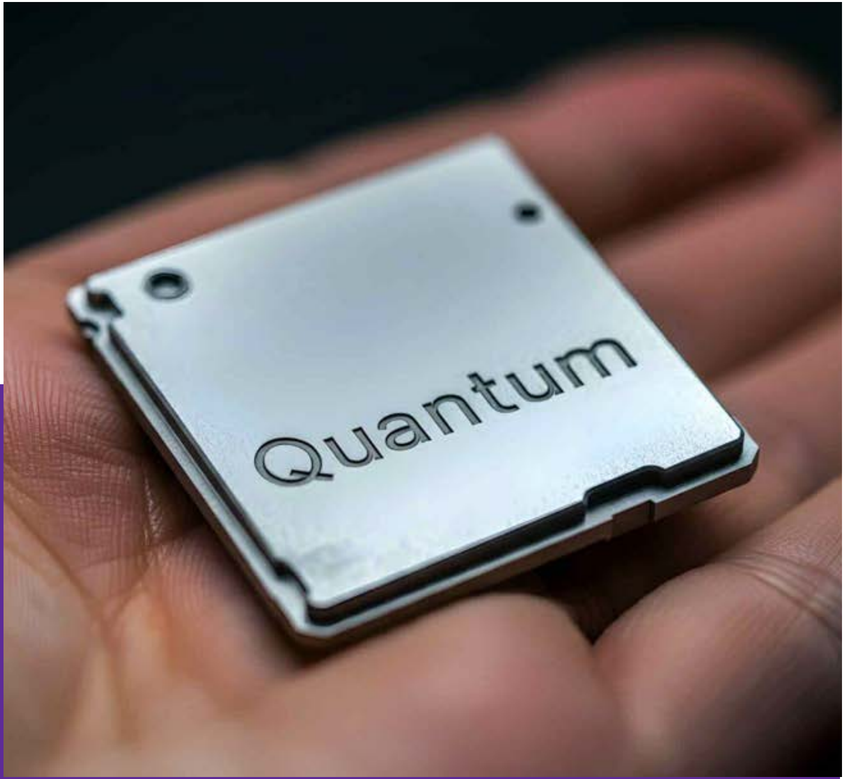
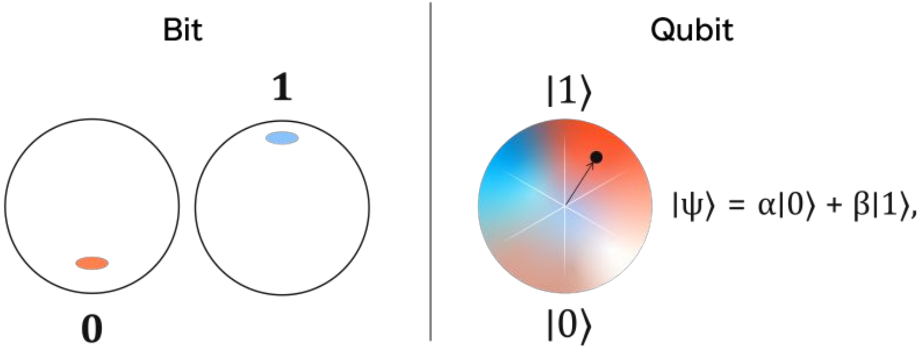
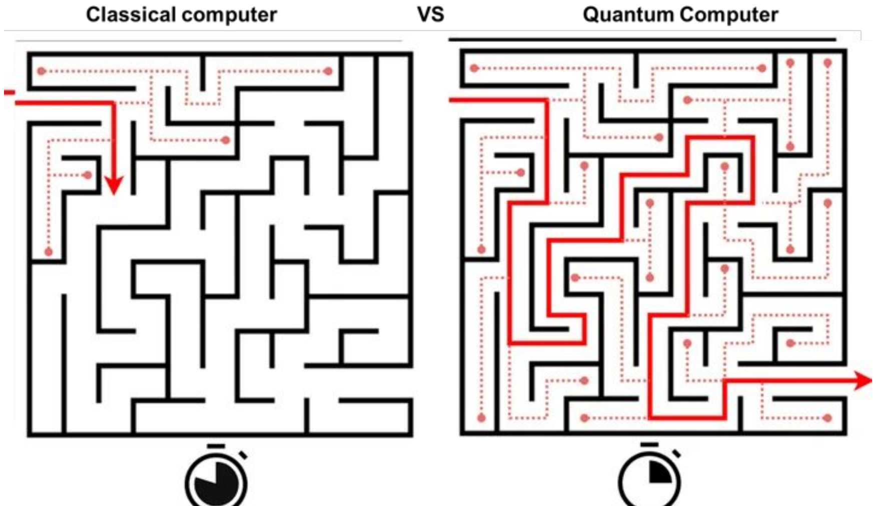
Quantum-Powered IoT: Unlocking the Next Era of Intelligence & Security



