Quantum Security **Overview**

National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

A JOINT INITIATIVE BY

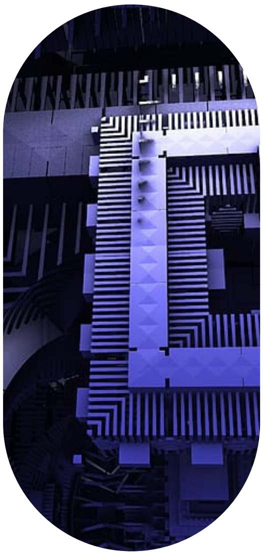
DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

सत्यमेव जयते
Ministry of Electronics &
Information Technology
Government of India

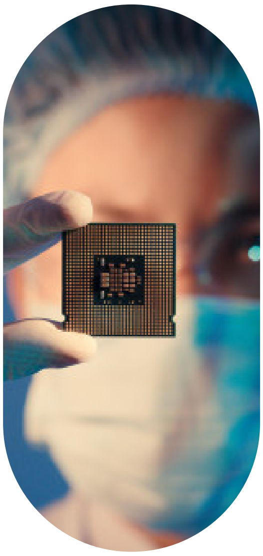
Quantum Security

With the advancements in the field of Quantum Computing, organizations now have the ability to conduct complex mathematical computations at lightning fast speed. Though quantum computing is a boom for the major part, it also brings with it, its own set of challenges for cyber security professionals. With quantum computing, breaking a standard cryptographic encryption algorithm becomes simple for an attacker. To tackle with this threat, quantum cryptography offers a solution. Quantum Cryptography relies on the fundamental Heisenberg Uncertainty Principle. What makes Quantum Security secure is because of the principle that if an eavesdropper tries to intercept keys during the communication, some of the anomalies get introduced in the photon's polarity thereby signaling a compromised communication. Once the anomaly is detected, the communication is aborted.

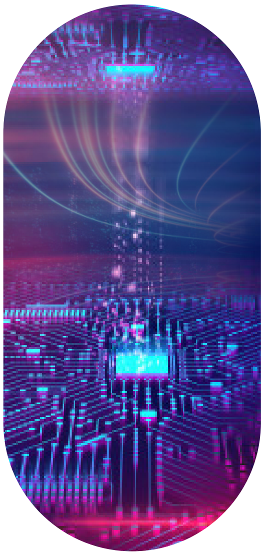
Challenges in Quantum Security:



Quantum Communication happens primarily through Dark fiber net, therefore limiting the distance at which the communication can be carried out.



The setup cost for establishing a quantum secure channel, infrastructure and hardware continues to be steep.



Key regeneration speed should be enough to ensure true randomness.

Bulky / non-portable hardware equipment.

Organizations have solutions in the following categories:

01 Portable solutions for Quantum Cryptography: Optimized for Mobile Phones, Cryptography on contactless security chip.

02 Quantum Key Distribution without distance limitation: using shared fiber network

03 Random Number Generator

04 Quantum Key Distribution

05 Quantum Entropy Enhancer

06 Random Number as a Service

Quintessence Labs

Centralized enterprise key and policy management solution, True Random Number Generator, and Entropy Enhancer.

1. Quantum Random Number Generator

- Delivers Random Numbers through the industry standard OASIS Key Management Interoperability Protocol (KMIP).
- Generates perfectly unpredictable random numbers, derived from a quantum source.
- QRNG at the speed of 1 Gbit/second.
- Provides encryption keys with full entropy.
- Satisfies NIST SP 800-22 (NIST STS), FIPS 140-2 Level 3 cryptographic modules and Dieharder tests.

