Quantum Supremacy and Its Implication to Cryptology

Arpita Maitra

TCG Centre for Research and Education in Science and Technology
[arpita76b@gmail.com]

August 27, 2020

Controversy: Supremacy Or Advantage!

Some researchers have suggested that the term “quantum supremacy” should not be used, arguing that the word “supremacy” evokes distasteful comparisons to the racist belief of white supremacy. A controversial Nature commentary signed by thirteen researchers asserts that the alternative phrase ”quantum advantage” should be used instead.

Controversy: Supremacy Or Advantage! (Contd.)

John Preskill, the professor of theoretical physics at the California Institute of Technology who coined the term, clarified: "I proposed the term 'quantum supremacy' to describe the point where quantum computers can do things that classical computers can not, regardless of whether those tasks are useful. With that new term, I wanted to emphasize that this is a privileged time in the history of our planet, when information technologies based on principles of quantum physics are ascendant." He further explained: "I considered but rejected several other possibilities, deciding that quantum supremacy best captured the point I wanted to convey. One alternative is 'quantum advantage,' which is also now widely used. But to me, 'advantage' lacks the punch of 'supremacy.' ....."

`https://en.wikipedia.org/wiki/Quantum_supremacy`

Introduction

- Basic model of classical computers: initially visualized by Alan Turing, Von Neumann and several other researchers in 1930's and the decade after that
- The model of computers, that Turing or Neumann studied, are 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.)

- Informally speaking, a quantum system of more than one particles can be explained by a Hilbert space whose dimension is exponentially large in the number of particles
- Thus, one naturally expects that a quantum system can efficiently solve a problem that may require exponential time on a classical computer
- During 1980's, the initial works by Deutsch-Jozsa (1992) and Grover (1996) could explain quantum algorithms that are exponentially faster than the classical ones
- Most importantly, in 1994, Shor discovered that in quantum paradigm, factorization and discrete log problems can be efficiently solved: huge implication to classical PKC

Cryptologic Aspects: 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 (Elliptic 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...."

Quantum Supremacy: Post Quantum Viewpoint

- By Post Quantum Cryptography (PQC) we commonly imply Classical Cryptologic Public Key Algorithms which are resistant against quantum attack, such as Lattice or Code based Cryptography.
- The broader perspective is to obtain an overview of the complete Post-Quantum Scenario from Cryptologic Viewpoint
- Quantum Supremacy (prime ideas)
  - Processor/Circuit: Parallelism
  - Secrecy: No Cloning
  - Communication: Entanglement
  - Advantages in terms of exploiting Quantum Primitives
  - We need to exploit quantum supremacy as a whole, not only in parts

Preliminaries: Qubit

- 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	Polarization	Horizontal	Vertical
Electrons	Electronic spin	Spin	Up	Down

Qubit and Measurement

- A qubit (quantum counterpart of 0, 1):

$$\alpha|0\rangle + \beta|1\rangle,$$

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

- Measurement in $\{|0\rangle, |1\rangle\}$ basis: we will get $|0\rangle$ with probability $|\alpha|^2$, $|1\rangle$ with probability $|\beta|^2$.
  The original state gets destroyed.

- Example:

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

  After measurement: we will get
  $|0\rangle$ with probability $\frac{1}{2}$,
  $|1\rangle$ with probability $\frac{1}{2}$.

Information content in a Qubit

- One may theoretically pack infinite amount of information in a single qubit
- A single qubit may contain huge information compared to a bit
- It is not clear how to extract such information
- In actual implementation of quantum circuits, it might not be possible to perfectly create a qubit for any α, β
- Technology is still at early stage, lot of problems in computation, storage and communication

Basic Algebra

- Basic algebra:
  $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$
  $= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle,$
  can be seen as tensor product.
- 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

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

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.)