BY
GAYATHRI JEGAN MOHAN,
SOFTWARE ENGINEER AT MICROSOFT
AZURE IOT

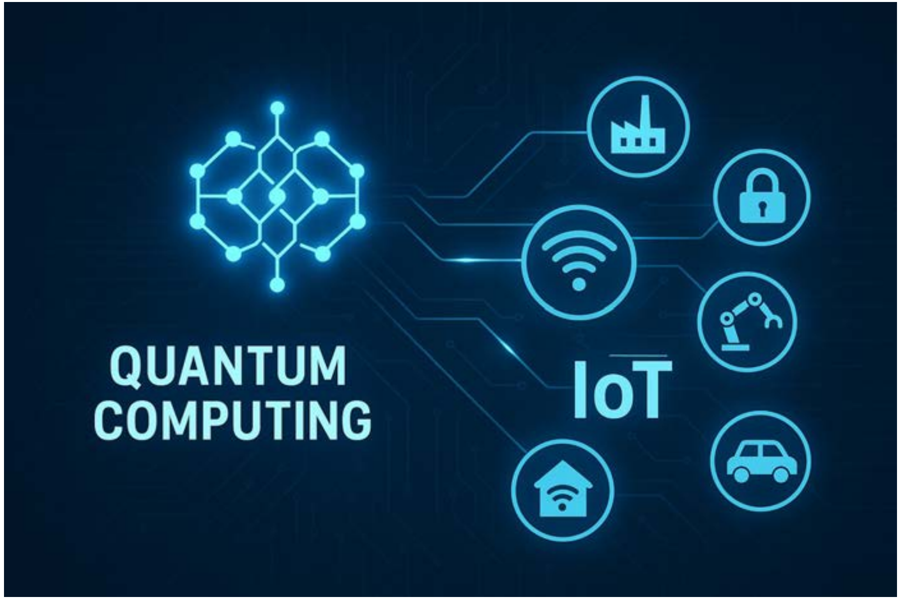
Quantum computing





- It uses **quantum mechanics** to process info way different than classical computers!
- Unlike classical bits of 0 and 1, quantum bits (qubits), **qubits exist in superposition** i.e state of 0 and 1 at the same time.
- **Entanglement** - state of one influences the state of other thereby a coordinated computation occurs

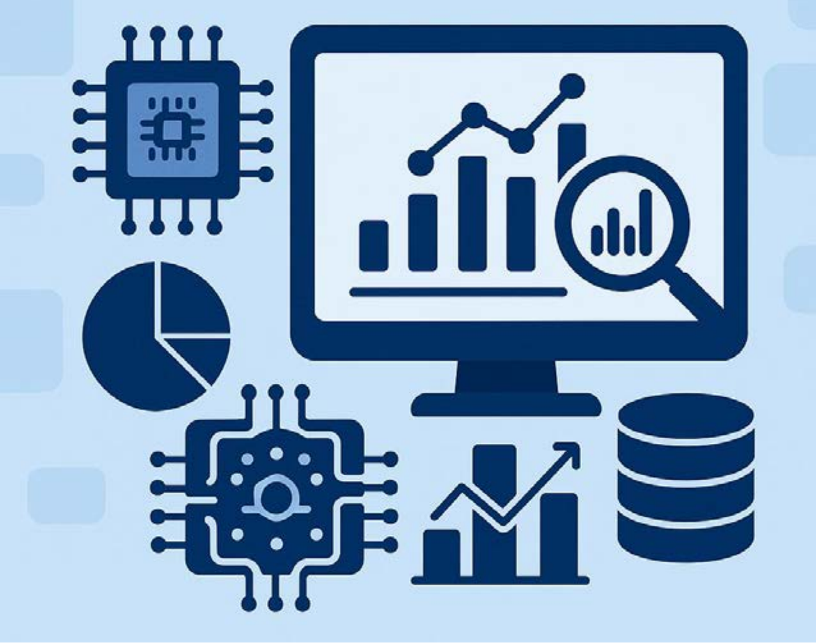
Quantum meets IoT



- Internet of things (IoT) faces some bottleneck challenges in the **2 major areas like intelligence and security.**
- Quantum computing can help in these 2 areas!
- Intelligence in 2 sub categories
    - **IoT Data Analytics**
    - **IoT Machine Learning**

