सत्यमेव जयते

CRITICAL TELECOM INFRASTRUCTURE AND TELECOM & CYBER SECURITY

2nd Broadband India Summit

27 September 2024

TABLE OF CONTENTS

Pager Crisis in the Middle East

- Recent incidents related to the reported explosion of radiopagers in the Middle East should be given proper attention from the perspective of telecom network security.
- It appears that such an engineered explosion might have resulted from a breach of network security or unauthorised access. This could have altered the configuration of the pagers, ultimately leading to the explosion.
- Key issue is possible breach of network security.

Probable Trajectory

Altered configuration using radio techniques /compromised user devices

Gaining access to the Telecom Network

Acquiring control of network

Multiply incidences at once to cause damages etc.

Can we rely upon Trusted Products?

- ‘Rip and Replace' initiative
- Telecom equipment must come from 'trusted sources’

Recent incident raises pertinent issues about ‘trust’ ?

- If it relates to Critical Telecom Infrastructure, trust should be based on credible challenge to threat actors (Zero trust architecture)
- Trust and deterrence, both should continue to be effective

Threat To Telecommunications Networks

Cryptography is the mechanism used to encrypt bearer data while passing through communication channels and decrypted at the remote key using symmetric and asymmetric public and private keys. The following standards are in widespread use:

RSA: RSA-2048 could be broken by a quantum computer with around 4,000 stable qubits running Shor's Algorithm. Quantum computers can efficiently factor large numbers using Shor's Algorithm.

AES :

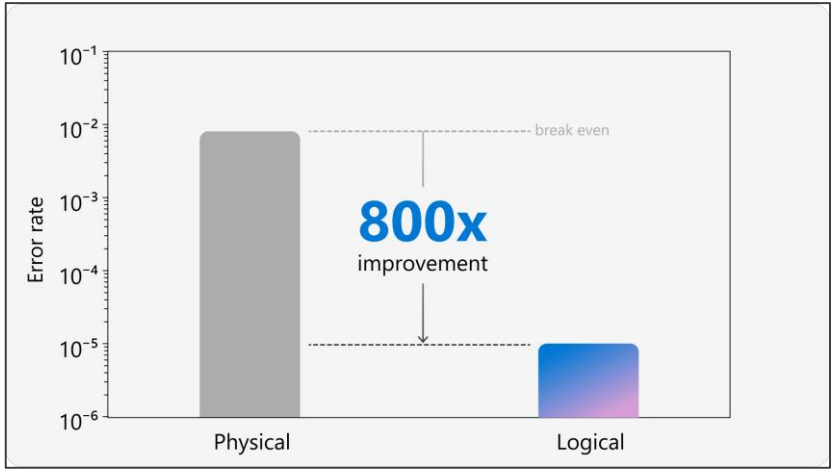
- A classical computer requires about 2^{128} operations to brute-force a 128-bit key.
- A quantum computer running Grover's algorithm reduces this to 2^{64} operations.

CRQC :

- risk due to a cryptanalytically relevant quantum computer (CRQC), time is limited !

RECENT DEVELOPMENTS IN RAW & LOGICAL QUBITS

- In April 2024**, Microsoft** and **Quantinuum** demonstrate the most reliable logical qubits on record with an error rate 800x better than physical qubits
- In Dec 2023, a quantum processor with **48 logical qubits** that can execute algorithms while correcting errors in real-time was unveiled in the US by Mikhail Lukin and colleagues at Harvard University, the Massachusetts Institute of Technology, and QuEra .
- In December 2023, IBM unveiled the world's first quantum computer with over 1,000 raw qubits (the "Condor" chip). This milestone represents a significant advancement in quantum computing.
- Previous quantum computing advancements by IBM:
  - 2022: **433-qubit** "Osprey" chip.
  - 2021: **127-qubit** "Eagle" chip.
- IBM is now focusing on improving error correction techniques to enhance the reliability and scalability of quantum computing for practical applications.

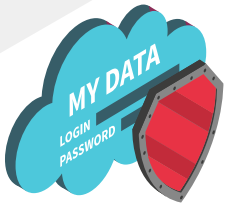


IBM: ~1000 Qubits

Google: 72 Qubits

Rigetti: 83 Qubits

Mitigation Strategies



Mitigation Strategies

- Software Based Approach
  - Post-Quantum Cryptography (PQC) Algorithms
    - Lattice Based Cryptography
      - *1. CRYSTALS-Kyber-FIPS 203*
      - *2. CRYSTALS-Dilithium-FIPS 204*
      - *3. FALCON*
    - Hash Based Cryptography
      - *4. SPHINCS+ FIPS 205*
    - Code Based Cryptography
    - Multivariate Polynomial Cryptography
- Hardware Based Approach
  - Quantum Key Distribution (QKD)
- Hybrid Approach
  - PQC + QKD

QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography

Quantum-safe cryptographic systems, also known as post-quantum cryptography, are designed to be resistant to attacks from both classical and quantum computers. These systems use algorithms that are believed to be secure even against quantum computers. Quantum-safe cryptography is becoming increasingly important as quantum computers continue to evolve and become more powerful.

