Opportunities & Security Challenges in Quantum Computing Technology

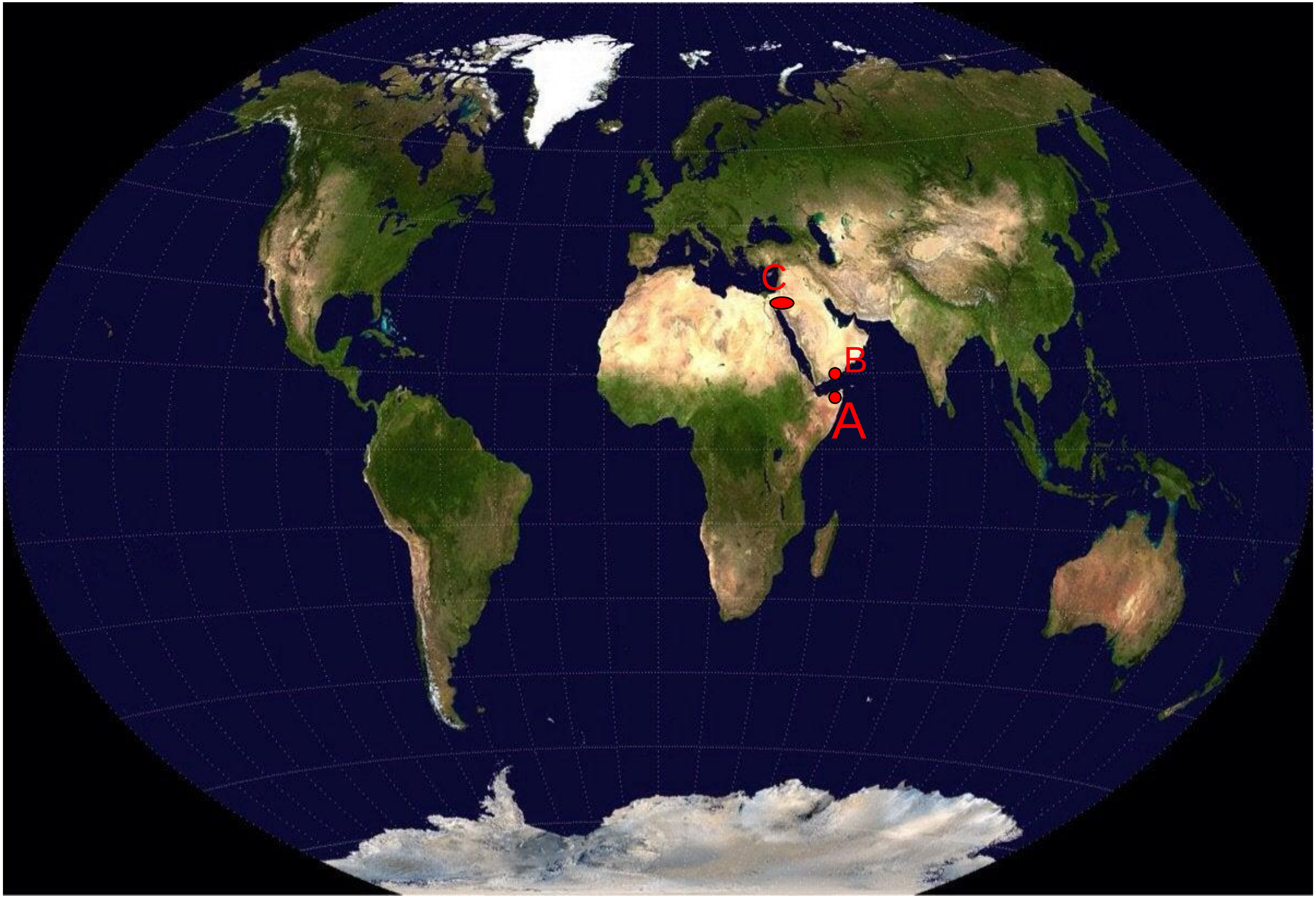
Dr. Om Pal , Associate Professor,

Department of Computer Science,

University of Delhi

(Ex-Scientist, MeitY. Ex-Sr Technical Officer, C-DAC.

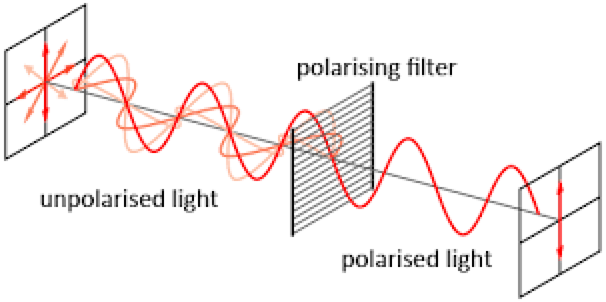
Ex-Engineer, NTPC)

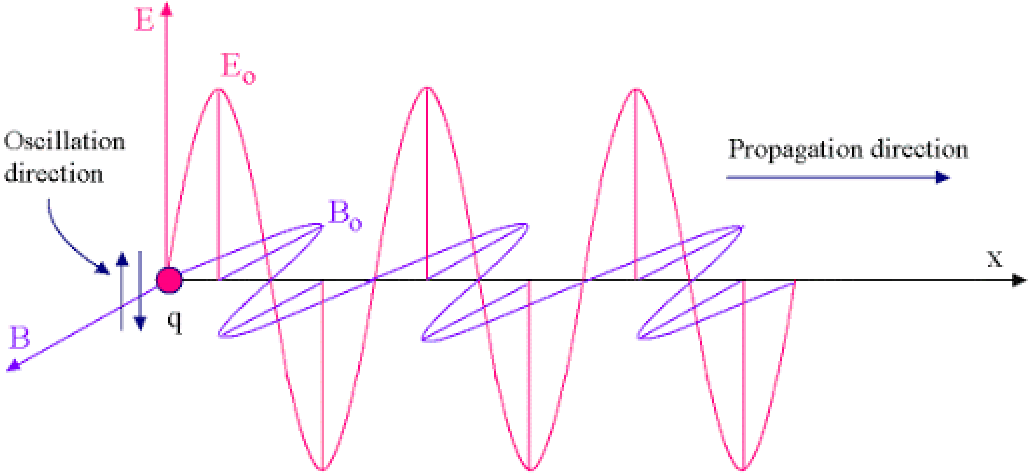

C
B
A

Quantum Computer?

- Zebra strips, Seeds, DNA, Firefly
- Classical Physics vs Quantum Physics
- A quantum computer is any device for computation that makes direct use of quantum mechanical phenomena such as superposition and entanglement, to perform operations on data.
- A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.
- In classical computing, transistors store information either in ‘on’ or ‘off’ state.
- In quantum, state may be ‘spin up’- ‘spin down’, ‘clock wise spin’-’anti-clock wise spin’, ‘Horizontal Polarization-Vertical Polarization’
- " I think I can safely say that nobody understands quantum mechanics." (R. Feynman)- 1982

Polarization of photon

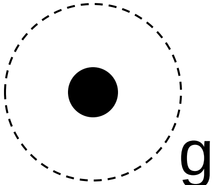




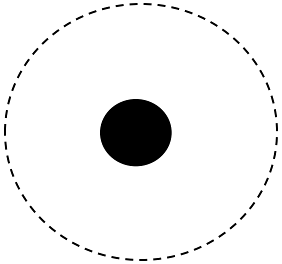
Let horizontal polarization represent 0 and vertical represent 1

Physical quantum bits

- Nuclear spin = orientation of atom’s nucleus in magnetic field.
- ↑ = |0>, ↓ = |1>.
- A bit of data is represented by a single atom.
- There are two base states denoted by |0> and |1>. A single bit of this form is known as a ***qubit***
- A physical implementation of a qubit could use nuclear spin or two energy levels of an atom. An excited state representing |1> and a ground state representing |0>.
- Energy states of an atom