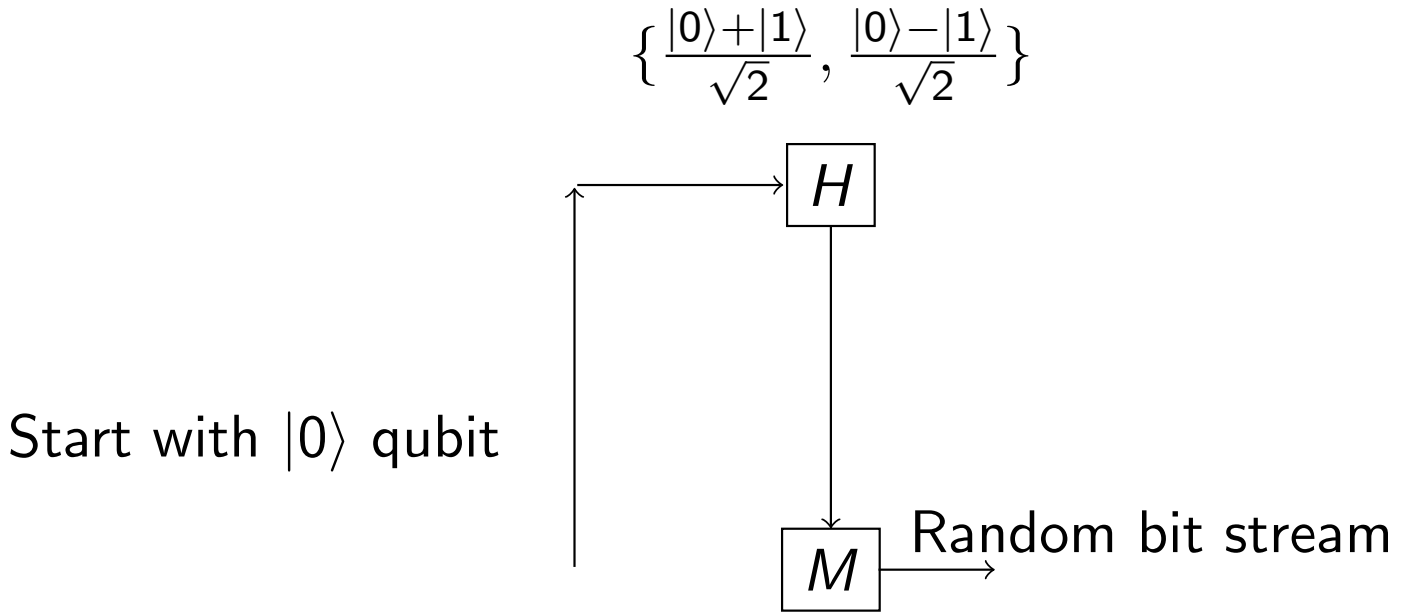
1 input, 1 output. Can be seen as $2^1 \times 2^1$ unitary matrices where the elements are complex numbers.

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

Example: A True Random Number Generator



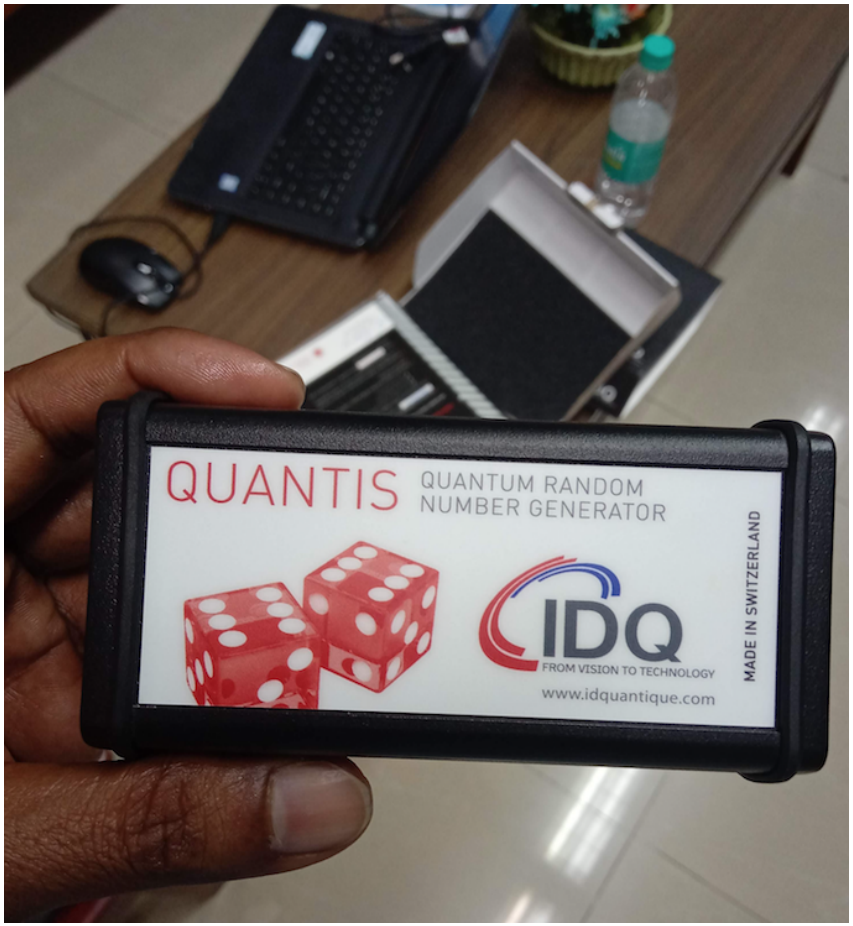
Measurement at $\{|0\rangle, |1\rangle\}$ basis