2.Quantum Entropy Enhancer

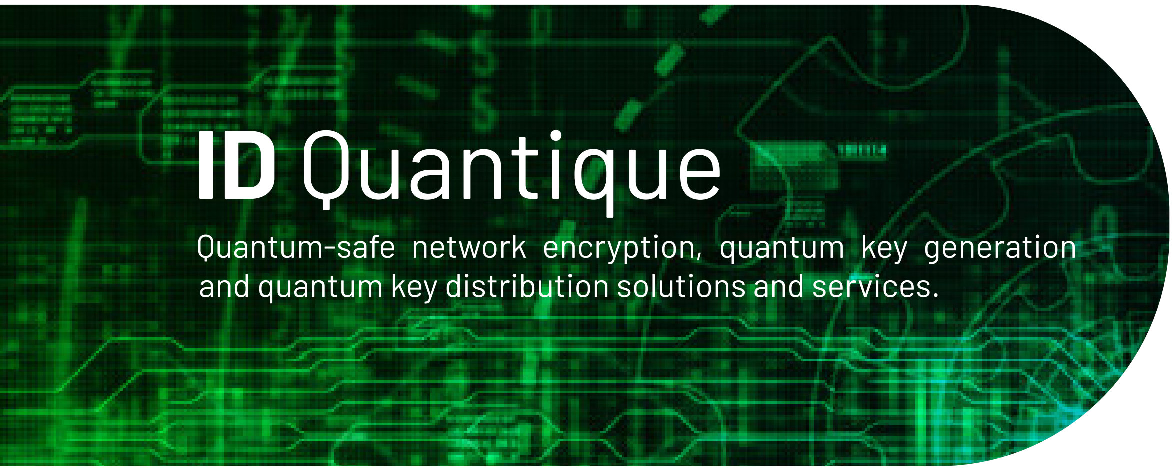
- Ensures applications always have sufficient entropy, even in virtual environments, thereby preventing pseudo-randomness.
- Feeds quantum random numbers to the entropy pool of a computer.

3. Encryption Key and Policy Manager

- Delivers secure, centralised, and highly interoperable key and policy management across any organization.
- Handles 8000 key requests/minute per node.
- Captures event Logs, audit logs, date and time of transactions.

Deployment:

- Management through SSH command line, TLS protected API calls, Web based interface.
- Delivered to clients over a standard TCP/IP network connection, or via mutually authenticated TLS at up to 1 Gbit/s.
- Can be deployed using VM or Hardware appliance.
- Can be integrated into organisation's legacy systems.



ID Quantique

Quantum-safe network encryption, quantum key generation and quantum key distribution solutions and services.

1. Random Number Generator

- Works on the principle that after photons are sent on a semi-transparent mirror, the reflections and transmissions are associated to a "0" and "1" bit value.
- Generates numbers in binary, integer and floating format.

2. Quantum Safe Network Encryption

- 1st commercially available certified high assurance 100Gbps Ethernet encryptor that supports the most complex fully meshed topologies.
- Provides high quality encryption key generation and distribution
- Enables 100% security for Big Data, Cloud and data centre services' ultra-fast networks.
- Provides robust, fault-tolerant security architecture.

3. Quantum Key Generation

- Uses quantum optics process to create true quantum randomness.
- Ensures key is (1) Unique (2) Truly random (3) Stored, distributed and managed securely.
- Passes all randomness tests: Swiss METAS certification, German BSI validation according to AIS 31, NIST SP800-22.

4. Quantum Key Distribution

- Works by sending photons, which are "quantum particles" of light, across an optical link.
- Meets Compliances: NIST SP800-22 Test Suite, METAS Certification, CTL Certification, BSI's AIS31 standard.

Deployment:

- Deployed in ATCA chassis, where various ATCA format blades will be inserted. One chassis is needed at each QKD node.
- Available as a PCI Express Card as well as a USB device.
- Can be accessed using a Command Line and is compatible with most commonly used OS.

MagiQ Tech

Advanced network security and fool-proof defense using Quantum Key Distribution;

Quantum Key Distribution

- Guarantees that keys cannot be intercepted during the key exchange session due to Heisenberg Uncertainty Principle.
- Eavesdropping is instantly detected.
- Encryption is used to protect the data link to the storage site (data in transit) and to protect the data at the site (data at rest).

Solution finds utility with Large Power Grid Providers, R&D organisations looking at protecting trade secrets, and Voice and data service providers who need to secure confidential data.

Deployment:

- Provides the cryptographic key exchange infrastructure and supports secure key exchange at distances upto 120Km.
- Supports a variety of network architecture.

Quantum Cryptography on a Contactless Security Chip

- Is a post quantum key exchange algorithm offering 256 bit security level.
- Serves as an efficient defense against backdoors.

Finds use cases in Identification documents, automotive security and communication protocols.

Deployment:

- Key exchange on a contactless smart card chip.

Crypta Labs

Quantum Random Number Generator technology

QSecure: World's 1st quantum seeded encrypted mobile phone

- Implements Quantum Random Number Generation on a Mobile Phone that can be used by any software or application on mobile phone.
- Secure communication not only for traditional encryption but also for post-quantum encryption by incorporating quantum safe encryption algorithms.

Patented Technology which is robust against vibrations, heat and other external influences. Can support the need for higher bitrates required in the future with the emergence of 5G connectivity. Random tests independently verified and tested by Newcastle University and NIST.