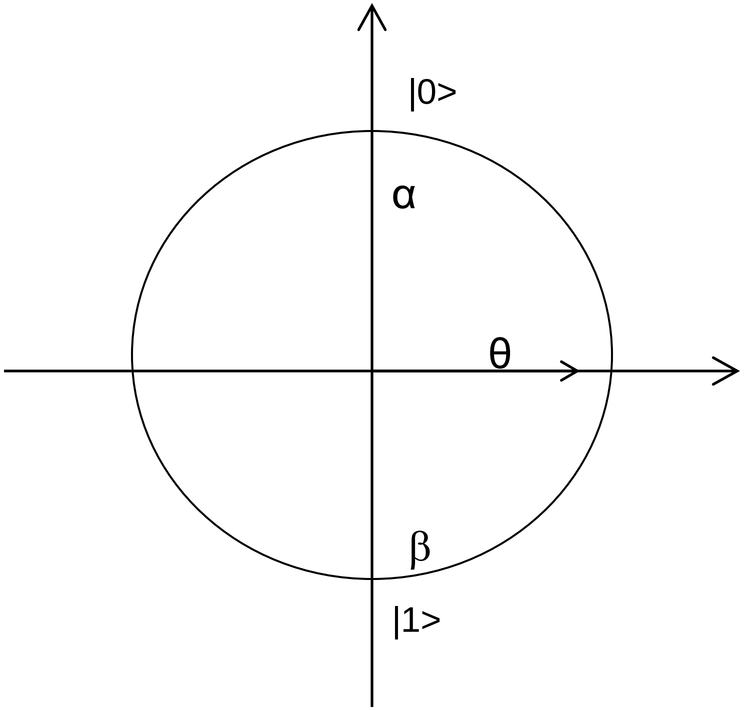
ground state



excited state

- Polarization of photon

Representation of Data- Quibit



- 2-dimensional vector of length 1,
- Basis states |0>, |1>.
- Valid state: α|0>+β|1>,
- α, β complex numbers,
- $|\alpha|^2 + |\beta|^2 = 1$.

- Multi-dimensional vector of length 1

Superposition and Multi-qubit

- quantum particle may remain in a third state which is neither excited state nor ground state.

- If quantum particle is in this new state then this new state represents both 1 and 0 simultaneously.

- Let α, β are two complex numbers over a 2-dimentional vector space of length 1 then superposition state of the particle can be expressed as

- $|\psi> = \alpha|0>+\beta|1>$
- where α, β complex numbers such as $|\alpha|^2+ |\beta|^2=1$. Here α represents probabilistic amplitude of base state $|0>$ and β represents probabilistic amplitude of base state $|1>$.

Qubut 1	Qubit 2	Super Position Vector
$\alpha|0>+\beta|1>$	$\Upsilon|0>+\eta|1>$	$\alpha\Upsilon|00>+\alpha\eta|01> +\beta\Upsilon|10>+\beta\eta|11>$

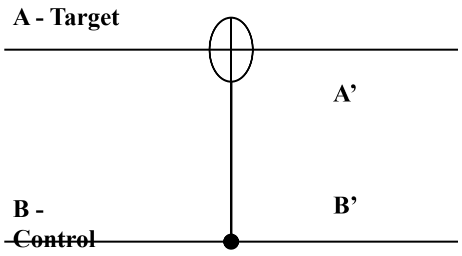
Quantum Entanglement

- ***Entanglement*** is the ability of quantum systems to exhibit correlations between two or more objects even though the individual objects may be spatially separated.
- Particles of light (**photons**) can be **entangled** by splitting a single particle into two **photons** in a laser arrangement with a special crystal.
- Imagine two qubits, each in state |0> + |1> (a superposition of the 0 and 1.)
- We can entangle the two qubits such that the measurement of one qubit is always correlated to the measurement of the other qubit.
- When a pair of diamond **crystals** is linked by quantum **entanglement,** Means: both **crystals** are simultaneously vibrating or not vibrating.

Quantum Gates - Controlled NOT

- **Quantum Gate**: It is a setup of quantum mechanical equipments which converts the present quantum state of quantum particle into a new quantum state.

- A gate which operates on two qubits (control qubit and target qubit) is called a ***Controlled-NOT (CNOT) Gate.*** If the bit on the control line is 1, invert the bit on the target line.



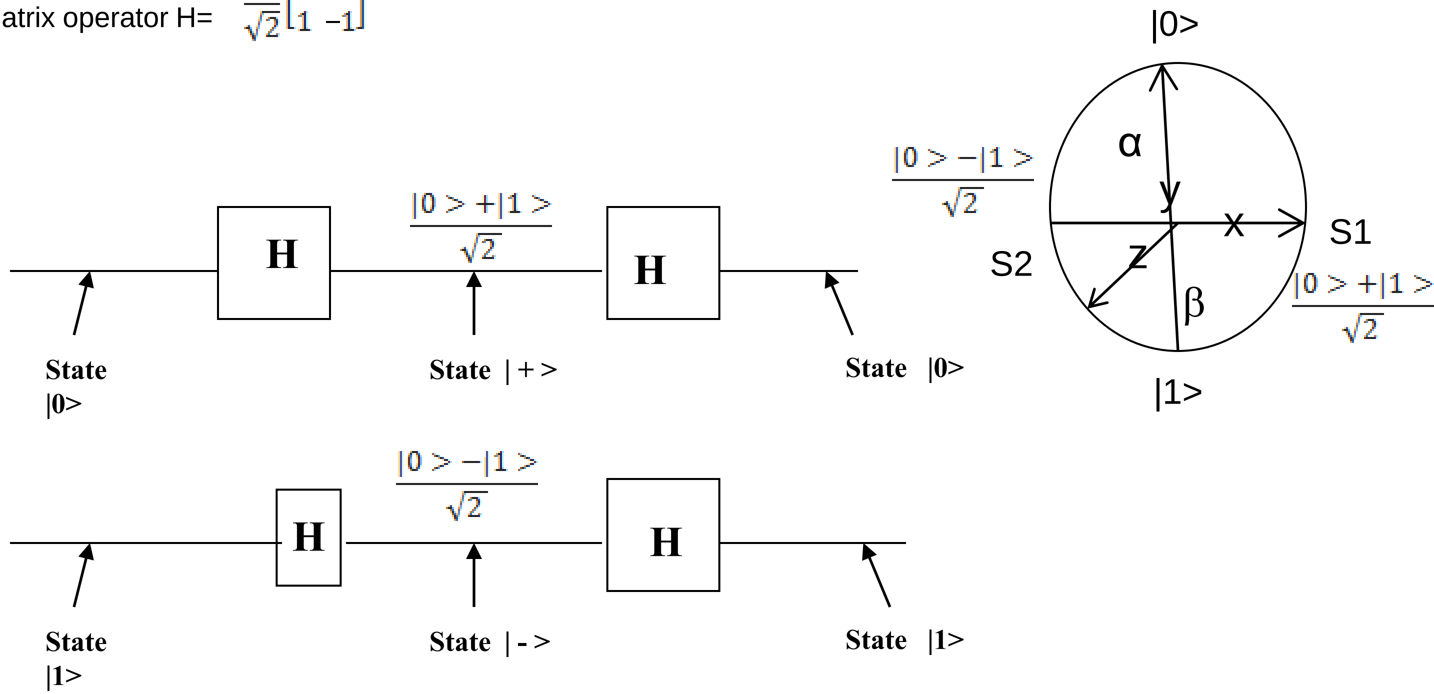
Input		Output	
A	**B**	**A’**	**B’**
0	**0**	**0**	**0**
0	**1**	**1**	**1**
1	**0**	**1**	**0**
1	**1**	**0**	**1**

Note: The CN gate has a similar behavior to the XOR gate with some extra information to make it reversible.

Quantum Gates - Hadamard

- Simplest gate involves one qubit and is called a ***Hadamard Gate (***also known as a square-root of NOT gate.) Used to put qubits into superposition.

