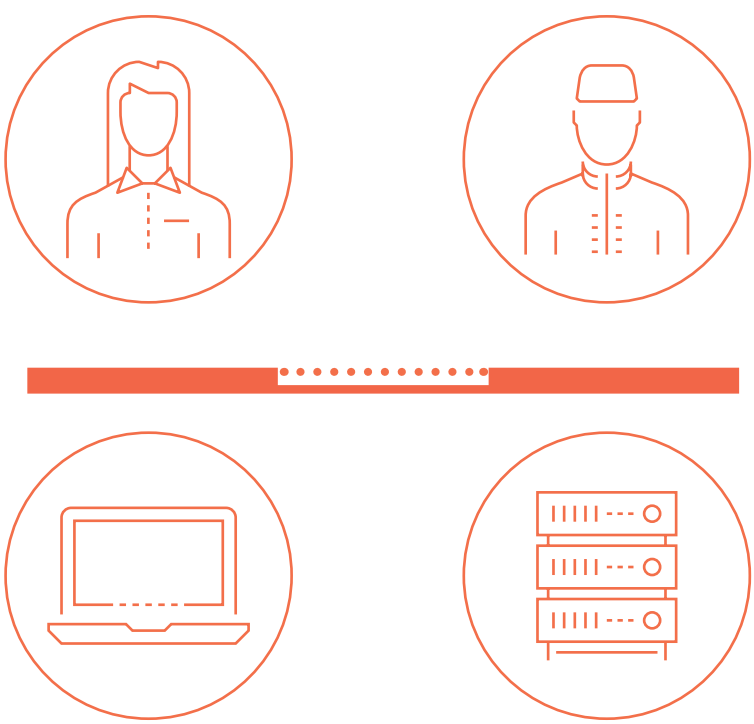
Q→NU

Proactively
Quantum™

Quantum Cryptography Test Platform Kit

Educational Institutes
Research Labs

Contents



01

Quantum Revolution

Welcome to the quantum revolution.

For long, quantum physics was confined to theoretical text books. But now the quantum revolution is truly underway. Quantum technologies are going to affect the very way we live. As we stand on the cusp of the Quantum Age, we would like to partner with you in creating educational material to bridge the gap between theoretical and practical applications.

Quantum technologies like quantum computers are going to revolutionise how computing is done. While on one hand quantum technologies promise new and exciting opportunities, it also brings its own challenges. Quantum computers also pose a serious and present danger to current encryption standards that allow us to live digitally.

If one quantum technology is posing a challenge, then another quantum technology is rising up to meet that challenge. This is where quantum cryptography comes in, neutralising the danger to data. QNu is at the vanguard of protecting data and the digital way of life.

Qnu, an India company, is one of the select few companies that have mastered the science and application of quantum cryptography. And now, you are one of the privileged few who get to have a hands-on experience of the how quantum cryptography works.

With this Quantum Cryptography Platform Kit, you will get to explore the frontiers of quantum cryptography with QNu's Quantum Key Distribution and Quantum Random Number Generator. The kit will enlighten about the theory and its applications in quantum cryptography. With this test one will find a set of experiments, procedures and expected results. This will enable one to better understand and master the technologies that will affect our lives in the future.

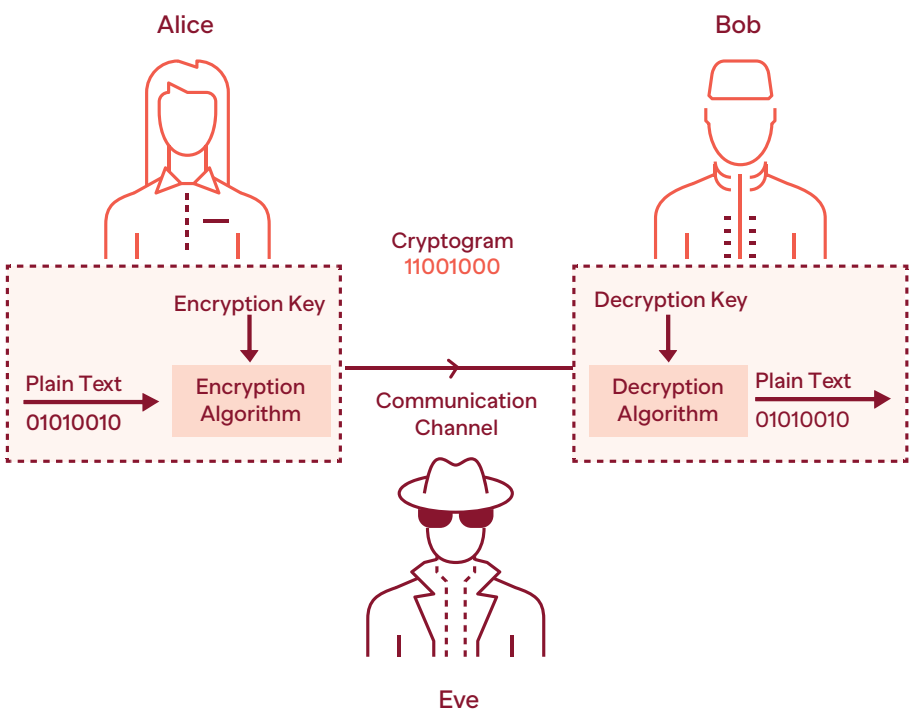
Leverage the kit and become part of an exclusive club and join the brigade to lead Quantum revolution in India.