Quantum Key Distribution

Quantum key distribution (QKD) system is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt & decrypt messages.

STANDARDIZATION EFFORTS IN PQC

NIST's (National Institute of Standards and Technology, US) Role in PQC:

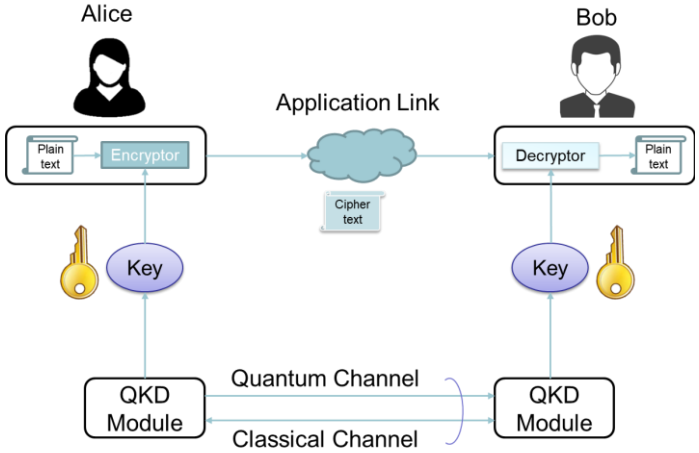
- In 2016, NIST launched a multi-phase, public evaluation process to standardize quantum-resistant algorithms.
- Submissions were invited across various categories, including encryption (key establishment), digital signatures, and hash functions.
- NIST initially received 82 proposals, which were narrowed down through rigorous evaluation processes.

- The evaluation process was divided into several rounds:
  - ✓ **Round 1**: In 2017, NIST announced the first round of 26 candidates for further consideration.
  - ✓ **Round 2**: In 2019, NIST selected a subset of candidates 7/8 for deeper analysis, focusing on those with strong security and performance characteristics.
  - ✓ **Round 3**: In 2020 and 2021, NIST refined its evaluations, involving extensive cryptographic analysis and public feedback.

- Following this five-year evaluation process, NIST selected 4 algorithms for standardization in 2022 as part of its Post-Quantum Cryptography (PQC) Standardization Process:
  - **Lattice-Based**: CRYSTALS-Kyber (ML-KEM) (FIPS-203), CRYSTALS-Dilithium (ML-DSA) (FIPS-204), and FALCON (ML-DSA)
  - **Hash-Based**: SPHINCS+ (SLH-DSA) (FIPS-205)
- In Aug 2024, NIST released the first 3 finalized Post-Quantum Encryption Standards
- ML-Module Lattice, KEM-Key Encapsulation Mechanism, FIPS-Federal Information Processing Standards

QUANTUM KEY DISTRIBUTION (QKD)

- QKD is a method for securely exchanging cryptographic keys using quantum mechanics. It ensures that the keys used for encryption are transmitted securely between parties.



Benefits of QKD:

- Provides security based on the laws of quantum physics, making it immune to attacks from future quantum computers.
- Any interference in the key exchange is detectable, ensuring the integrity and confidentiality of the key.

Limitations of QKD:

- Dedicated Hardware Needed: QKD relies on specialized equipment (e.g., dedicated fiber, free-space transmitters) and cannot be implemented as software or easily integrated with existing networks.
- Security is based on hardware and engineering, not just theoretical physics, making it difficult to validate and prone to vulnerabilities.
- DOS Risk: QKD's theoretical basis makes it vulnerable to denial-of-service attacks due to its sensitivity to eavesdropping.