`https://www.idquantique.com/random-number-generation/products/`

Available commercially in market for almost a decade

Quantis

Quantis is a commercial product which is a Random Number Generator. The Quantis generates random numbers based on quantum phenomenon.



Proper Evaluation of QTRNG

- Actual measurement of speed
- Basic randomness test by NIST suite (statistical testing)
- Are the used qubits entangled? Concept of DI QTRNG
- Analysis for existence of any trap-door in the equipment/algorithm
- Mask the (claimed) True Random stream from third-party equipment with indigenous cryptographic strategy
- Require complete laboratory set-up for exact evaluation and comparison of such QTRNGs

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:

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

Circuit for preparing entangled state

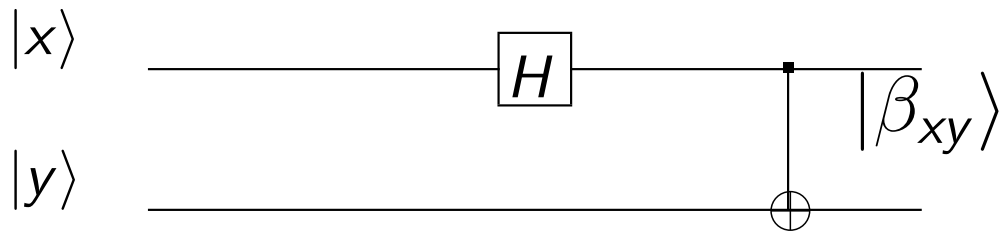


Figure: Quantum circuit for creating entangled state

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

Communication: Quantum Entanglement

- Quantum entanglement is a physical resource, like energy, associated with the peculiar non-classical correlations that are possible between separated quantum systems.
- Entanglement can be measured, transformed, and purified.
- A pair of quantum systems in an entangled state can be used as a quantum information channel to perform computational and cryptographic tasks that are impossible for classical systems.
- Quoted from: `https://plato.stanford.edu/entries/qt-entangle/`
- Testing of Maximally entangled states is part of many Device Independent (DI) protocols

Quantum Supremacy: 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 (classical): 0.75
- Probability of success (quantum): $\frac{1}{2}(1 + \frac{1}{\sqrt{2}}) = 0.853$
- Quantum Strategy outperforms Classical Strategy
- Entanglement required
- Exploited in Device Independent Quantum Cryptography

Quantum Teleportation (wiki)

- Quantum teleportation is a process
  - in which quantum information (e.g. the exact state of an atom or photon) can be transmitted (exactly, in principle) from one location to another,
  - with the help of classical communication and previously shared quantum entanglement between the sending and receiving location.
- Because it depends on classical communication, which can proceed no faster than the speed of light, it cannot be used for faster-than-light transport or communication of classical bits.
- Quantum teleportation (not as in fiction) is limited to the transfer of information rather than matter itself.
- It provides a way of transporting a qubit from one location to another without having to move a physical particle along with it.