02

Cryptography

Cryptography is the art of secret writing. The primary objective of cryptography is to protect the authenticity, integrity and confidentiality of the information being sent. The architecture of a cryptosystem is presented in the figure below. It comprises of two or more parties sharing an encrypted message. The message (plain text) is encrypted by an encryption algorithm using an encryption key and delivered to the recipient through a conventional channel as a cryptogram. The encryption algorithm is again applied in an inverse manner to retrieve the message from the cryptogram.

The architecture of a cryptosystem



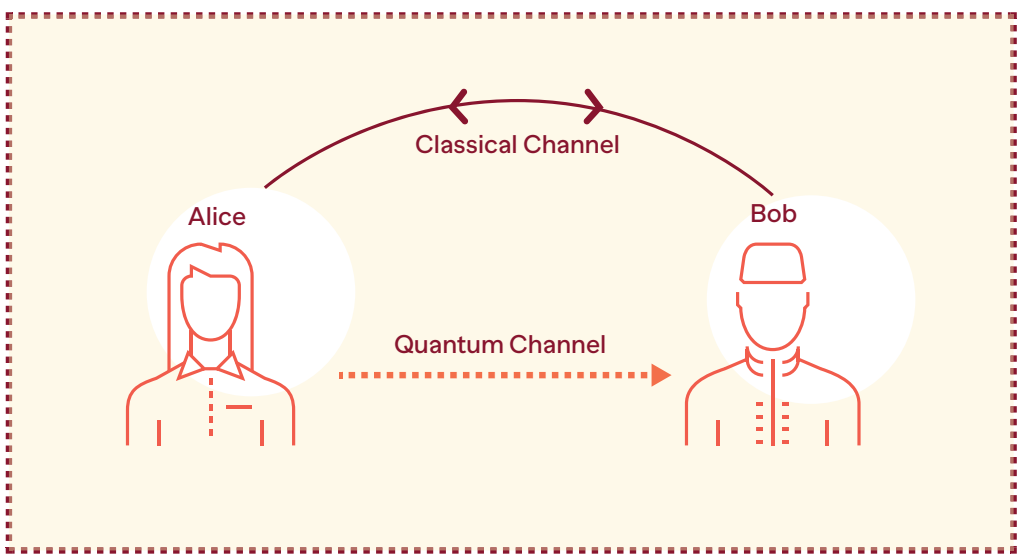
03 Quantum Cryptography

Quantum Key Distribution

Quantum Cryptography is the art of applying quantum information in cryptography. Quantum Key Distribution (QKD) is a state-of-the-art key exchange mechanism that ensures elimination of every possible threat of eavesdropping or leakage by treason, to make the key unconditionally secure.

The key exchange is done by means of encoding on the properties of the quantum particles and sending them across on a quantum channel. This is done right under the presence of an eavesdropper and any attempt to eavesdrop gets detected by virtue of the properties of quantum mechanics.