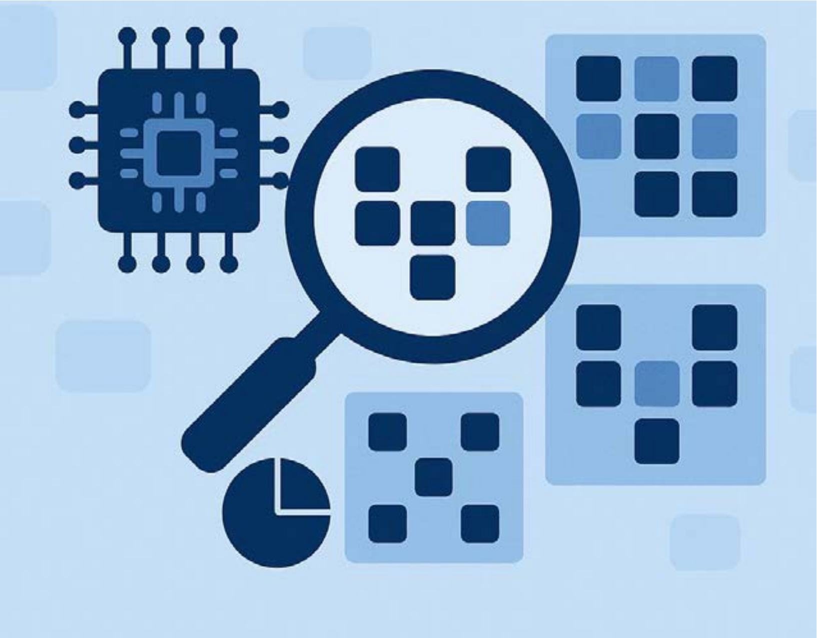
Quantum Computing in IoT Intelligence

Quantum Computing IoT Data analytics



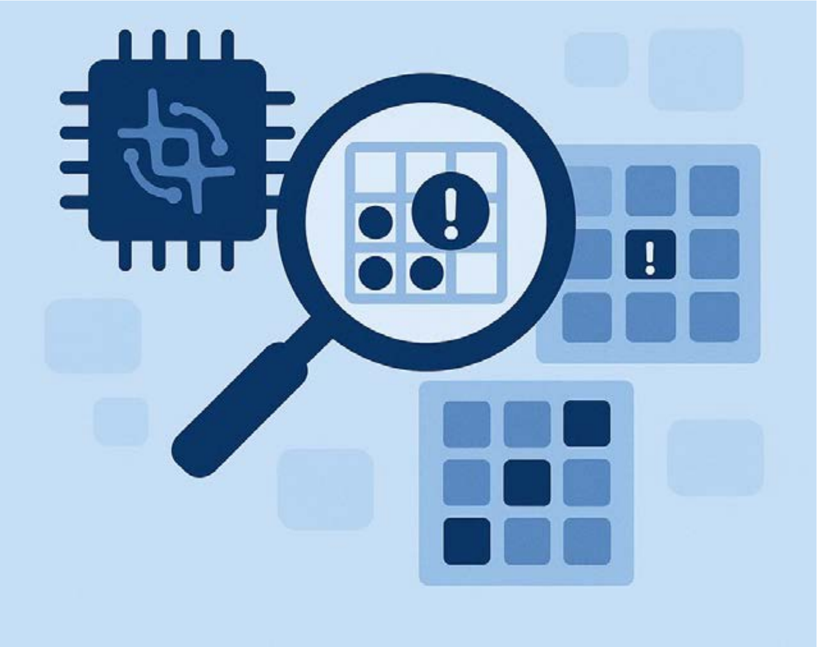
- Internet of things (IoT) generates **lots of data** that is not easy to analyze as they are **unstructured and noisy**
- With QC, it can **analyze** vast, **unstructured datasets** more efficiently as classical computers have memory & time constraints
- It can accelerate **anomaly detection**
- It also enhances **AI/ML model training** through QML (Quantum machine learning)

Quantum Computing IoT Data analytics for Pattern recognition



- Quantum algorithms like the **HHL algorithm** or **Quantum k-Means** can find patterns in data exponentially faster.
- **Volkswagen** used a quantum algorithm to detect traffic flow patterns and predict vehicle distribution in urban areas, helping optimize smart city traffic systems.