Teleportation: Circuit/Communication

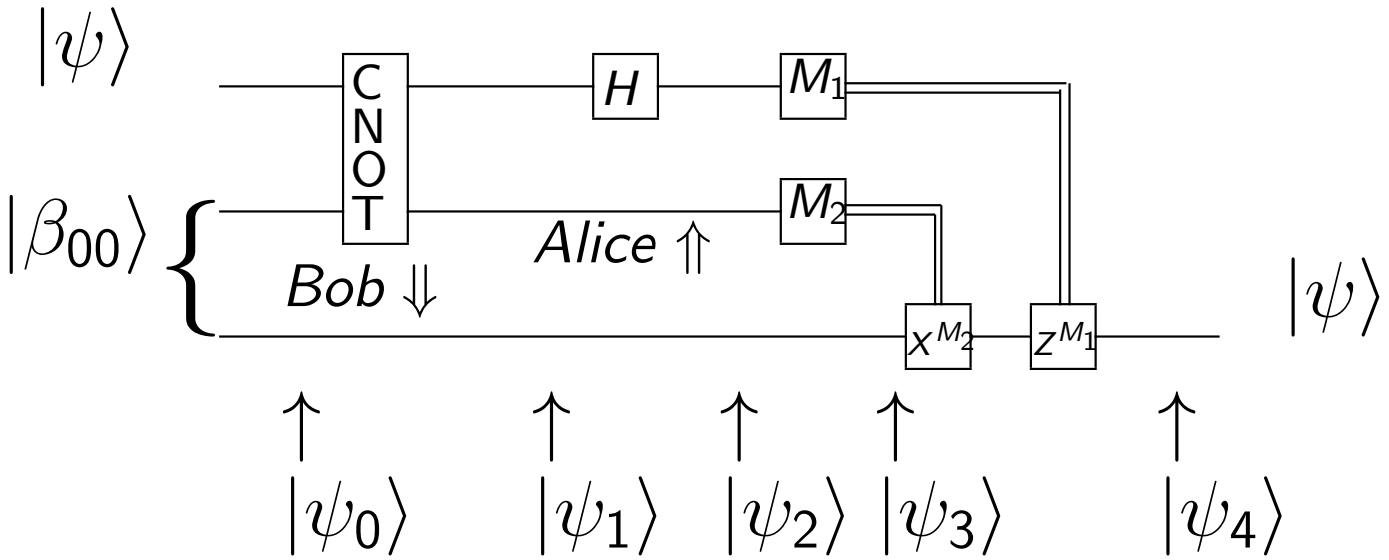


Figure: Quantum circuit for teleporting a qubit: Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters, 1993. Present citation: 12495 (Google Scholar).

Teleportation (step by step algorithm)

- $|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$
- $|\psi_1\rangle = \alpha|0\rangle\frac{(|00\rangle+|11\rangle)}{\sqrt{2}} + \beta|1\rangle\frac{(|10\rangle+|01\rangle)}{\sqrt{2}}$
- $|\psi_2\rangle = \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{(|00\rangle+|11\rangle)}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{(|10\rangle+|01\rangle)}{\sqrt{2}} =$
  $\frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle) +$
  $|10\rangle(\alpha|0\rangle - \beta|1\rangle) - |11\rangle(\beta|0\rangle - \alpha|1\rangle))$
- Observe 00, nothing to do.
- Observe 01, apply X.
- Observe 10, apply Z.
- Observe 11, apply both X, Z.
- The idea of Quantum Teleportation is exploited in Quantum Secret Sharing

Remote state preparation

- A. K. Pati. Minimum cbits for remote preparation and measurement of a qubit. Phys. Rev. A 63, 014302 (2000).
- In teleportation the state $|\psi\rangle$ is unknown. In this case the state is known: $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$.
- Entangled state $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$ is shared between two parties.
- Transformed to different basis $|\psi\rangle$, $|\psi_\perp\rangle$. The entangled state on the new basis can be seen as $\frac{|\psi\psi_\perp\rangle - |\psi_\perp\psi\rangle}{\sqrt{2}}$.
- Alice measures on $|\psi\rangle, |\psi_\perp\rangle$ basis.
- If Alice gets $|\psi_\perp\rangle$, then Bob obtains $|\psi\rangle$, so no change is required. Alice sends cbit 0 in this case.
- If Alice gets $|\psi\rangle$, then Bob obtains $|\psi_\perp\rangle$, so he needs to apply a transformation. Alice sends cbit 1 in this case.
- Note that only one cbit communication is required for remote state preparation.

Cloning: Possible in classical domain, not in quantum

Possible to copy a classical bit

Not possible for an unknown quantum bit

No cloning

- A result of quantum mechanics
- Not possible to create identical copies of an arbitrary unknown quantum state
- It was 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.