Quantum key distribution

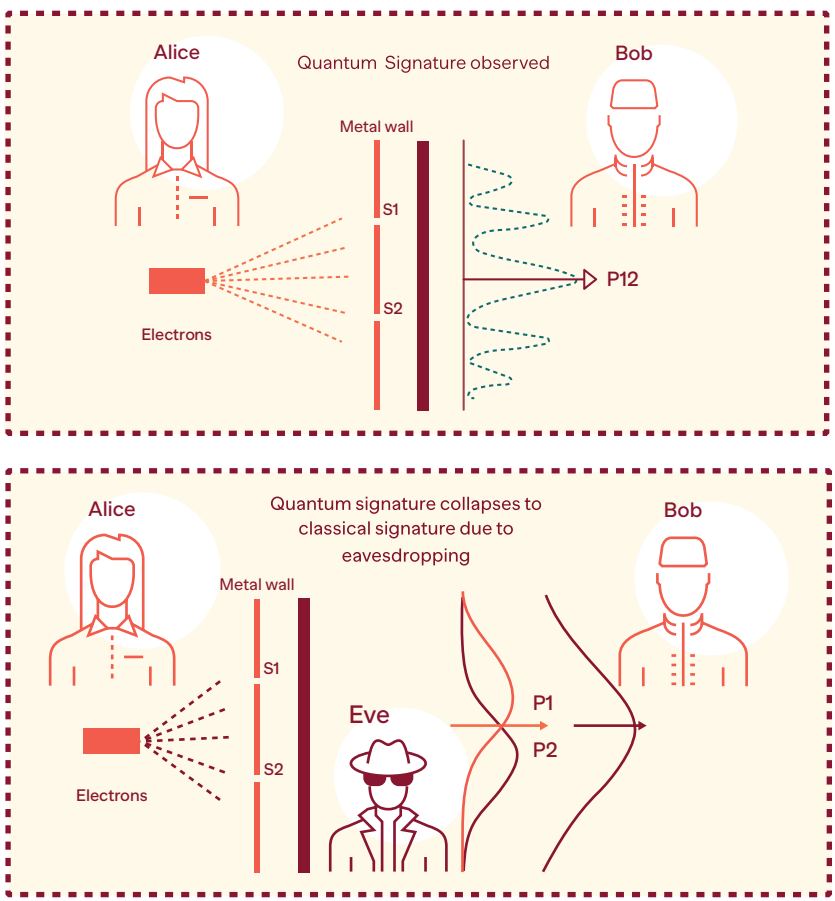


04

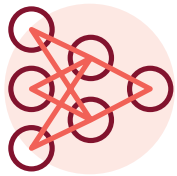
Quantum Physics of QKD

The fundamental laws of quantum mechanics like Heisenberg's uncertainty principle and No-cloning theorem enable effective monitoring of the key distribution channel against eavesdropping. According to Heisenberg's uncertainty principle, measuring the key data causes perturbation in the system. The No-cloning theorem prohibits duplicating the quantum state.

The security of QKD is governed by these laws of quantum physics. Consider Alice's information similar to Quantum interference pattern. If Eve is trying to observe which slit the electron has gone through it will collapse to classical interference pattern.



05 Kit Specifications

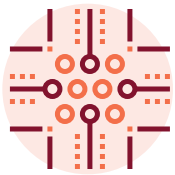


Source

In quantum key distribution, the carriers of binary information is a quanta of light. Ideally, it is a single photon but QKD is mostly implemented by faint laser pulse/weak coherent source at different wavelengths. This kind of source obeys Poisson statistics.

Variable mean photon number

We can provide a set of attenuations and the student can study the impact on QKD key rate through software controlled / user interface.



Length of Quantum channel

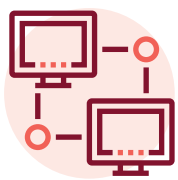
Quantum channel of different length up to < 100 km can be provided. Customised fibre length and fibre type option can be provided for research purposes. This will help the students to understand the impact of distance on different parameters of QKD like key rate and quantum bit error rate .

Hacking

The educational kit shall make provisions for realistic attacks on quantum channel on request for research purposes only.

Noise

We can/may induce noise from different sources like electrical and optical on the QKD system for research purposes.



Classical channel

The classical communication between Alice and Bob can happen with either Ethernet.

Key

The sifted key and final secure key will be generated. The rate of generation will be typically in Kbps. Provision for extraction of sifted key and final key from both Alice and Bob system will be provided.

QBER

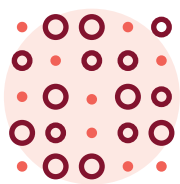
The tolerated error rate can be between 1% to 20% above which, only the QBER will be announced, and post processing will be not be done. Required QBER for specified QKD protocol will be stated.

Privacy amplification

The error corrected key, will be compressed by a well established algorithm to generate final secure key.

1. There can be provision made to vary compression factor between fixed set of values on request for research purposes.

2. We can provide the facility to the student to extract the sifted key and implement their own Privacy Amplification algorithm.



