Quantum Technologies

C-DAC Patna

Outline of the Presentation

- Quantum Mechanics
- Quantum Computation
- Path entangled QRNG
- Post Quantum Cryptography

Quantum Mechanics

"Quantum" - Smallest possible quantity of some physical thing.

- Waves behave like particles
- Electrons(particles) behave like waves
- Wave-particle duality
- Black Body radiation
- Photoelectric effect

$$h\nu = E_2 - E_1$$

Energy is discrete

Quantum Mechanics

The discovery of Quantum Mechanics in the 20^{th} Century opened a new paradigm of Technological developments.

Phenomena in Quantum Physics:

- Superposition
- Entanglement
- Interference
- Heisenberg Uncertainty Principle

Bra-Ket notation

- It uses *angle brackets* and *vertical lines* for representation
- Bra-Ket notation or Dirac notation is used to denote quantum states
- Bra–ket notation is a notation for linear algebra and linear operators on complex vector spaces
- It is specifically designed to *ease* the types of *calculations* that frequently come up *in quantum mechanics*

$$\vec{v} = |v\rangle = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

$\lvert\psi\rangle$	*Ket*
$\langle\psi\rvert$	*Dual of Ket - Bra*
$\langle\varphi\vert\psi\rangle$	*Inner Product*
$\lvert\varphi\rangle\lvert\psi\rangle$	*Tensor product*

Quantum Mechanics Phenomena

- ***Superposition***

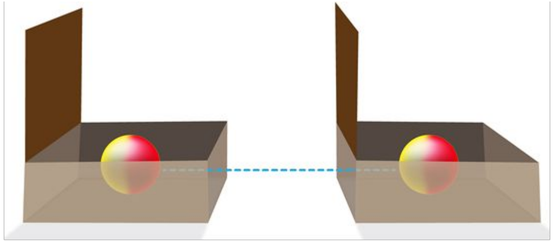
Superposition analogous to a spinning coin

The principle of quantum superposition states that if a physical system may be in one of many configurations—arrangements of particles or fields—then the most general state is a combination of all of these possibilities, where the amount in each configuration is specified by a complex number.

Quantum Mechanics Phenomena

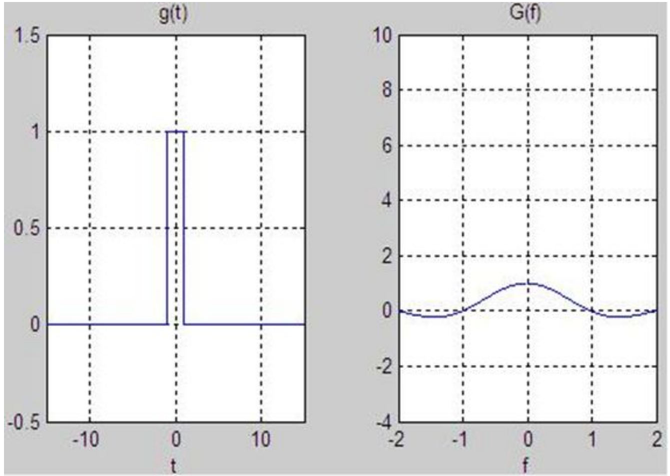
- ***Entanglement***

It is a physical phenomenon in which quantum states of two systems cannot be independent of each other. They essentially act as a single system.



Ball-Box analogy to explain entanglement

Quantum Mechanics Phenomena



- ***Heisenberg's Uncertainty Principle***

Two non-commuting variables cannot be measured simultaneously with exact precision.