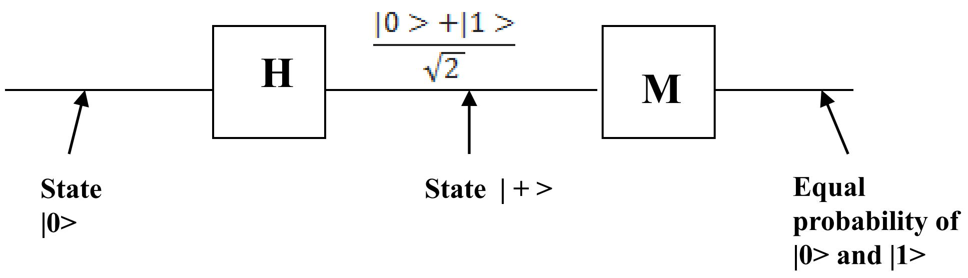
Hadmard matrix operator H= $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$



H
$\frac{|0>+|1>}{\sqrt{2}}$
H
State |0>
State | + >
State |0>
H
$\frac{|0>-|1>}{\sqrt{2}}$
H
State |1>
State | - >
State |1>
|0>
α
y
x
S1
$\frac{|0>-|1>}{\sqrt{2}}$
S2
z
β
$\frac{|0>+|1>}{\sqrt{2}}$
|1>

Quantum Random Number Generation

Hadamard Gate *can be used for quantum random number generation*

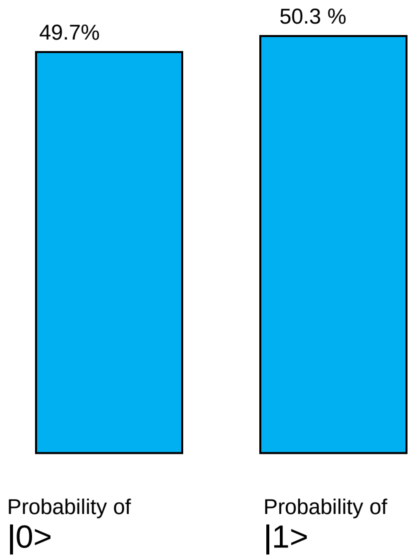


State |0>

State $|+>$

Equal probability of |0> and |1>

```
qc=QuantumCircuit(1)
qc.h(0)
qc.measure_all()
job=execute(qc, backend=QasmSimulator(),
shots=1000)
plot_histogram(job.result().get_count())
```



Quantum Computing Power vs. Classical Computing

- Quantum computing operations are reversible.
- Classical computing operations are irreversible
- All qubits can be operated simultaneously hence, exponential speedup is guaranteed.
- Classical bits are operated sequentially.
- There are only two states (0 and 1) in Classical computing.
- Superposition state represents a new state in Quantum computing hence, more numbers can be stored in qubits in compared to classical bits.

Quantum Oracle with CNOT Gate

- $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$
- $U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$
- $U_f|x\rangle|1\rangle = |x\rangle|f(x)'\rangle$

- Let $x \varepsilon \{0,1\}^n$ and $f: \{0,1\} \rightarrow \{0,1\}$

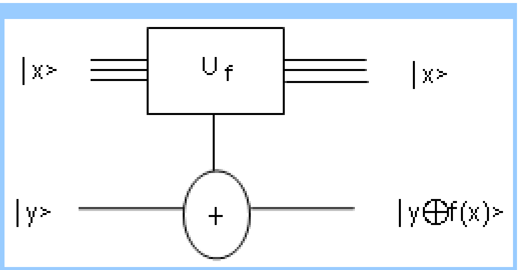


Fig 1

Constant (f(x)=0):

$U_f|x\rangle|y\rangle = |x\rangle|y \oplus 0\rangle = |x\rangle|y\rangle$ Means $U_f = I$

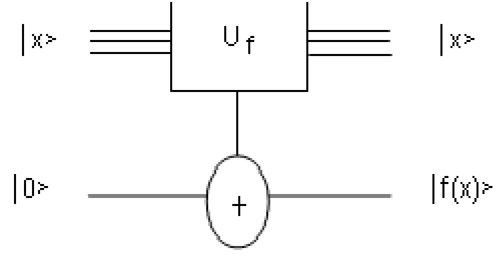


Fig 2

Constant (f(x)=1):

$U_f|x\rangle|y\rangle = |x\rangle|y \oplus 1\rangle = |x\rangle|y'\rangle$

Deutch Problem

Aim: The aim of the Deutch problem is to find out if a given black box oracle represents a constant function or a balanced function.

- Let f(x) is an n-bit boolean function. The input string x can have 2^n possible values.
- Value of f(x) is either 0 or 1 for 2^n possible values of x. $f: \{0,1\}^n \rightarrow \{0,1\}$

Constant function: either f(x) =0 for all 2^n possible values or f(x) =1 for all 2^n possible values.

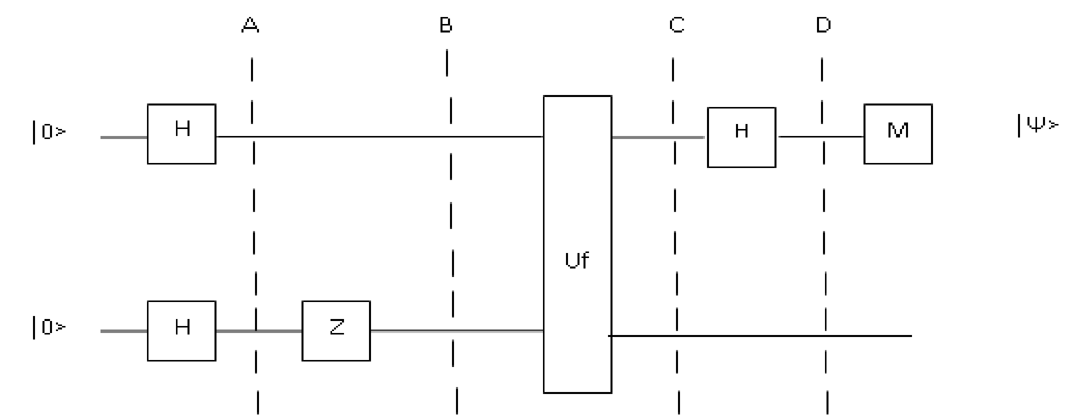
Balanced function: f(x) =0 for 2^{n-1} times and f(x) =1 for 2^{n-1} times

Problem: Let given function f(x) is either constant or balanced. Implementation of function is a black box oracle, so form of f(x) is unknown.

Now we have to find out the function whether it is constant or balance.

Deutch Problem

- To certify that function is constant, 2^{n-1} +1 number of queries are needed in classical computing.



At step A:

|0>|0> ($H^{x}H$)→ |+>|+>

At step B:

Transformation $I^{x}Z$ is applied to the state |+>|+> So, |+>|+> ($I^{x}Z$)→ |+>|-> Now target qubit is in |-> state.