Deployment:

- The QSecure Case attaches to the mobile, transforming it into a quantum random number generator.

Quantum XChange

1st company to effectively implement point to multi pint key distribution including QKD across any distance.

Phio: Quantum Key Distribution and traditional key transmission

- Uses global colocation sites to remove distance limitation for quantum security.
- Leverages the fundamental properties of quantum mechanics.
- Use photons of lights using point to multi point transmission.
- Solution separates the data and key delivery channel making a brute force, quantum computer attacks practically impossible.
- Enhanced quantum security both with and without fiber.
- Interoperable between fiber and non-fiber locations: extends unparalleled security over any TCP/IP link.

Deployment:

- Can be integrated into an organisation's existing cryptography controls.
- Offered as a managed service offering by giving access to 1,000 kilometers of existing optical fiber and 19 co-location centers. Even with shared services, the organization maintains absolute control and visibility of encryption keys and critical data
- Easily scalable
- Keys can be sent over a fiber cable, the Internet or other networks.

QNu Labs

Quantum-safe cryptography products and solutions

Tropos - Quantum Random Number Generator

- Tropos, uses the principles of quantum mechanics to generate truly random numbers. Tropos forms the heart of other products of QNu Labs by delivering true random number.

Armos - Quantum Key Distribution

- Armos is a Quantum Key Distribution (QKD) product that provides unconditional protection to data while it is at its most vulnerable-in motion. Using the principles of quantum physics, Armos secures the distribution of symmetric encryption keys.

  Armos is pre-integrated with Cisco and many other local encryptor technologies in India thus makes the upgradation of classical crypto infra to quantum safe crypto infra in no time thus offers "Faster Time to Value".

Hodos - Quantum Secure Platform

- Powered by Tropos and Armos, the quantum secure platform, Hodos provides key management and application layer for the users to plug and play. Hodos is designed to integrate with existing infrastructure and give the organization a higher security poster instantly.

  Hodos also exposes some of the functionality of the system to run experiments by researchers and students.

EaaS - Entropy as a Service

- Service architecture provides secure access to high entropy as a service.

  EaaS facilitates easy pay per entropy service or monthly subscription service, helping organization's accelerate transition into quantum services.

  EaaS is used to offer quantum security to a Video Conference Application and is also integrated in to an AI PaaS being offered by a partner in U.S to offer entropy to AI algorithms.

Anudos – Intelligent Single Photon Detector

- Fully indigenized SPD from QNu Labs is designed to understand the intricacies involved in the operations of the SPDs. Intelligence built in this SPD will help take measurements of several parameters and analyze those to understand the behavior of QKD system and take decisions accordingly.

  Anudos also has the capability to understand the behavior of SPD under different attacks and avert those in the right manner.

Deployment:

- Armos is a physical device, which is used for quantum encryption using dedicated fibre optical channel.
- Hodos is built to integrate with existing infrastructure. It's a Plug and Play, REST API driven infrastructure that allows us to integrate with existing security suites.
- Armos and Tropos are deployed/under deployment in following use cases:

  1. Quantum Secure VPN
  2. Quantum Secure Dropbox in Cloud – BYoK (Bring Your own Keys model)
  3. Quantum secure Video Conference Application
  4. Quantum Secure networks in a Hub and Spoke model
  5. Multifactor Authentication for Digital Transactions
  6. Securing blockchains using One Time Pads
  7. Using QKD to transport ciphers securely over the internet
  8. Increase randomness using QRNG for the keys generated by HSM
- Use cases:

  1. Use in Armos and Tropos systems thus improving key rate, QBER and security.
  2. Used in Academic and training kits to allow student and researchers to understand the behavior of the QKD system and the SPD.

Others

Post-Quantum

Qubitekk

About DSCI's National Centre of Excellence

DSCI's National Centre of Excellence (National CoE) is a Joint Venture between Data Security of India (DSCI) and the Ministry of Electronics and Information Technology (MeitY) with the objective of providing impetus to the startup ecosystem in India. DSCI has set up a facility, which houses technology research lab, experience zone for demonstration of national cyber capability, experimental SOC, co-creation spaces, training facility for niche capability building, and an incubation center.

Disclaimer: This is a content series for National Centre of Excellence to dissect the emerging security technology products to reveal use-cases, technology stack and deployment strategies. This effort is to create awareness and understanding of technology and not to promote any particular product or company.

@nationalcoe   @CoeNational   company/nationalcoe

www.dsci.in/content/national-centre-excellence-cyber-security-technology-development

ncoe@dsci.in