Quantum Computation

- ***What is Quantum Computing?***

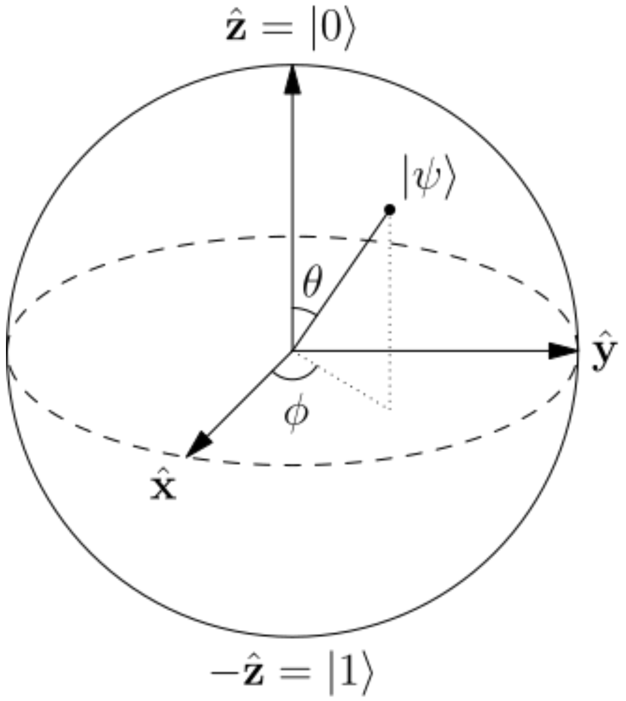
It refers to *computation utilising the principles of quantum physics*. The common principles applied in the computing system are the superposition, entanglement, and quantum interference.

A Quantum Computer is expected to perform well beyond the computational capability of a classical computer.