At step C: U_f is applied to state |+>|-> hence

$\frac{|0>+|1>}{\sqrt{2}}$|-> U_f → $((-1)^{f(0)}|0>+(-1)^{f(1)}|1>)$/sqrt 2|-> $\{U_f\,|x>|-> = (-1)^{f(x)}|x>|->\}$

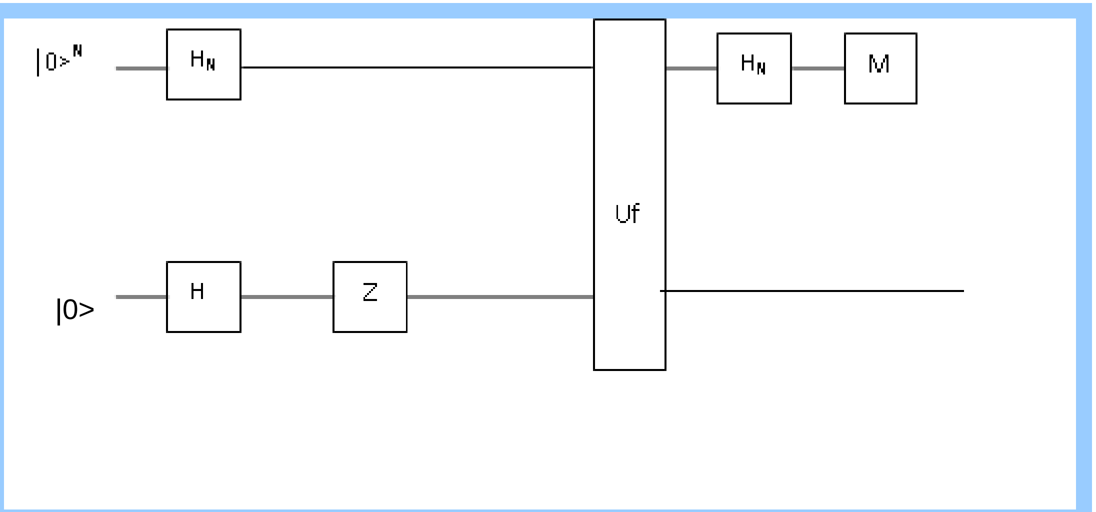
At step D: Transformation $H^{x}I$ is applied. If f(0)=f(1) then input state is |+>|-> and result is |+>|-> ($H^{x}I$)→ |0>|->

If f(0)≠ f(1) then input state is |->|-> and result is |->|-> ($H^{x}I$)→ |1>|->

Conclusion: If f(0)=f(1) then function is constant and |ψ>=|0>. If f(0)≠ f(1) the function is balanced and |ψ>=|1>. Hence measurement of first qubit reveal the function.

Deutch-Jozsa Problem

- This is the extension of Deutch problem. Instead of Single qubit input (|0>) n number of qubits (|0>^{n}) Are given as inputs.



Deutch algorithm:

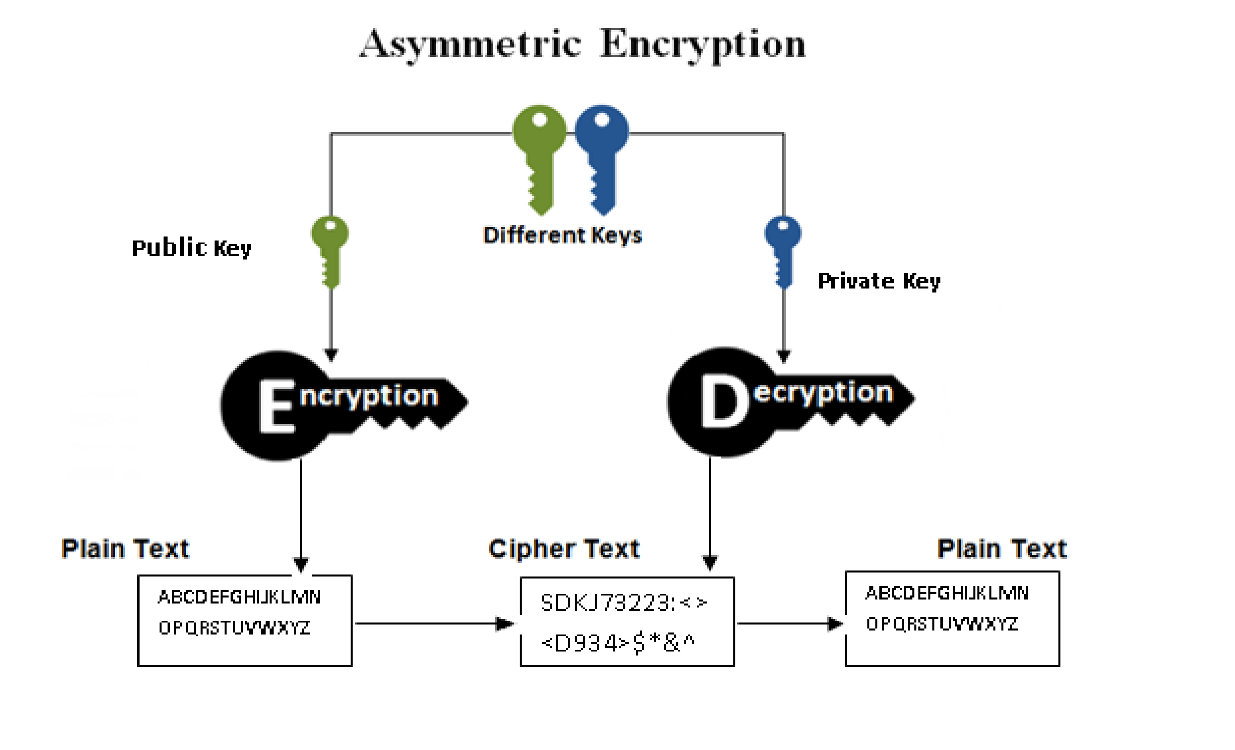
An oracle (black box) function f: {0,1}→{0,1} maps 1 bit to 1 bit. Here f is either constant or balance. Deutch algorithms needs only one query for determining whether function is constant or balance.

Deutch-Jozsa algorith:

An oracle (black box) function f: $\{0,1\}^n \rightarrow \{0,1\}$ maps n bits to 1 bit. Here f is either constant or balance. Deutch-Jozsa algorithms needs only one query for determining whether function is constant or balance.

Public Key Cryptographic System

One of these two keys should be kept private, called private-key, and the other can be made public (it can even be sent in mail), called public-key.



RSA (Rivest–Shamir–Adleman) Algorithm

Each user generates a public/private key pair by:

- selecting two large primes at random - p, q
  - computing their system modulus $N=p.q$
    - Then $\varnothing(N)=(p-1)(q-1)$

- selecting at random the encryption key e

  where $1<e<\varnothing(N)$, $\gcd(e,\varnothing(N))=1$

- solve following equation to find decryption key d
  - $e.d=1 \bmod \varnothing(N)$ and $0\leq d\leq N$

- publish their public encryption key: KU={e,N}
- keep secret private decryption key: KR={d,p,q}

RSA use

- To encrypt a message M the sender:
  - obtains **public key** of recipient `KU={e,N}`
  - computes: $C=M^e \bmod N$, where $0 \le M < N$

- To decrypt the ciphertext C the owner:
  - uses their private key `KR={d,p,q}`
  - computes: $M=C^d \bmod N$

RSA mathematical attack

- Mathematical attacks (based on difficulty of computing ø(N), by factoring modulus N).

  N=p.q

- If we can factor N then we know p and q
  - note ø(N)=(p-1)(q-1)

- Solve following equation to find decryption key d
  - e.d=1 mod ø(N) and 0≤d≤N (Use Euclidean polynomial time algorithm)

- If above steps completed successfully then it means that RSA cryptosystem has been compromised.

RSA & Shor’s Algorithm

- Recently (February 2020), RSA-250 number (250 decimal digits / 829 binary digits) has been factored successfully by Boudot.

- With current computing power, it is estimated that to factor a number of 1000 digits, it would require much longer than the age of universe (13.8 billion years).

- In 1994, Peter Shor proposed a quantum algorithm which can factor an integer N in polynomial time by utilizing the quantum gates in order of $((\log N)^2(\log\log N)(\log\log\log N))$
- As modern public cryptographic systems such as RSA-1000 are using the hardness of integer factorization for security.

- Therefore, these public cryptographic algorithms are not safe after practical implementation of Shor algorithm.

Grover’s Algorithm

- Average complexity of searching an element in a classical bit space of n bits is $2^{n-1}$and worst case complexity is 2^n.
- By using Grover’s algorithm an element can be searched in sqrt(N) steps where N is total elements in the database.
- Grover’s Quantum algorithm reduced the security level of symmetric key cryptographic systems.
- By using Grover’s algorithm symmetric key space is reduced to $2^{n/2}$ from 2^n.
- To maintain the same level of security, double symmetric key length is required in quantum computing environment.