No Cloning (contd.) & No Deleting

- The advantages are in the domain of quantum cryptography, where by the laws of physics copying an unknown qubit is not possible
- However, in terms of copying or saving unknown quantum data, this is actually a potential disadvantage.
- Clarification: given a known quantum state, it is always possible to copy it; this is because, for a known quantum state, we know how to create it deterministically and thus it is possible to reproduce it with the same circuit

A. K. Pati and S. L. Braunstein, "Impossibility of Deleting an Unknown Quantum State", Nature 404 (2000), p164.
"Given two copies of some arbitrary quantum state, it is impossible to delete one of the copies ..."

No Cloning (contd.)

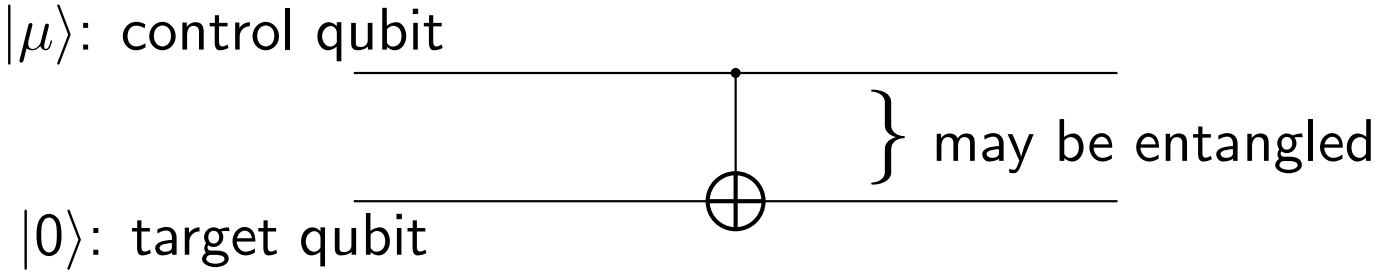


Figure: Explanation of No Cloning with a simple circuit.

- If an unknown qubit $|\mu\rangle$ is either $|0\rangle$ or $|1\rangle$, then it will be copied perfectly without creating any disturbance to $|\mu\rangle$
- However, if $|\mu\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, say, then at the output we will get entangled state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Thus copying is not successful here.

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.

BB84 History (summary)

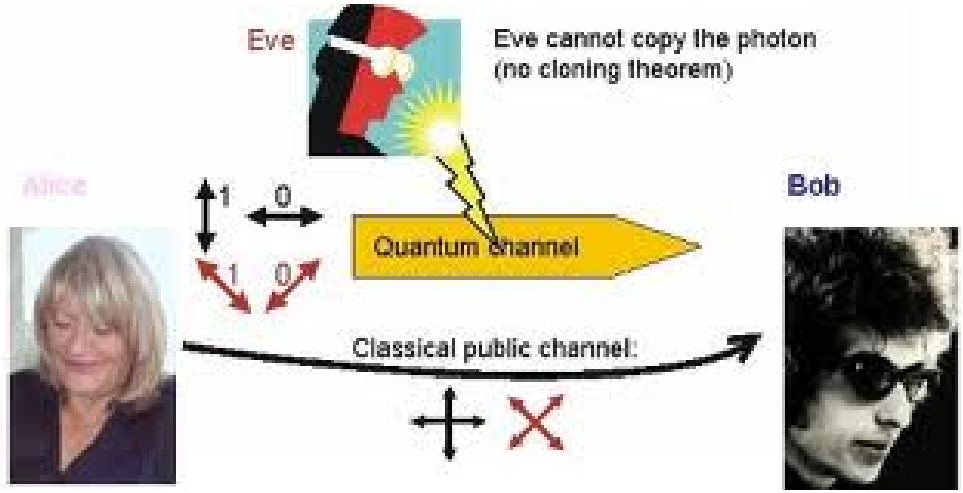
- Initiated by Charles Bennett and Gilles Brassard in 1979

  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: 8275 in Google Scholar
- A scheme for quantum key distribution
- 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 (contd.)