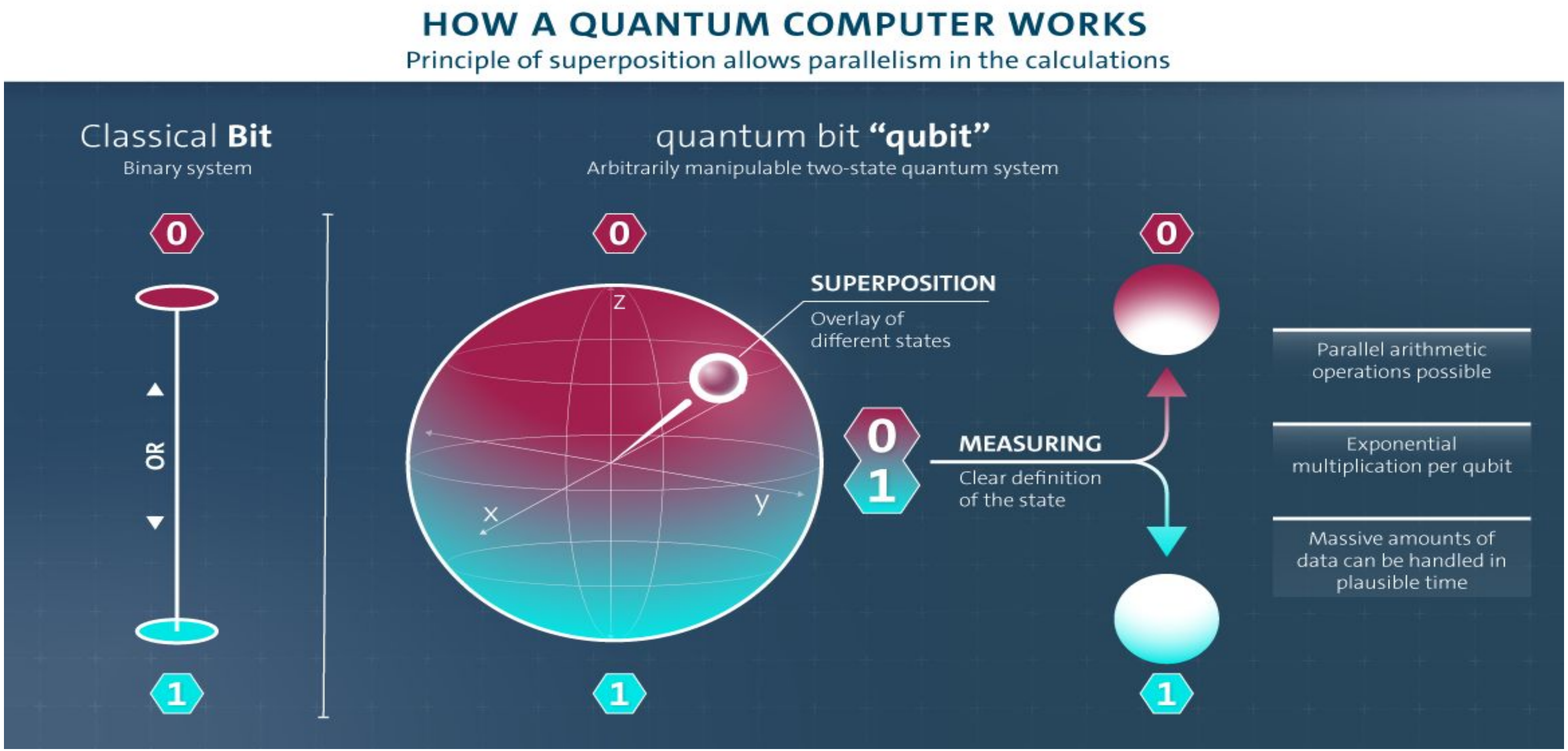
Qubits

- ***Qubits***
  Quantum bits are analogous to bits in a classical computer

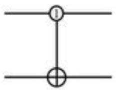
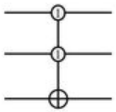
- ***Bloch Sphere***
  The Bloch sphere is a geometrical representation of the pure state space of a two-level quantum mechanical system (qubit)



Qubits versus Classical Bits

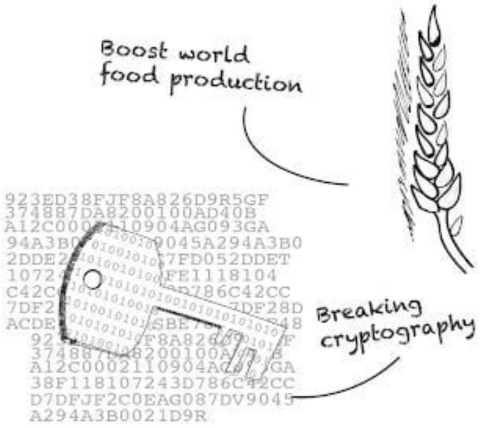


Quantum Gates

Gate	Equation	Matrix	Transform	Notation
Identity (I)	$I = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$I\|0\rangle = \|0\rangle$ $I\|1\rangle = \|1\rangle$	$-\boxed{\mathrm{I}}-$
Pauli-X (X or NOT)	$X = \|0\rangle\langle 1\| + \|1\rangle\langle 0\|$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$X\|0\rangle = \|1\rangle$ $X\|1\rangle = \|0\rangle$	$-\boxed{\mathrm{X}}-$
Hadamard (H)	$H = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}\langle 0\| + \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\langle 1\|$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$H\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $H\|1\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$-\boxed{\mathrm{H}}-$
Controlled-NOT (CNOT)	$\mathbf{CNOT} = \|0\rangle\langle 0\| \otimes I + \|1\rangle\langle 1\| \otimes X$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$\mathbf{CNOT}\|00\rangle = \|00\rangle$ $\mathbf{CNOT}\|01\rangle = \|01\rangle$ $\mathbf{CNOT}\|10\rangle = \|11\rangle$ $\mathbf{CNOT}\|11\rangle = \|10\rangle$	
Toffoli (T or CCNOT)	$\mathbf{T} = \|0\rangle\langle 0\| \otimes I \otimes I + \|1\rangle\langle 1\| \otimes \mathbf{CNOT}$	$\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{pmatrix}$	$\mathbf{T}\|000\rangle = \|000\rangle, \mathbf{T}\|001\rangle = \|001\rangle$ $\mathbf{T}\|010\rangle = \|010\rangle, \mathbf{T}\|011\rangle = \|011\rangle$ $\mathbf{T}\|100\rangle = \|100\rangle, \mathbf{T}\|101\rangle = \|101\rangle$ $\mathbf{T}\|110\rangle = \|111\rangle, \mathbf{T}\|111\rangle = \|110\rangle$	

- Basic circuits which operate on a few qubits
- *Building blocks for Quantum Circuits*, analogous to Logic gates in classical computers
- Reversible, unitary operators, described as unitary matrices relative to some basis (generally, Computational Basis)

Quantum Advantage

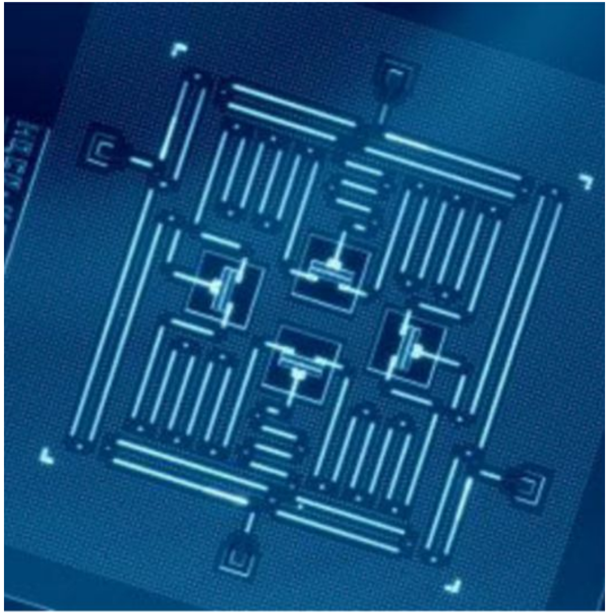


- A quantum computer can perform computations which no classical computer can perform at all — also referred to as *quantum supremacy*.