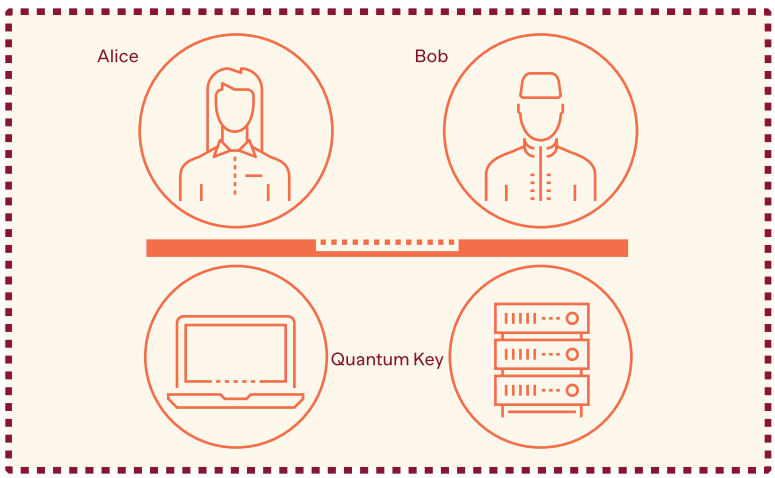
Quantum Random Number Generator

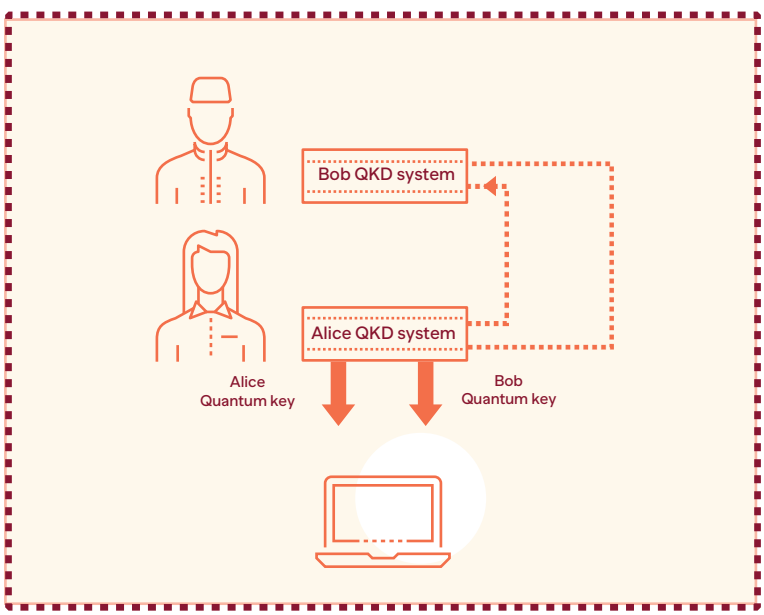
The random numbers generated from quantum mechanical process are quantum random numbers. Random numbers from time of arrival based QRNG will be generated. A standard customisved test suite will be provided to test the random numbers.

Housing

We can house the QKD system into two following configurations.

Configuration 1: Alice and Bob are housed separately.





Configuration 2: Alice and Bob are housed on different racks of same case.

06

Feedback

Email

.....

Contact

.....

Comments

.....

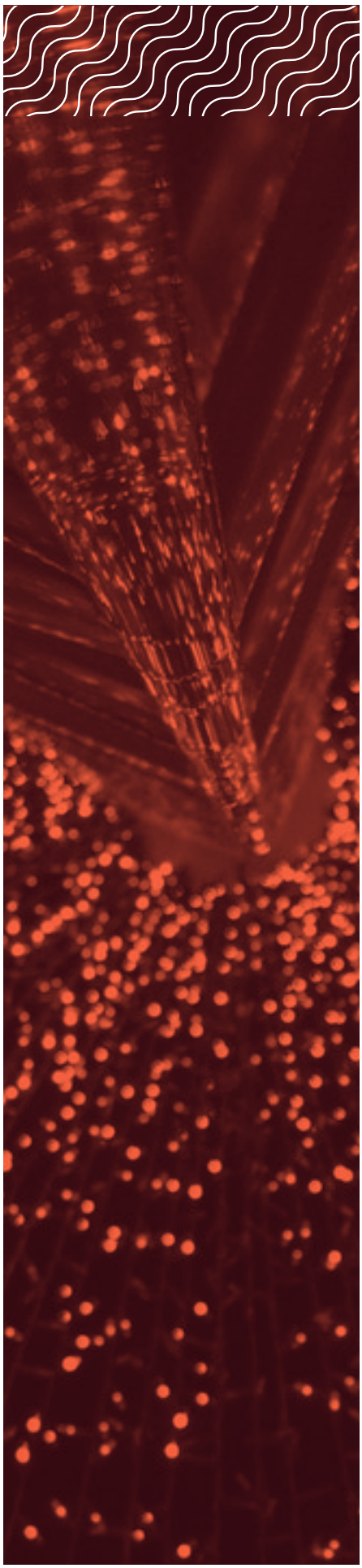
.....

.....

.....

.....

.....



+91 81305 60038
info@qunulabs.in
qunulabs.in

Let's challenge the status quo of data security paradigms. Here's how you can reach us to explore a partnership.

Proactively Quantum™