- The protocol is provably secure
- 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

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

- Alice chooses $(4+\delta)n$ many random data bits referred as binary string a
- Alice further chooses a random binary string b of $(4+\delta)n$ bits
- For $i = 0$ to $(4+\delta)n - 1$
  - if $a_i = 0$ and $b_i = 0$ Alice selects the qubit $|0\rangle$
  - if $a_i = 1$ and $b_i = 0$ Alice selects the qubit $|1\rangle$
  - if $a_i = 0$ and $b_i = 1$ Alice selects the qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - if $a_i = 1$ and $b_i = 1$ Alice selects the qubit $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Alice sends the resulting state (qubits) to Bob
- After receiving $(4+\delta)n$ many qubits Bob announces the fact and measures each qubit either in $|0\rangle, |1\rangle$ basis or in $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis at random
- Alice then announces b

BB84 Algorithm (contd.)

- Bob then discards the bits where he measured the qubit in a different basis than Alice prepared and Alice also does the same thing; with high probability there are at least $2n$ bits left (not discarded) and if this does not happen then the protocol is aborted; they work with $2n$ bits
- A subset of n bits are selected by Alice that will serve as checks on the interference of Eve; Alice also tells Bob which bits she actually selected
- Both Alice and Bob announce and compare the values of the n many check bits; if the number of disagreement is more than an acceptable limit then the protocol will be aborted
- Information reconciliation and privacy amplification are performed by Alice and Bob on the remaining n bits to obtain m shared key bits

BB84 Algorithm (example)

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

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

QKD Commercial Products

A partial list:

- Quantum Key Distribution Equipment. ID Quantique (IDQ). `http://www.idquantique.com/`
- Quantum Key Distribution System (Q-Box). MagiQ Technologies Inc. `http://www.magiqtech.com`

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' labs
  - 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 motto of 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 follows from some input-output statistics of devices, for example testing Bell inequality or CHSH inequality (John Clauser, Michael Horne, Abner Shimony, and Richard Holt)
- Some important papers on DI-QKD:
  - Braunstein and Pirandola, 2012;
  - Lo, Curty and Qi, 2012,
  - Vazirani and Vidick, 2012.

Quantum Parallelism

- n-bit binary patterns: 2^n many
- Generating all these patterns in classical computer takes 2^n steps
- $H^{\otimes n}(|0\rangle^{\otimes n}) = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}}$
- n many $|0\rangle$ qubits (linear resource)
- n many 1-input, 1-output H gates (linear resource)
- Equal superposition of all 2^n states (parallelism at exponential level) in a single step

f to U_f

- Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$
- n-input 1-output, not reversible
- Quantum Gates must be reversible
- carry n-inputs to n-outputs
- Add another input y and output $y \oplus f(x)$
- The $(n+1)$-input, $(n+1)$-output function is reversible
- If implementation of f in classical domain requires $T(n)$ gates, the implementation of U_f in quantum domain will require $O(T(n))$ gates
- U_f should be designed in quantum framework, i.e., using quantum gates