- Utilising *Quantum Superposition* through Qubits can potentially achieve Quantum Supremacy

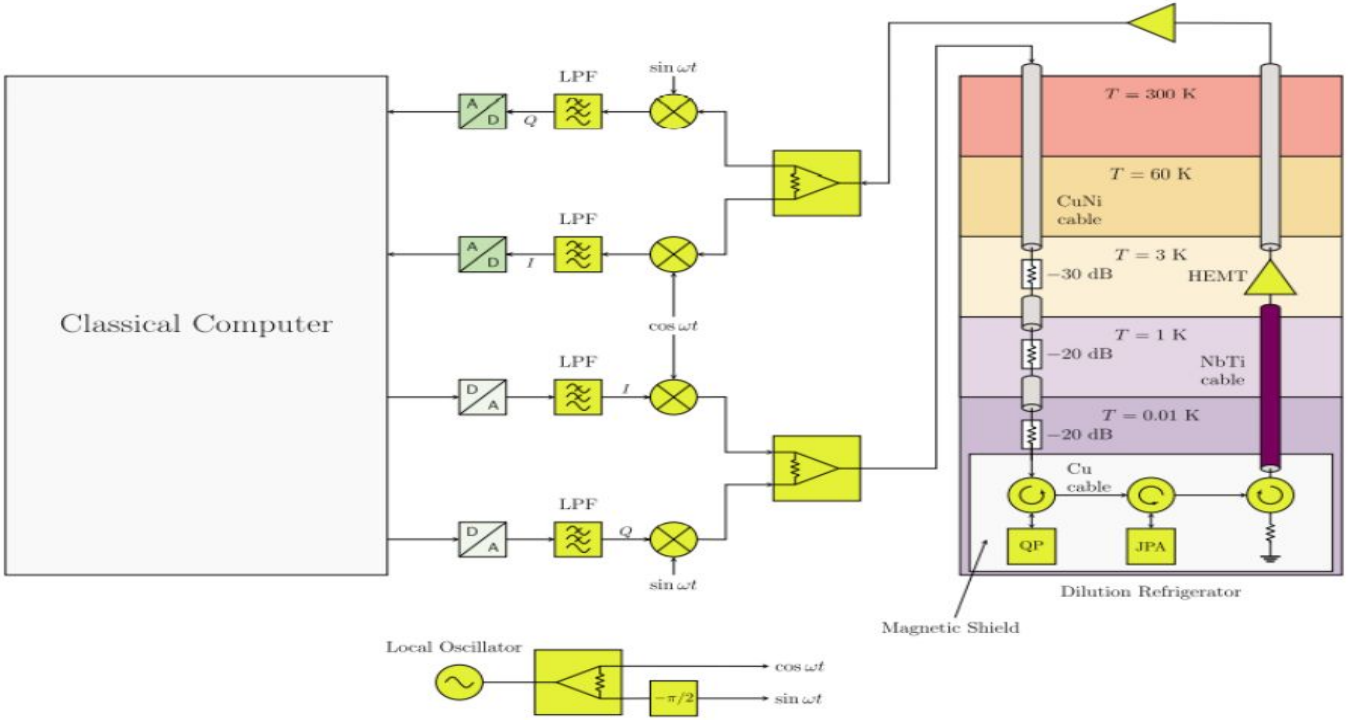
- The essence of quantum parallelism is the Hadamard transform, which can place a collection of qubits into a superposition of quantum states. In particular, k qubits can be placed into 2^k quantum states.