US-Migration to post-quantum cryptography (PQC)

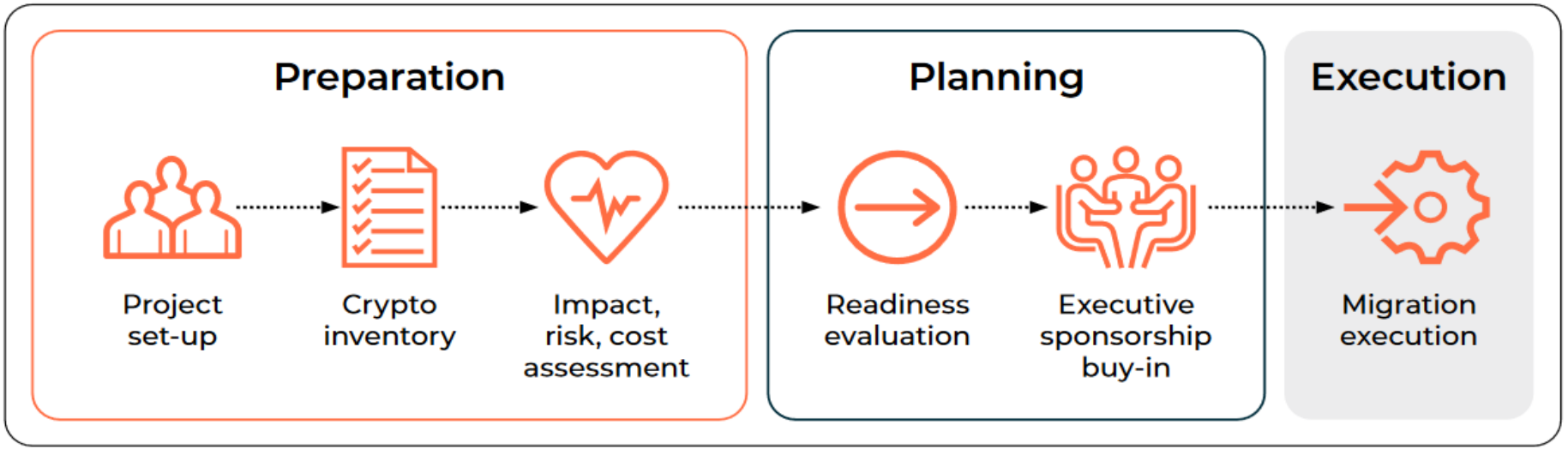
Quantum Computing Cybersecurity Preparedness Act 2022 (US)

- ✓ Strategy for addressing risk due to a CRQC
- ✓ Estimated funding required for migration to PQC
- ✓ Developing standards for PQC adoption

Crypto agility

Crypto implementations should allow for easily changing the algorithms used.

Within 10 years only



US-Migration to post-quantum cryptography (PQC)

Whats' the hurry ?	What are the speed-brakers ?
- Advent of CRQC possible before 2030 - Migration process is long-drawn process - Sensitive data needs long-term protection - Threat actors store data now to harvest it later.	- Standardisation is on the way in select destinations - Network Protocols not ready yet - Comprehension- & skill- gap - Interoperability risk - Certifications to be developed & adopted

- ✓ **Prioritise the components with a high risk of being attacked or with a high damage potential.**
- ✓ **The riskiest items should be migrated first, then followed by less critical components.**

European Commission's Recommendation on Migration

April 2024

- ✓ encourage Member States to develop and implement a harmonised approach as the EU transitions to post-quantum cryptography (PQC).
- ✓ implement a harmonised approach as the EU transitions to PQC
- ✓ develop a Coordinated Implementation Roadmap addressing the transition to PQC within 2 years
- ✓ EU approach should address respective sovereign requirements under one-market principle
- ✓ interoperability between countries, allowing systems and services to function seamlessly across borders is crucial.

Developments at the National Level

NATIONAL QUANTUM MISSION (NQM)