Quantum Parallelism: Background towards DJ algorithm

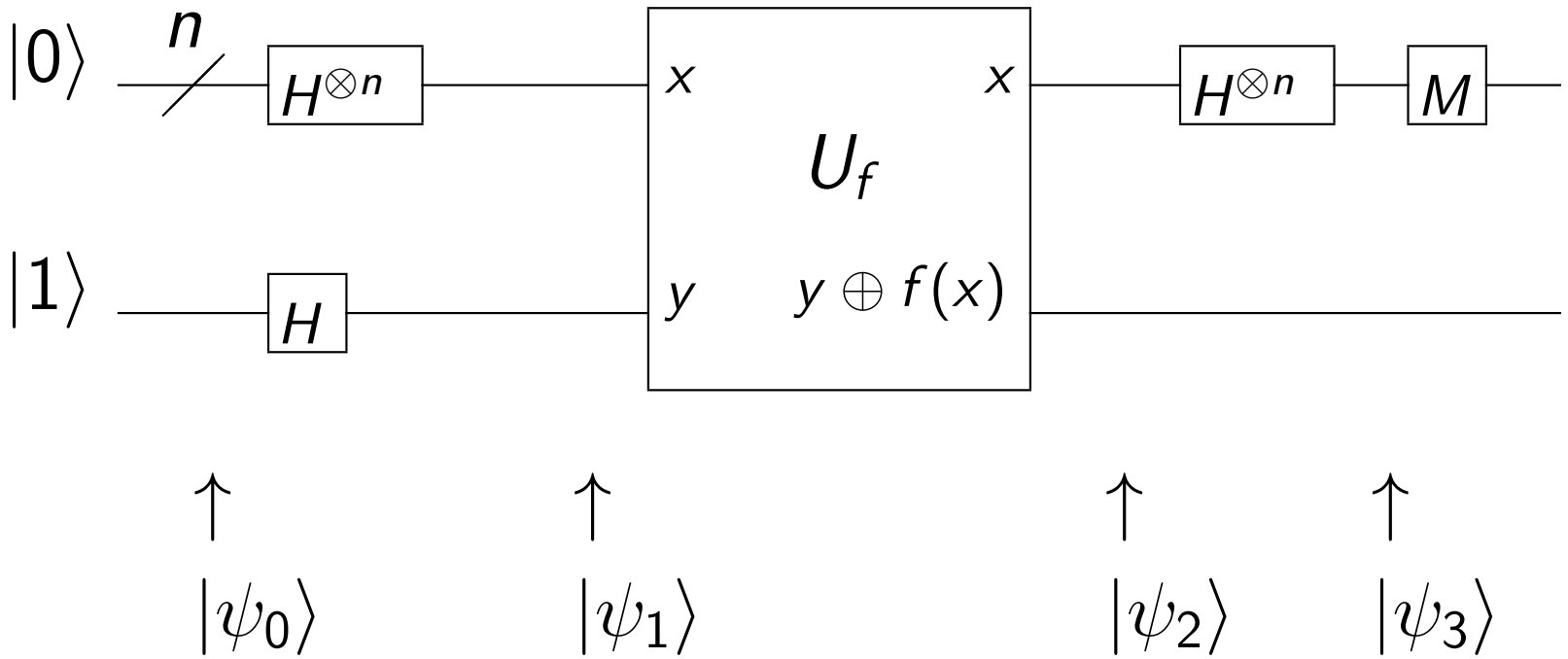
- Given a classical circuit f, there is a quantum circuit of comparable efficiency which computes the transformation U_f that takes input $|x, y\rangle$ and produces output $|x, y \oplus f(x)\rangle$.
- Let f be either constant or balanced. Consider f as an oracle. How fast one can decide which one it is.
- Deterministic classical algorithm may require $2^{n-1} + 1$ queries in worst case. Probabilistic classical algorithm requires a few steps to give an answer with very good probability.

Given such an U_f is available, Deutsch-Jozsa (1992) provided a quantum algorithm that can solve this problem in constant time deterministically.

D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. Proceedings of Royal Society of London, A439:553–558 (1992).

Deutsch-Jozsa Algorithm

Quantum circuit to implement Deutsch-Jozsa Algorithm



DJ Algorithm

- A Boolean function f on n variables is available in the form of the transformation U_f
- Take an $(n+1)$ qubit state $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$
- Apply Hadamard Transform on $|\psi_0\rangle$ to get a superposition $|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$
- Apply U_f on $|\psi_1\rangle$ to get $|\psi_2\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$
- Apply Hadamard Transform on the first n qubits of $|\psi_2\rangle$
- $|\psi_3\rangle = \sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} \frac{(-1)^{x\cdot z \oplus f(x)}|z\rangle}{2^n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$.
- Measurement at M: measure the first n qubits of $|\psi_3\rangle$; all zero state implies that the function is constant, otherwise it is balanced.

Important Quantum Algorithms

- Three algorithms that shows quantum supremacy
- Grover (1996): Search
- Simon (1994): Special case of period finding
- Shor (1994): Factorization

Grover's Algorithm

- n-input 1-output Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$
- The Boolean function is available as a black box
- There exists an x, such that $f(x) = 1$, all the other outputs are 0
- Classical algorithm will require $O(2^n)$ queries to the black box in worst case
- Grover's algorithm requires $O(\sqrt{2^n})$ i.e., $O(2^{\frac{n}{2}})$ queries

Simon's Algorithm

- n-input n-output Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}^n$
- The function is available as a black box
- The function satisfy the property that, for some $s \in \{0,1\}^n$, we have, for all $x, y \in \{0,1\}^n$, $f(x) = f(y)$ if and only if $x \oplus y \in \{0^n, s\}$
- $f(x) = f(y)$ is trivially correct, i.e., when $x \oplus y = 0^n$, the all zero pattern
- The main issue is to find non-zero bit pattern s
- Classical algorithm should require $\Omega(2^{\frac{n}{2}})$ queries
- Quantum algorithm requires $O(n)$ queries