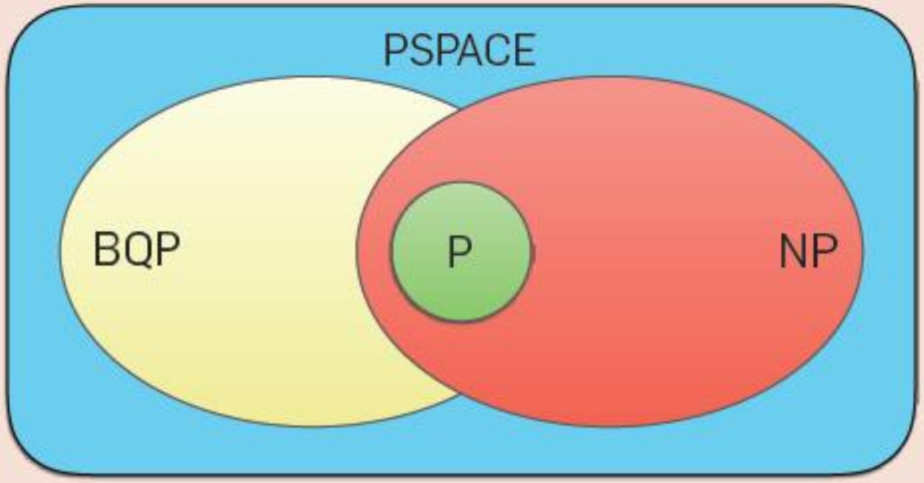
Effective Key Length of Crytpo Systems

Crypto systems	Equivalent symmetric key length (in classical computing scenario)	Quantum Security	Equivalent symmetric key length (in Quantum computing scenario)
RSA-1024	80	Not secure	0
ECC-256	128	Not secure	0
AES-256	256	Secure	128
3-DES-112	112	Not secure (Brute force)	56
SHA-256	256	Secure	85 (Grover's algorithm with birthday paradox)
DSA, ECDSA, ECDH	Secure	Not secure	0

Bounded-error Quantum Polynomial (BQP) Time

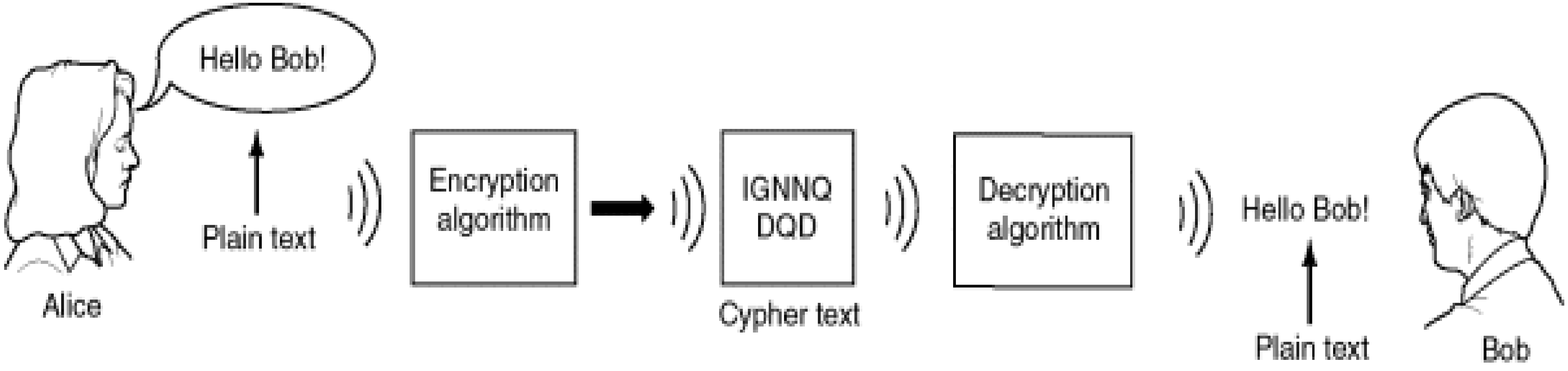
- BQP is the class of decision problems solvable by a quantum computer in polynomial time, with an error probability of at most 1/3 for all instances.

The conjectured relations are reinforced by the existence of oracle results that separate BQP with NP.

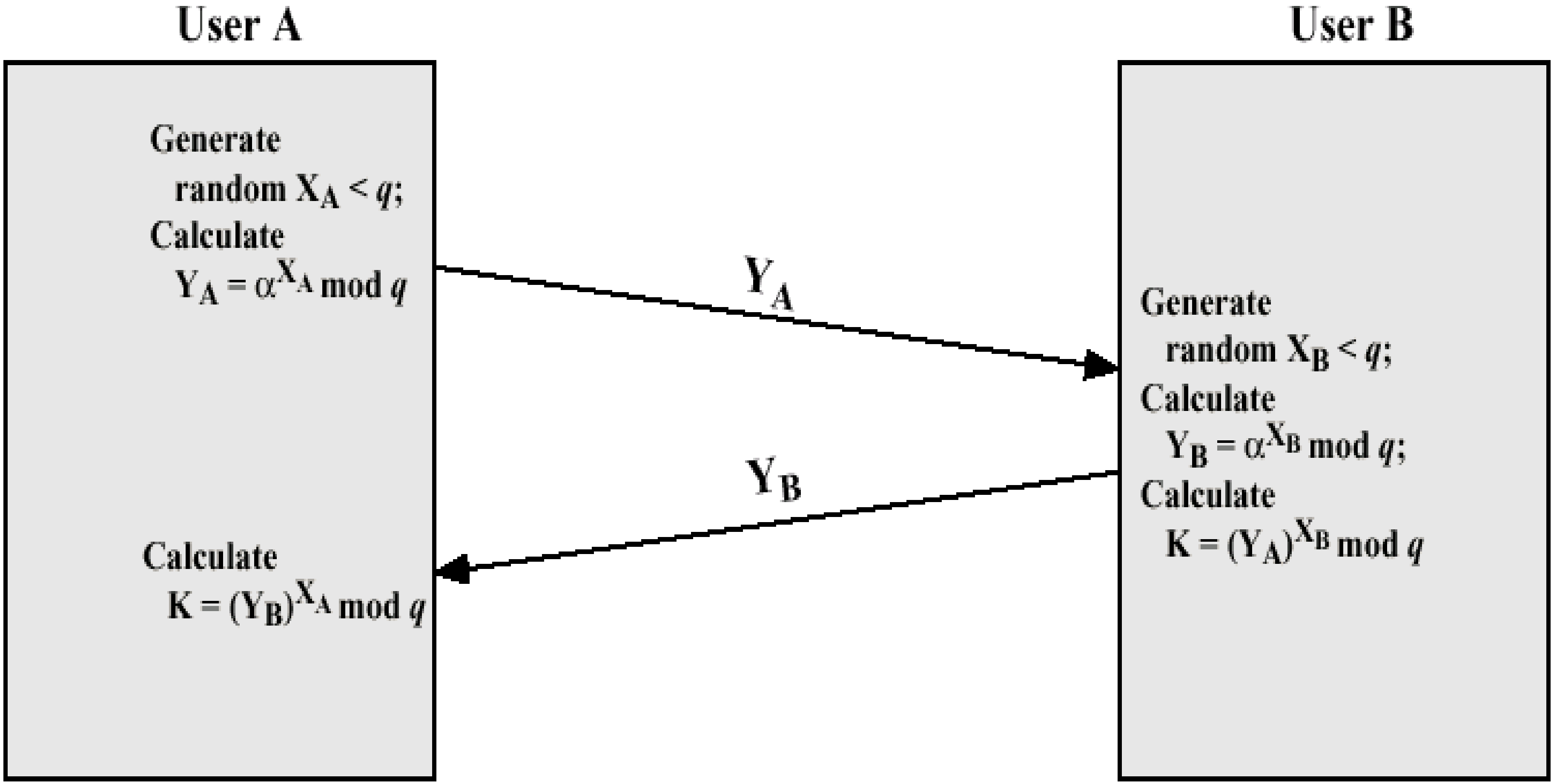


Diffie-Hellman Key Exchange

- Two Internet users, Alice and Bob wish to have a secure conversation.
  - They decide to use the Diffie-Hellman protocol