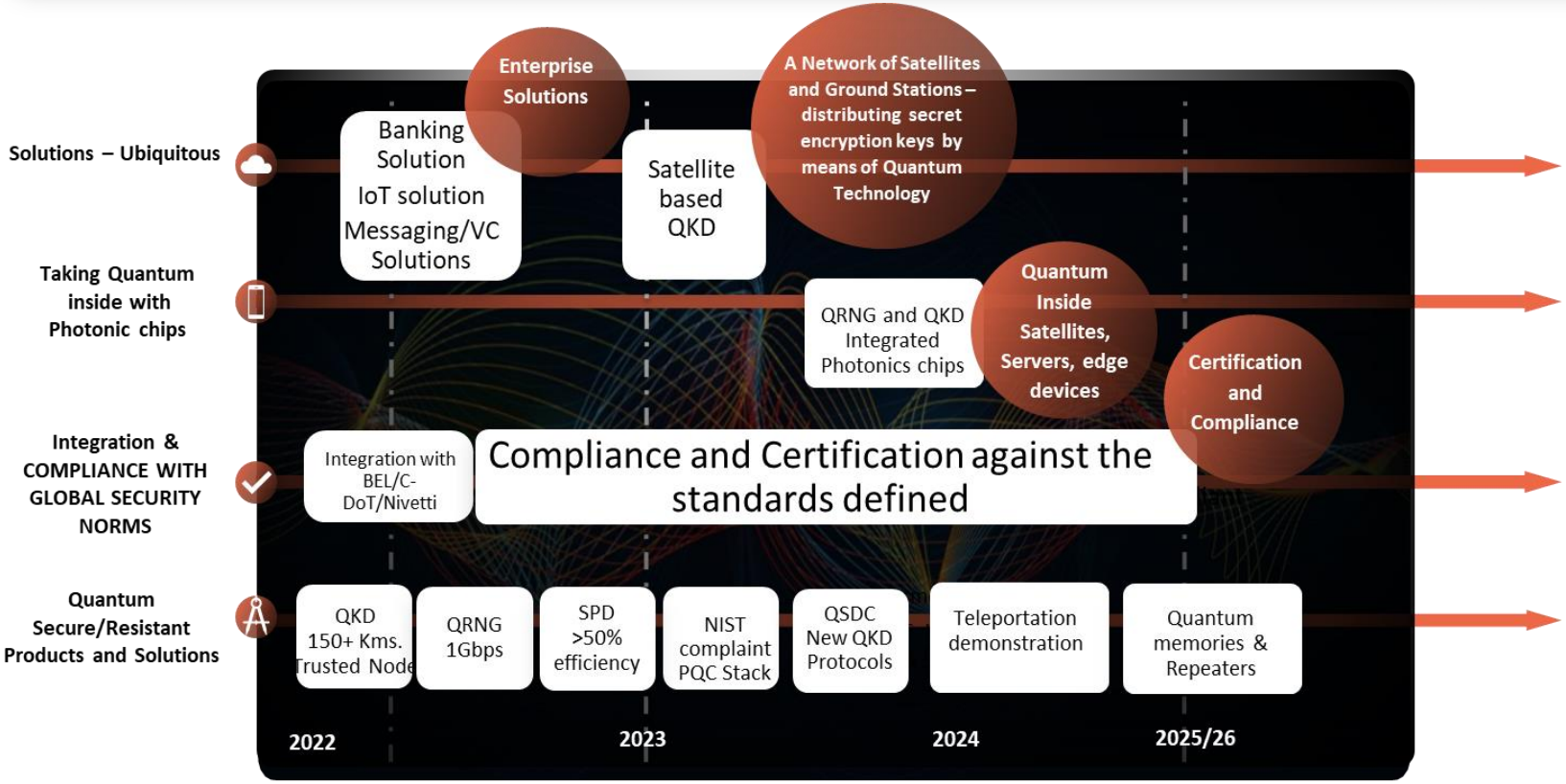
- The Union Cabinet approved NQM on 19th April 2023 at a total cost of **Rs.6003.65 crore** from 2023-24 to 2030-31.

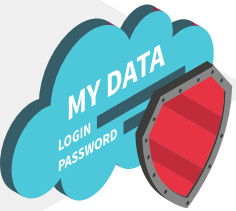
- **Mission Goals:**
  - **Development of Quantum Technologies (QT):** Seed, nurture, and scale scientific and industrial R&D
  - **Global Competitiveness:** Position India among leading nations in Quantum Technologies & Applications (QTA)

- **Key Objectives:**
  - Develop quantum computers with 50-1000 physical qubits in 8 years
  - Satellite-based secure quantum communication across 2000 km
  - Inter-city quantum key distribution and multi-node quantum networks

- **Four Thematic Hubs (T-Hubs) in Top Institutes:**
  1. Quantum Computing
  2. Quantum Communication
  3. Quantum Sensing & Metrology
  4. Quantum Materials & Devices

QUANTUM COMMUNICATION R&D ROADMAP





National Digital Communications Policy, 2018

Goals under Secure India Mission :

a) Establish a comprehensive data protection regime for digital communications that safeguards the privacy, autonomy and choice of individuals and facilitates India's effective participation in the global digital economy.

b) Ensure that net neutrality principles are upheld and aligned with service requirements, bandwidth availability and network capabilities including next generation access technologies.

c) Develop and deploy robust digital communication network security frameworks.

d) Build capacity for security testing and establish appropriate security standards.

e) Address security issues relating to encryption *and security clearances.*

f) Enforce accountability through appropriate institutional mechanisms to assure citizens of safe and secure digital communications infrastructure and services.

THANKS