Quantum Computing IoT Data analytics for Anomaly detection



- By scanning multiple possibilities simultaneously, quantum systems can detect **outliers or rare events more accurately and quickly.**
- In cybersecurity, **Cambridge Quantum** developed quantum-enhanced anomaly detection tools to spot unusual patterns in **network traffic**—especially relevant in large-scale IoT networks.

Quantum Computing IoT Data analytics for Recommendation Systems

- Quantum-inspired algorithms can better model user-item interactions in sparse matrices, **enhancing personalization.**
- **Netflix and Amazon** researchers are exploring quantum-enhanced collaborative filtering models to improve content and product recommendations.

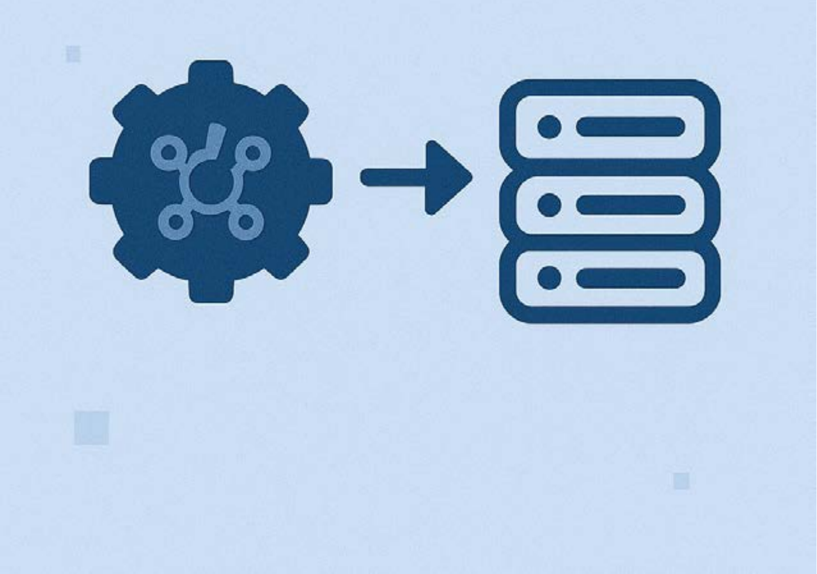
Quantum Computing IoT Data analytics for Fraud detection

- **Quantum Monte Carlo methods** provide faster and more accurate simulations for risk modeling and fraud detection from transactional datasets.
- **Goldman Sachs and JP** Morgan are investing in quantum computing to analyze market trends and detect anomalies in trades faster than current systems allow.

Quantum Computing IoT Data analytics for Bioinformatics

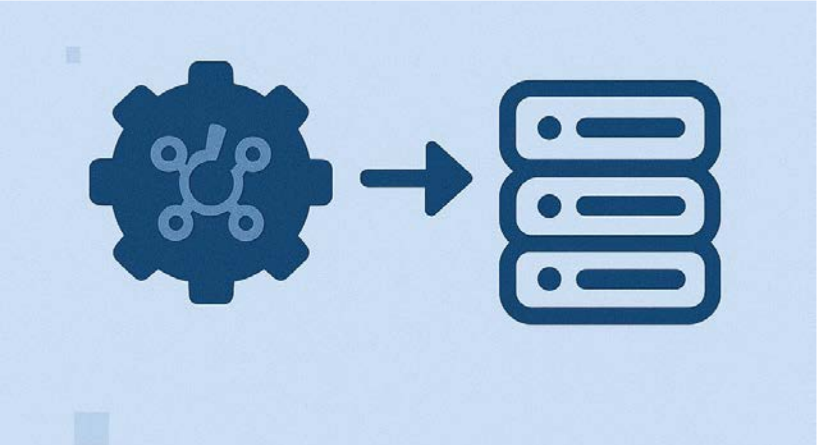
- Used in genomic sequence alignment or protein folding predictions, which are computation-heavy tasks.
- **D-Wave Systems** has collaborated with healthcare startups to accelerate **DNA analysis** workflows using quantum annealing.

Quantum Computing IoT Machine Learning



- Internet of things (IoT) faces bottlenecks in training, inference and also need real time processing
- IoT devices generate continuous, high velocity and often noisy data
- IoT devices have limited compute and energy
- There is increase in the need for real time decisions.