Shor's Algorithm

- Factorization of an integer of value N, i.e., of n bits, where $N = 2^n$, i.e., $n = \log N$
- Related to Quantum Fourier Transform
- The algorithm requires quantum gates of order $O\big((\log N)^2(\log\log N)(\log\log\log N)\big)$, which is lower than $O\big((\log N)^3\big)$, i.e., $O\big(n^3\big)$
- Most efficient classical factoring algorithm (known), the general number field sieve, works in sub-exponential time $O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$, i.e., $O\left(e^{1.9(n)^{1/3}(\log n)^{2/3}}\right)$

Cryptographic Implications

- Deutsch-Jozsa: Linear approximation of a Boolean function used in a cryptographic circuit by exploiting high Walsh spectrum values
- Grover: For any symmetric key cryptosystem with n bit secret key, the key can be recovered in $O(2^{n/2})$, reducing the effective key length to half.
- Simon: Exploited in Differential Cryptanalysis in symmetric ciphers
- Shor: Complete break of popular PKCs like RSA or ECC
- Several papers in top cryptology conference connecting, improving and implementing these results

Actual Implementation Issues

- Substantial work has been done on the quantum attack of symmetric ciphers
- However, most of the papers are theoretical; practical implementation issues remained unexplored

State-of-the-art Situation

- Large scale fault tolerant commercial quantum computers are still out of the reach
- Publicly available Quantum Computers:
  - IBM (Quantum Information Tool Kit (QISKIT))
  - Microsoft (Quantum Development Kit (QDK))
  - Google (Cirq, an open source framework for Noisy Intermediate Scale Quantum (NISQ) computers)
  - Rigetti (Forest Quantum Computing Software, a cloud platform that enables programmers to write quantum algorithm)
  - D-Wave (Ocean Tools Suite)

A basic question

- A quantum black box is available
- If large processing power available, then exponentially fast processing will prove quantumness; however, this is not the present situation
- Available: less number of qubits, less processing power compared to present day classical computers or their clusters
- One may feed classical input and obtain classical output
- One can input a program, and run that in the machine with some specific classical inputs and obtain some classical outputs
- How to check quantum-ness?

How to Check Quantum-ness?

- To check quantumness, we need to stream-line our interaction with quantum computers
- If you ask a quantum computer to perform a computation for you, how can you know whether it has really followed your instructions, or even done anything quantum at all?
- PhD thesis of Urmila Mahadev: important result in Theoretical Computer Science
  - `https://www.quantamagazine.org/graduate-student-solves-quantum-verification-problem-20181008/`
  - `https://arxiv.org/abs/1804.00640`
- However, it seems not that easy to perform the protocol on existing limited publicly available resource like IBM Q

Google's Supremacy

- The paper published in Nature on 23rd October 2019 claimed that Google has achieved quantum supremacy with their 53 qubit quantum processor, Sycamore.
- Claim:
  - In the task of sampling the output of a pseudo-random quantum circuit, they found some bitstrings are much more likely to occur than others in 200 seconds
  - Classically computing this probability distribution becomes exponentially more difficult with the number of qubits and the number of gate cycles.
  - In classical computer for the circuits which have been demonstrated in Sycamore takes 10,000 years
- However, IBM challenges their claim. They found that using some clever strategy the problem can be solved in 2.5 days in super computer
- How to check quantum-ness?

Basic Question (2)

- Third-world countries are not front-runner in fabrication of quantum equipments
- As in case of classical computational and communication equipments, it is expected that they would purchase quantum equipments from external agencies only
- How to evaluate the third-party quantum equipments?

What we should explore? (1)

- Theoretical analysis of existing quantum algorithms
- Exploring new quantum algorithms
- A long list of algorithms are discussed in Quantum zoo, `https://quantumalgorithmzoo.org/`
- Need to understand how fast those algorithms can be implemented in classical environment, may be using super-computer
- We should carefully choose/explore problems for exploiting quantum algorithms

What we should explore? (2)

- Actual implementation of quantum algorithms
- Most important ones will be cryptanalytic techniques
- To create toy cipher, and attempt to break those in existing infrastructure
- Identify exact problems in implementation given quantum environment

What we should explore? (3)

- Lots of classical preprocessing and post processing are required before and after the quantum module
- Example: Error correction and hashing after QKD algorithms
- Such classical modules should be implemented, studied and interface with the quantum modules should be finalized

Thank you