Diffie-Hellman Key Exchange



User A

Generate
random $X_A < q$;
Calculate
$Y_A = \alpha^{X_A} \bmod q$

Calculate
$K = (Y_B)^{X_A} \bmod q$

Y_A

Y_B

User B

Generate
random $X_B < q$;
Calculate
$Y_B = \alpha^{X_B} \bmod q$;
Calculate
$K = (Y_A)^{X_B} \bmod q$

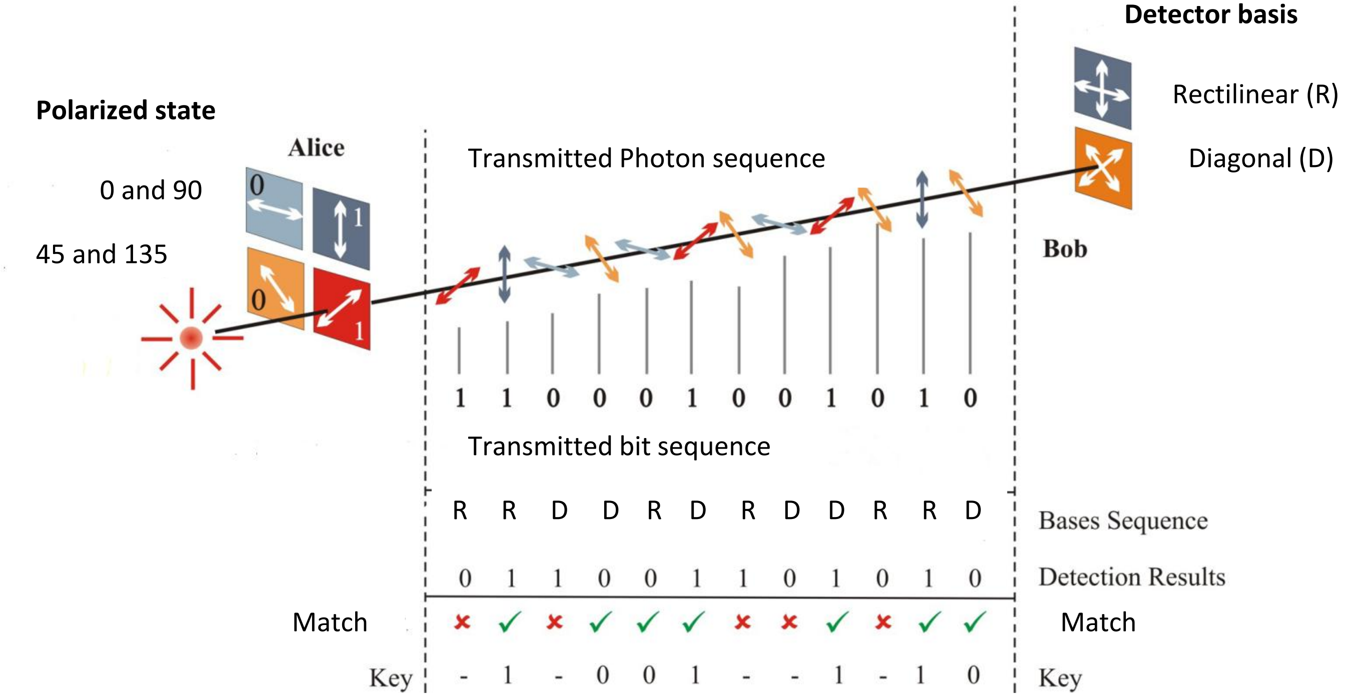
Security issues in Classical protocols / systems

- No true randomness in generated symmetric key
- Systems based on discrete logarithmic are not safe under quantum attack
- Man-in-Middle attack in D-H
- Trust on third party in case of Digital Signature certificate
- Signatures based on RSA or hardness of factorization of integers are not safe under quantum scenario.
- Therefore, there is a urgent need to design the quantum attack resistant key distribution protocols and digital signatures.

Quantum Key distribution (QKD)

- Quantum protocols are secured against any adversary.
- The only assumption: quantum mechanics.
- **Heisenberg's Uncertainty Principle** states that it is not possible to measure the momentum and position of a quantum particle with absolute precision.
- **Non-cloning theorem** states that it is impossible to make the identical copies of any quantum state.
- **Quantum cryptography** uses the photon particles on different bases for Quantum Key Distribution.

BB84 QKD Protocol



Transmitted bit sequence	1	1	0	0	0	1	0	0	1	0	1	0
Bases Sequence	R	R	D	D	R	D	R	D	D	R	R	D
Detection Results	0	1	1	0	0	1	1	0	1	0	1	0
Match	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓
Key	-	1	-	0	0	1	-	-	1	-	1	0

Horizontal and anti-diagonal polarization of photon represent the bit 0 and, vertical and diagonal polarization represent the bit 1

Bennett & Bessette Key Exchange Protocol

QKD Challenges

- Setup an error free key distributing environment-A Challenge.

- If measurements of Alice and Bob are not matching with each other then there is no way to decide whether mismatch is occurred due to presence of Eve or noisy & imperfect equipments.

.

- In year 2010, Lydersen et al. proved that in principle BB84 protocol is unconditionally secure but secrete key can be deduced if hardware implementation is faulty.

- Lydersen et al. blinded the avalanche photodiode-based detector and successfully inspected the secrete key without the notice of receiver.

- In Photon Number Splitting (PNS) attack, Eve split the photon and can keep extra photon with him. Eve can measure the stored photon at chosen basis and can deduce the key.

- To protect the PNS attack, there are variations of BB84 such as SARG04 which are resilient against the PNS attack

Post-Quantum Digital Signature

- The goal of post-quantum cryptography is to design the quantum attack resistant encryption, key management and signature schemes.

- National Institute of Standards and Technology (NIST) called the proposals for short listing of quantum resistant encryption, key management and signature schemes and their standardization.

Signature Category	**Signature schemes**
Lattice	1. CRYSTALS-DILITHIUM 2. FALCON 3. qTESLA
Multivariate Quadratic	4. GeMSS 5. LUOV 6. MQDSS 7. Rainbow
Hash-based	8. SPHINCS+ 9. Picnic

Round 2

Signature schemes **(Moved to round 3)**
1. CRYSTALS-DILITHIUM 2. FALCON 3. Rainbow

Round 3

Winner **(05 July 2022)**
CRYSTALS-DILITHIUM
FALCON will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large.

