \frac{1}{\sqrt{2}})$	0
	$(1,\ 1)$	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$	0	$\frac{1}{4}(1 - \frac{1}{\sqrt{2}})$

Quantum Strategy: Success Probability

- $\Pr(a \oplus b = x \wedge y) = \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) = 0.853$
- Quantum Strategy outperforms Classical Strategy.

Quantum Key Distribution Equipments

- Several commercial products are available in international market
- Quantum Key Distribution System (Q-Box). MagiQ Technologies Inc. `http://www.magiqtech.com`
- Company which provides quantum key distribution equipments, quantum random number generator, single photon counter etc.
  ID Quantique (IDQ).
  `http://www.idquantique.com/`
- No equipments for DI-QKD are reported till date
- Industries in India are yet to catch up with recent developments

Summary

- Quantum computer: a real threat to RSA and ECC based cryptography
- Post Quantum Cryptography: Code based and Lattice based; believed to be hard in quantum domain
- Alternative solution: Quantum Cryptography
- Quantum key distribution has been proven secure
- QKD devices are available in the international market
- Important to have complete knowledge of the devices
- Recent trends: Device Independent Quantum Protocols

Thank You