Superconducting Qubit Computers



- Using Superconducting Electronic Circuits, Quantum Computers are implemented
- *SQUIDS* - Superconducting Quantum Interference Devices
- Cryogenic Cooling is used to remove thermal noise
- *Josephson Junction* is the device at the heart of such chips

Superconducting Qubit Computer Schematic



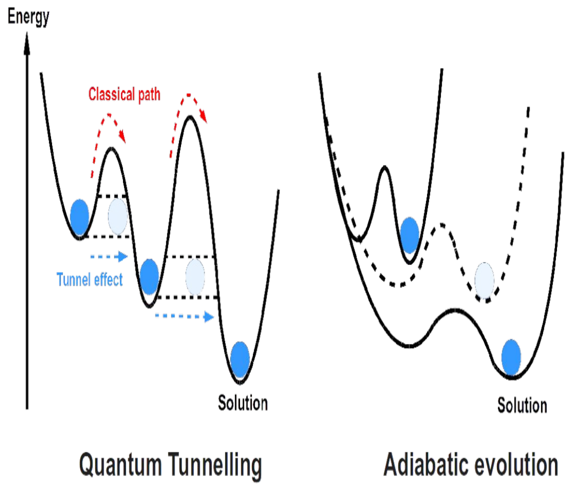
Annealing Based Quantum Computers

- Quantum Annealing is an *optimization process*.

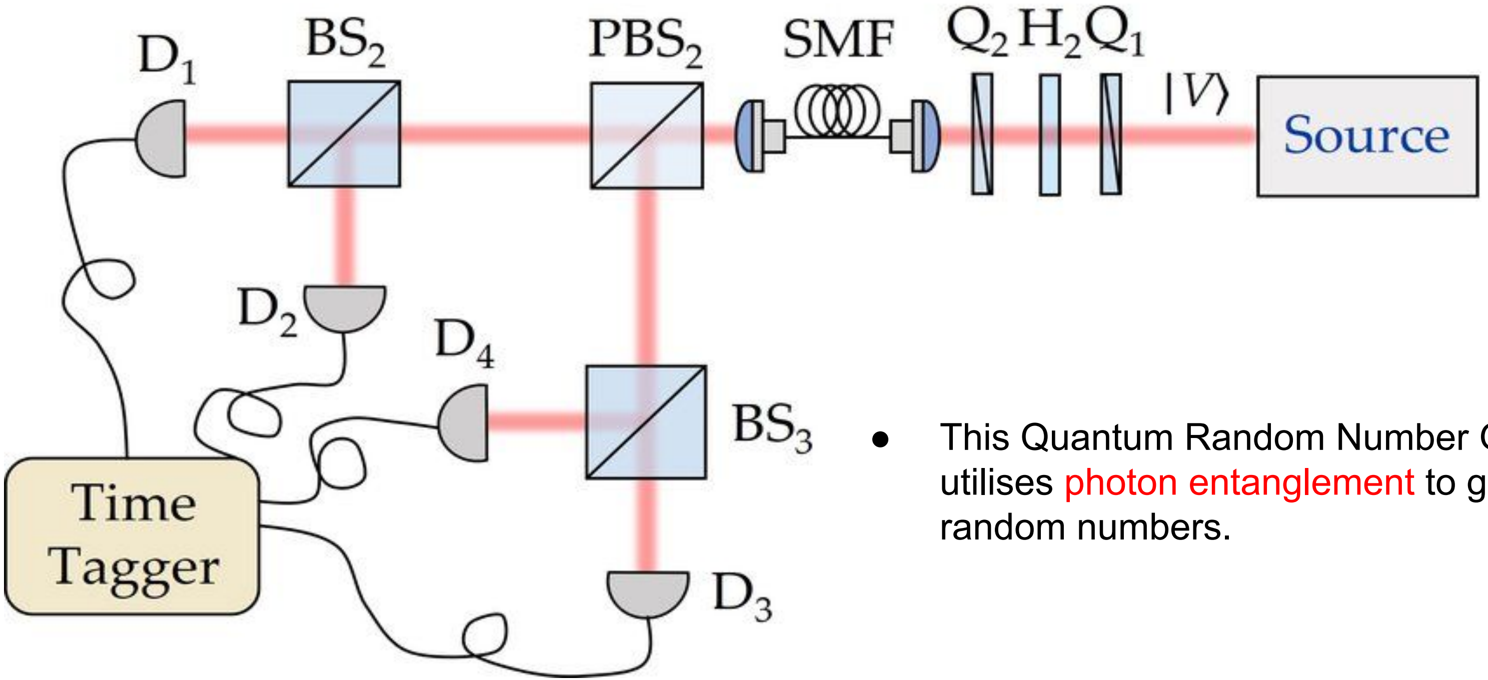
- It finds the *global minimum* of a given function over a given set of candidate solutions (candidate states) by a process using quantum fluctuations.