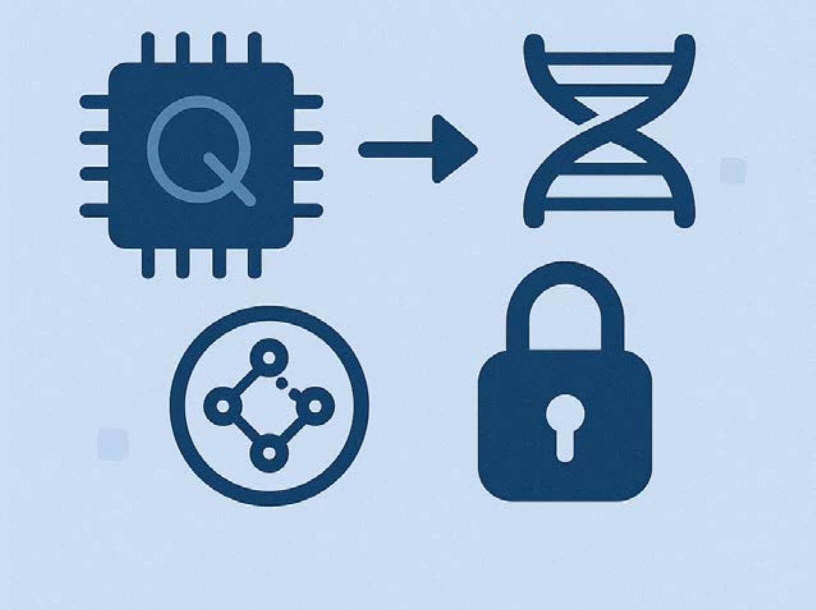
How Quantum Computing enhances IoT Machine Learning



- **Faster Training on Large Datasets**
  - Quantum Support Vector Machines and Quantum Kernel Estimation can reduce training M models thereby helps predictive maintenance
- **Handling high dimensional sensor data**
  - Multi sensor fusion in smart cities, agriculture, AV
- **Improves backend Inferencing**
  - with ML model optimization like Quantum Approximate Optimization Algorithm