Standardization Result of Post-Quantum Schemes

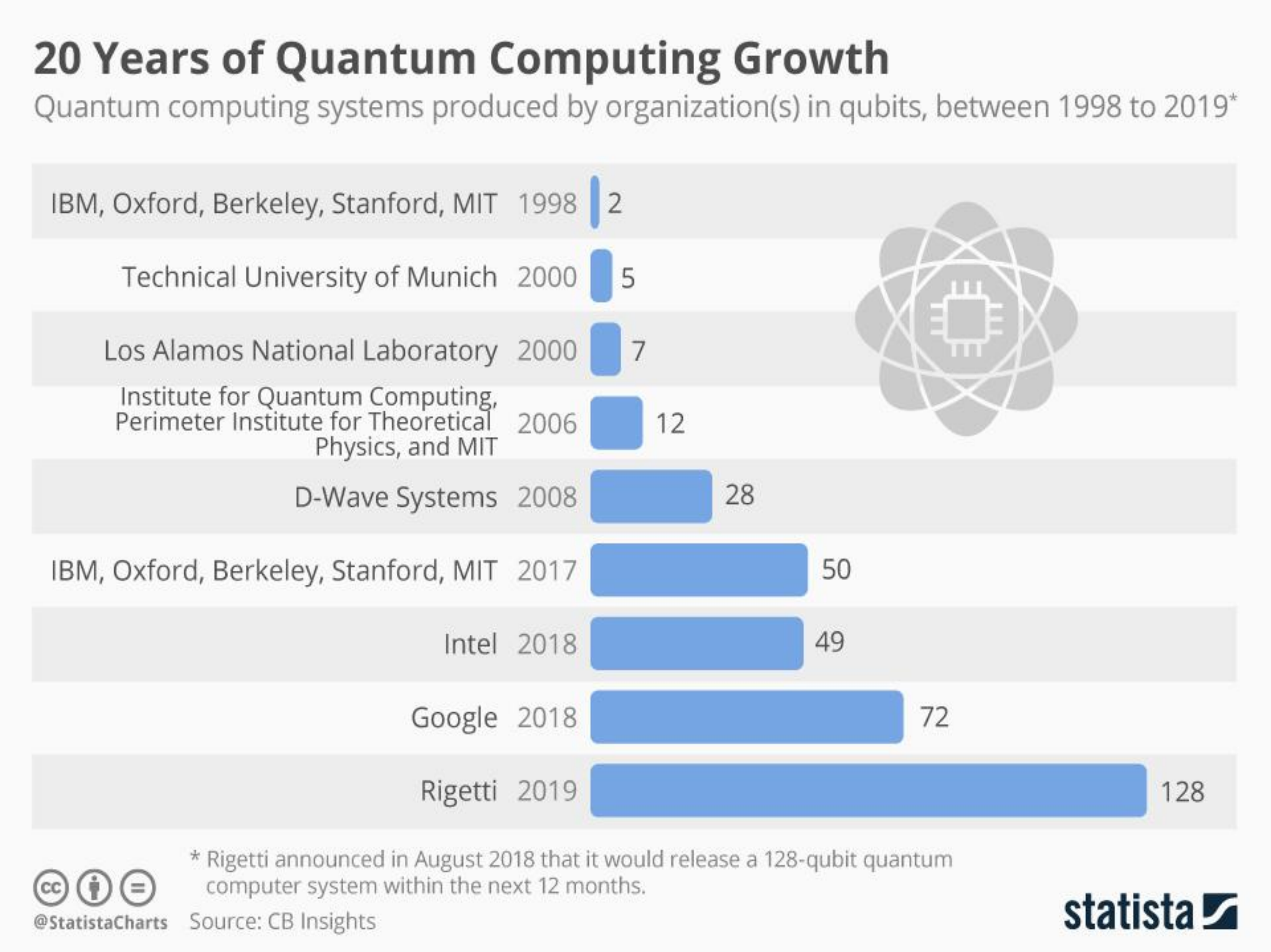
On 13th Aug, 2024, NIST approved three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography

- FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard

- FIPS 204, Module-Lattice-Based Digital Signature Standard

- FIPS 205, Stateless Hash-Based Digital Signature Standard

These standards specify key establishment and digital signature schemes that are designed to resist future attacks by quantum computers, which threaten the security of current standards.



Figures for Google and Rigetti were expected figures in 2018

Source: Statista

Development of Quantum Computers: Global Scenario

In 2018, IBM announced the development of a 53-qubit quantum computer and simulation of 56-qubit design.

Google has claimed (on 23rd October 2019) the quantum supremacy and announced the development of 53-qubits quantum computer.

Google group also claimed that a task that can be completed in 10,000 years on a fastest super computer of IBM, has been completed by their 53-qubit quantum computer in just 200 seconds only.

Intel also announced the development of 49-qubit superconducting quantum chip called 'Tangle Lake‘.

Microsoft is also a leading player in field of quantum computing, it is working on scalable quantum computer based on topological qubits.

In topological quantum computing, Microsoft is using electron fabrication technology which splits electron in two parts for making redundant qubit states.

Microsoft's aim is to create quantum states which are less vulnerable to quantum noise or interference.

Rigetti has also built up three quantum processors namely 16Q Aspen-1, 8Q Agave and 19Q Acorn.

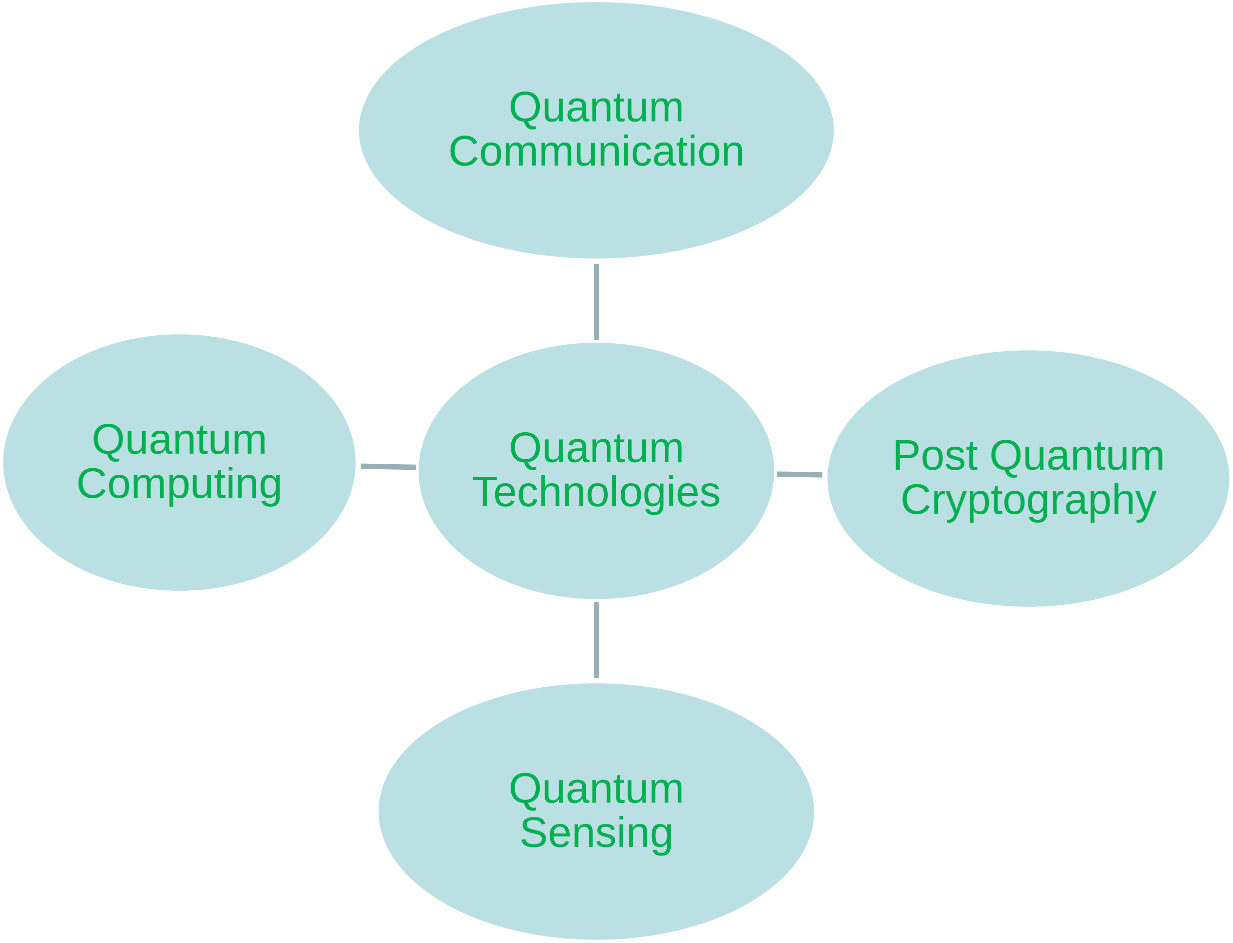
Regetti is offering quantum computing services through cloud.