- System starts with superposition of all candidate states with equal weights.

- Following the time-dependent Schrödinger equation, a natural quantum-mechanical evolution of physical systems, *system evolves to the solution state*.

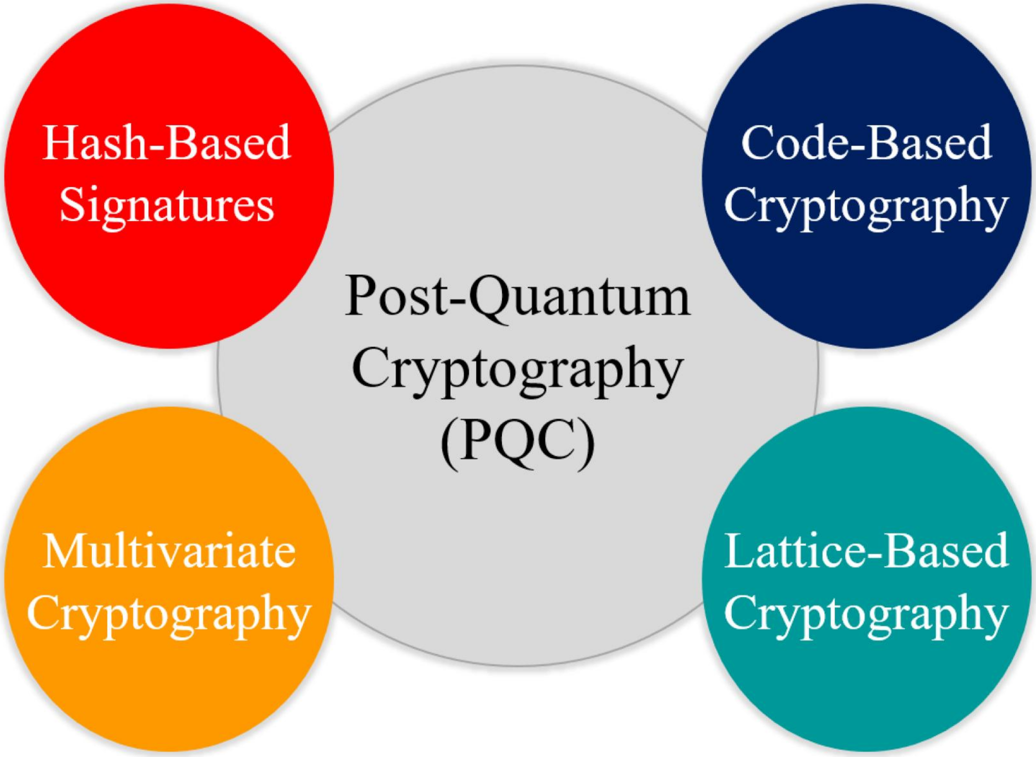


Path Entangled QRNG



- This Quantum Random Number Generator utilises photon entanglement to generate random numbers.

Post Quantum Cryptography (PQC)



Post Quantum Cryptography (PQC)

- ***Shor's Algorithm***

  - Peter Shor (1994)
  - Solves the *Integer Factorization & Discrete log problem in polynomial time* using Quantum Computers
  - Direct impact on public key cryptosystem such as RSA and Diffie-Hellman
  - A 2048-bit RSA would take a traditional computer about 6.4 quadrillion years
  - A Quantum computer with perfectly stable 4096 qubits will break RSA 2048 in 10 seconds.
  - Current State-of-the-Art: *IBM Eagle 127* qubit Quantum Computer

Post Quantum Cryptography (PQC)

- ***Grover's Algorithm***

  - Quantum Computers give $\sqrt{n}$ speed up on search problems
  - Halves the time complexity of search from $O(n)$ to $O(\sqrt{n})$
  - Can be applied for brute force search of cryptographic keys
  - The complexity of AES-128 key search reduces from 2^{128} to 2^{64}

Challenges

- ***To achieve Quantum Supremacy***

    - Translation of qubits to arbitrary values
    - Readable qubit for public use
    - Creating a scalable physical system that can support qubit number
    - Developing quantum gates that operate faster than the decoherence time
    - Creating spare parts that can handle the job

Thank You