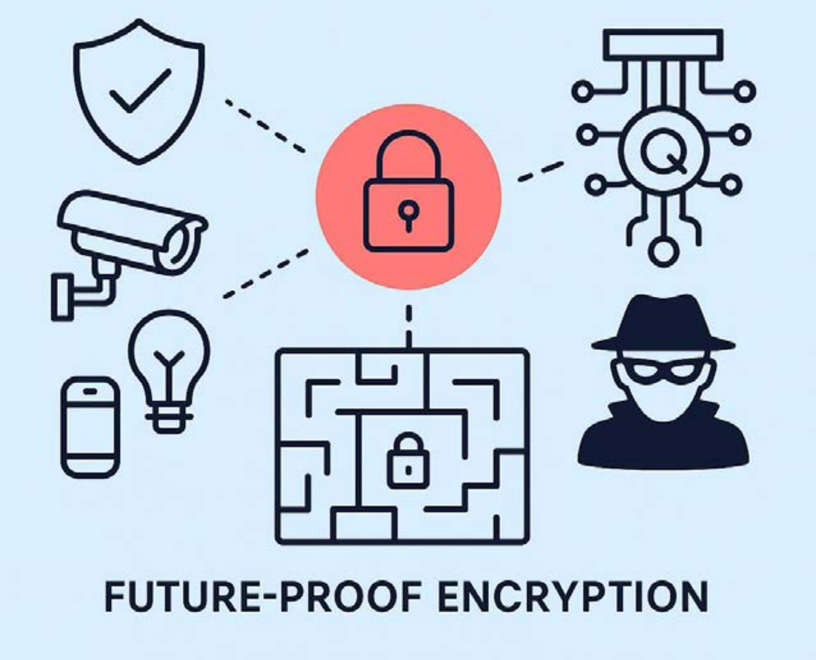
Quantum Computing in IoT Security

Quantum Computing IoT Security



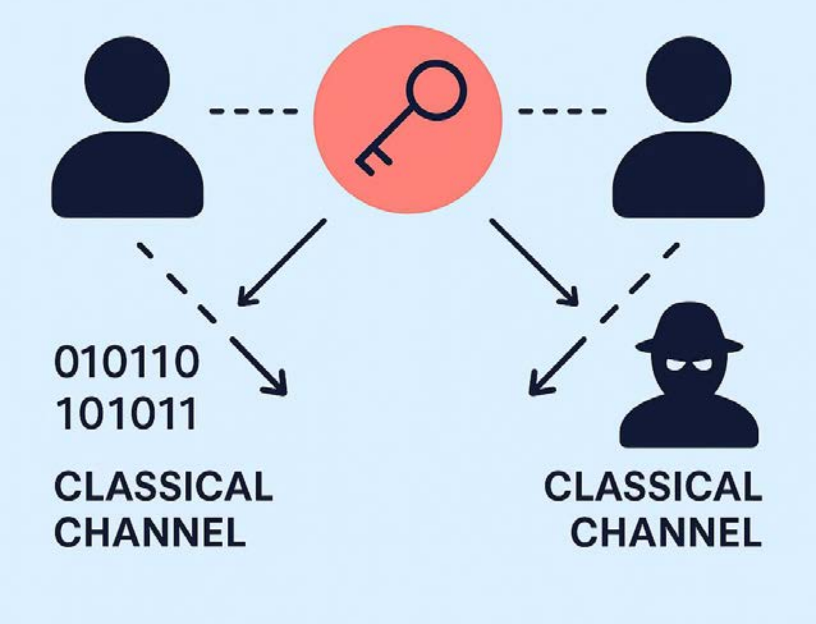
- It enhances IoT security by addressing critical vulnerabilities that classical cryptography and conventional IoT systems struggle with.
- 4 techniques are followed
  - **Defence against Quantum Attacks**
  - **Quantum Key Distribution**
  - **Quantum Random Number Generation**
  - **Tamper Proof Identity Management**

Defence Against Quantum Attacks



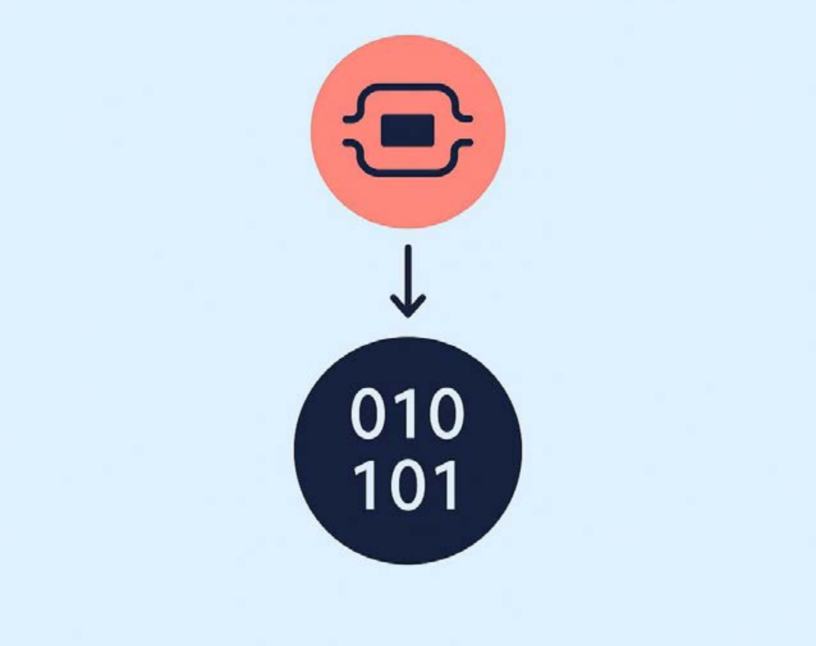
- IoT deployments often use **RSA, ECC, or AES**—all of which are vulnerable to Shor's algorithm on future quantum computers
- Quantum-safe protocols future-proof IoT ecosystems—especially those with long lifecycles (like vehicles, medical implants, or satellites).

Quantum Key Distribution



- A method of secure communication that uses the principles of quantum mechanics to exchange encryption keys.
- Guarantees detection of any eavesdropping (via quantum no-cloning theorem).
- Enables unbreakable key exchange between IoT devices and control centers.
- **Example**: Secure key exchange between autonomous vehicles and roadside units.

Quantum Random Key Generator



- Uses quantum phenomena to generate **truly random numbers.**
- Enhances encryption key strength, device authentication, and secure firmware updates.
- **Example**: QRNG for secure session initiation in industrial sensor nodes.

Tamper Proof Identity Management

Quantum-enhanced authentication methods (like quantum digital signatures) ensure:

- Devices are verifiable and not spoofed.
- Communication is traceable and non-repudiable.
- **Example:** In critical infrastructure, only authenticated, quantum-signed devices can send actuation signals (e.g., to open a valve or shut down a turbine).

Thank you!