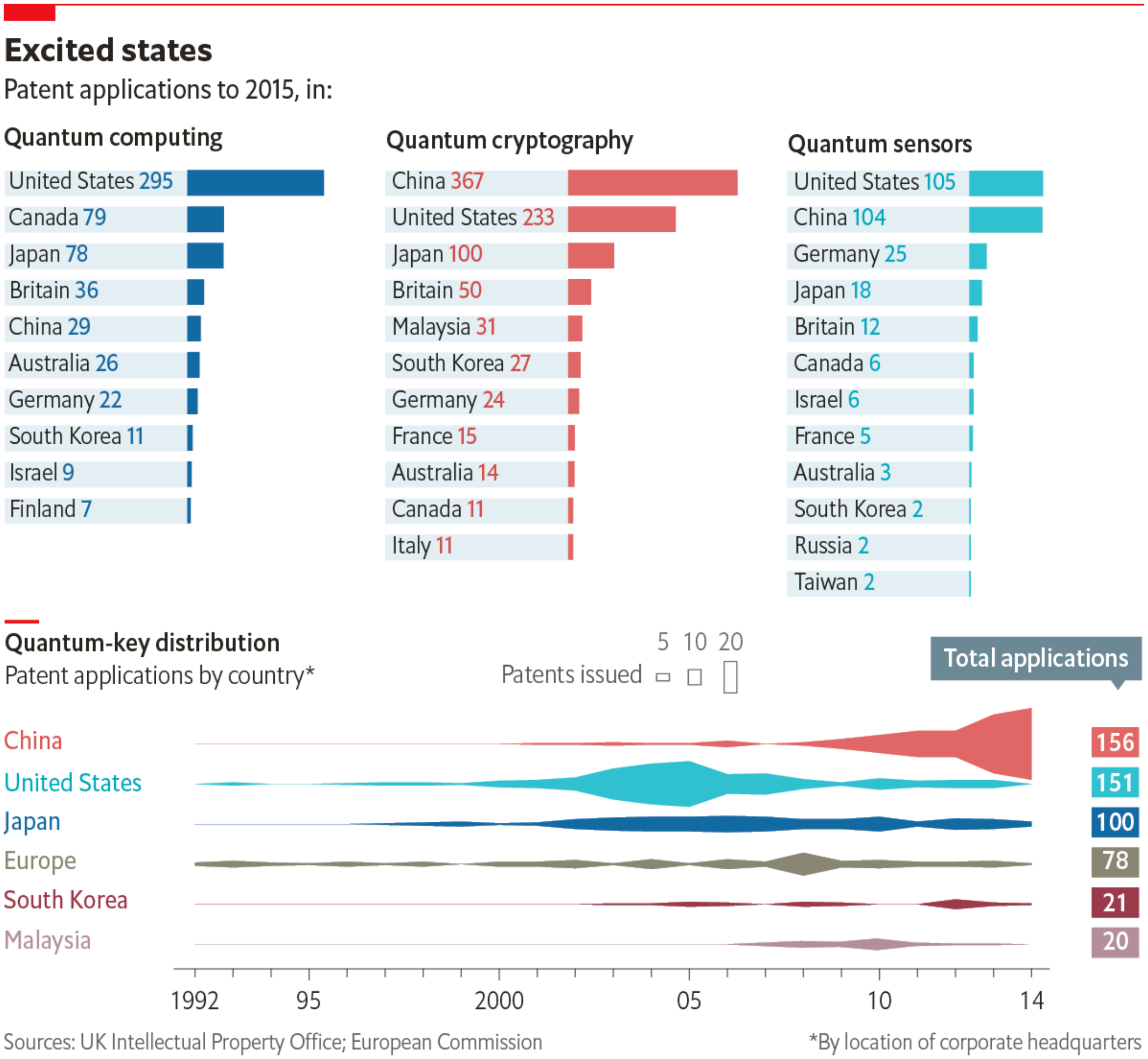
Possible applications of Quantum Computing

- Weather forecasting
- molecular comparison and simulation of chemical reactions for making medicines
- To understand the behavior of deadly virus like Covid-19 using a large database for next hundred years
- Optimization of transportation cost in field of operation research
- optimum assignment of jobs to a large population
- optimization of inventory cost at country level
- key distribution in cryptography
- To make a real time decision in financial sector

Areas	Applications
High-tech	ML & AI, Element Search, Algorithm optimization, Cyber Security, Online product marketing
Industrial goods	Logistics, Automotive, Aerospace, Simulation
Medical Industry	Bioinformatics, Catalyst and enzyme design, Pharmaceuticals R&D
Finance	Trading Strategies, Portfolio optimization, Risk Analysis, Fraud detection, Market Simulation
Energy	Network Design, Energy Distribution, Oil Well Optimization

Quantum Technologies





Source- UK Intellectual Property Office, European Commission

Quantum Computing research status in India

- Indian Government has boosted the quantum research by approving Rs. 6,000 crores in 2023 for quantum computing over a period of eight years. Proposal have been called under NQM mission.
- In India companies like IBM India, Qunu Labs, Automatski and Entanglement Partners are working in area of quantum computing.
- In 2017, Department of Science and Technology (DST) launched a quantum mission programme on Quantum Science and Technology called QuEST.
- In Quantum research, institutions like IISc Bangalore, TIFR Mumbai, IISER Pune, RRI Bangalore, IIT Kanpur etc are leading institutions in India

Quantum Implementing Approaches

- **Nuclear Magnetic Resonance Approach(NMR)**

  - uses spin states of nuclei as qubits within the molecules.

- **Ion Trap Approach**

  - ions/charged particles are confined in free space using electromagnetic field.

- **Neutral Atom Approaches**

  - cool down atoms and trap in the controlled environment.

- **Optical Approach**

  - photons are used to transfer the information from one place to another

- **Solid State Approach** (long decohrence time and scalability)

  - Example- silicon are electron spin in semiconductor quantum dot, chains of ^{29}Si nuclei etc.

- **Superconducting Approach**

  - pair of electron is cooled down to near 1 Kelvin. Superconducting approach works at macroscopic quantum phenomena, where population of paired electrons produces a coherent quantum state

Quantum Computing Challenges

- Prevention of Quantum attacks- Attacks on PKC systems, Key Distribution, Digital Signature.
- Development of reliable quantum hardware/devices.
- Development of Quantum Standards.
- Transformation from Classical to Quantum infrastructure.
- Practical implementation of theoretical quantum research.
- Unethical use of Quantum Cloud services to break classical systems.
- Skilled manpower

MeitY's initiative

1. Design and Development of Quantum Computing Toolkit (Simulator, Workbench) and Capacity Building.

2. Post-Quantum digital signature for document signing.

3. Creation of CoE for Quantum Technologies.

4. Femtosecond laser approaches to Quantum Information and Computation: towards a perfectly secure channel for robust and scalable information processing.

5. Setup of Quantum Computing Lab in collaboration of MeitY and Amazon Web Services (http://quantumcomputing.negd.in/).

Future Directions

- Manpower development programme need to be initiated at various engineering and science institutions in the country to develop trained manpower in the field of Quantum Technology.
- Short Term and Long Term courses may be initiated to train student in the field of Quantum Computing, Quantum Cryptography.
- Content on quantum security may be added in ‘Network and Security’ course for UG/PG students.
- To develop manpower in quantum programming, training on Quantum programming language like Q#, QisKit, Quantum Development Kit (QDK), Quantum simulations (Qasm, IQS, Staq, QuEST) etc may be given to students.
- Brain storming sessions/workshop/Seminar are need to be conducted.

Future Directions

- Establishments for fabrication of Quantum Devices, Superconducting Qubit Devices, sources and detectors for Quantum Communication.

- Focus areas should be R&D on Quantum Materials, quantum sensors, quantum communications, Quantum security and quantum simulations.

Focus Areas:

Quantum Algorithms

QKD

MQKD

Post-Quantum Digital Signature

Parallelism in Grover's algorithms etc.

Quantum Languages

Quantum Compiler

Thank You

Dr Om Pal
Mob: 8929874957
E-mail: opal@cs.du.ac.in