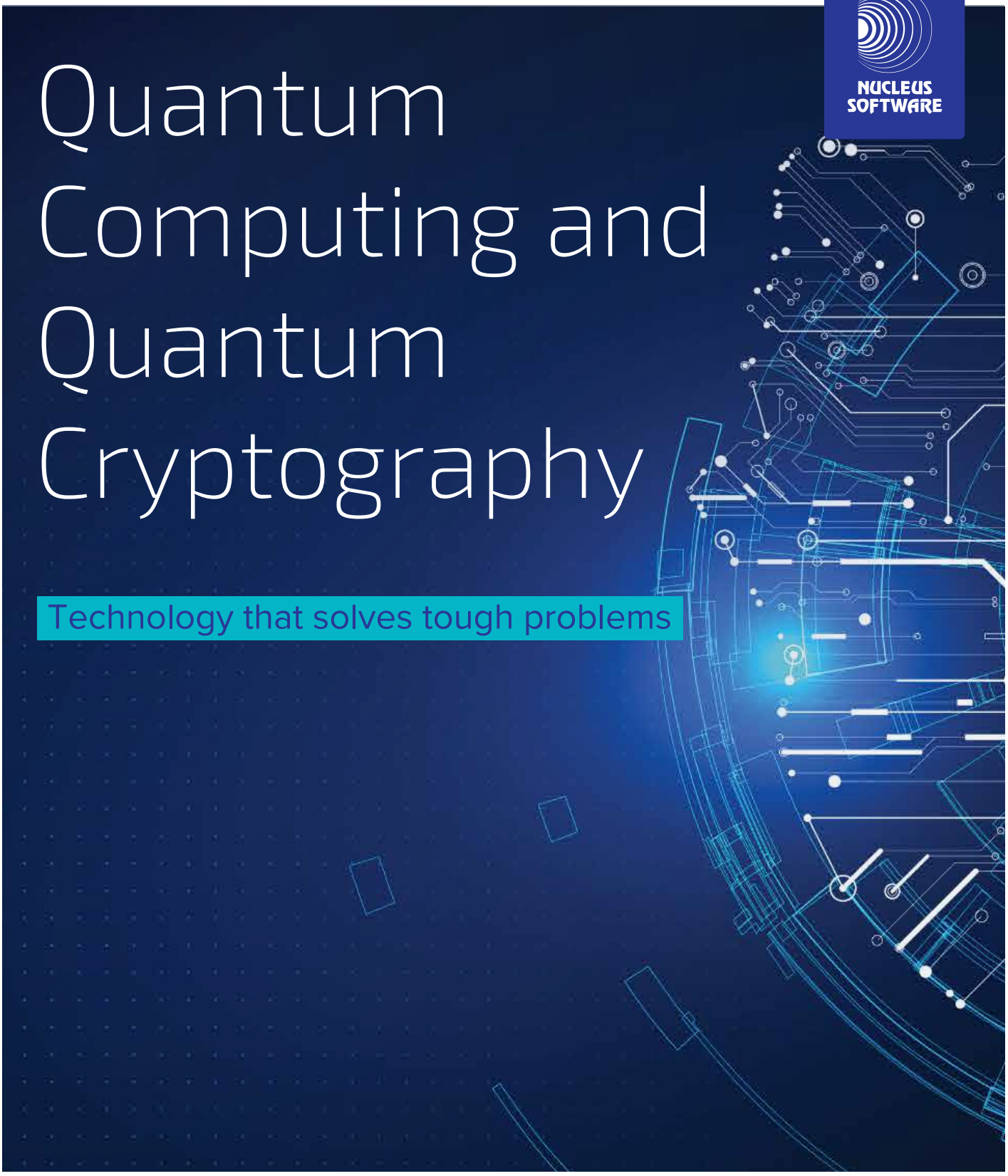
NUCLEUS SOFTWARE

# Quantum Computing and Quantum Cryptography

## Technology that solves tough problems



German physicist Max Planck proposed that a ‘perfect black body’ emitted and absorbed electromagnetic waves as discrete bundles of energy referred to as ‘quanta’. This was the birth of quantum mechanics that gave scientists unprecedented, and unique mathematical tools to understand our world on the atomic scale.

Now, in the 21st century, the concept of quantum-mechanical states forms the basis of 'quantum computers' - a term coined by Richard Feynman in the early 1980s during his call for producing quantum mechanical computer systems. Quantum computers are potentially exponentially faster and much cleverer in cracking codes deemed impossible for classical technology to accomplish.

This whitepaper will take you through Quantum Computing, Quantum Cryptography, Quantum Computing use cases in Financial services industry and challenges in quantum computing.

## QUANTUM COMPUTING

Let's start by enhancing our understanding about quantum computing. Quantum computing is a type of computation whose operations can harness the phenomena of quantum mechanics, such as superposition, interference, and entanglement mechanics to solve very complex problems. Devices that perform quantum computations are known as quantum computers. Quantum computer carried out a specific calculation that is beyond the practical capabilities of regular, 'classical' machines. Quantum computer can do complex calculation in less time whereas the same calculation would take even the best classical supercomputer 10,000 years to complete. From Security Encryption perspective quantum computers would be more powerful than classical computers.

**The two main properties of quantum computers that distinguish them from classical computation are:**

- In quantum computing computation values 'quantum bits' or 'qubits' exist as the superposition of 0's and 1's. This can be imagined as 0 and 1 corresponding to the horizontal and vertical directions of a physical quantity, such as the polarization of light, and in conventional computers bits are only oriented along the horizontal or vertical axes.

- The second property is quantum entanglement. The bits of classical computers can only be manipulated independently of each other. In other words, a change in the state of one bit does not affect other bits. Quantum bits, however, can exist in so called entangled states where manipulation of one bit simultaneously affects the other bit(s). Quantum entanglement is a property unique to quantum systems and Scientists have exploited these two properties for the development of quantum algorithms.

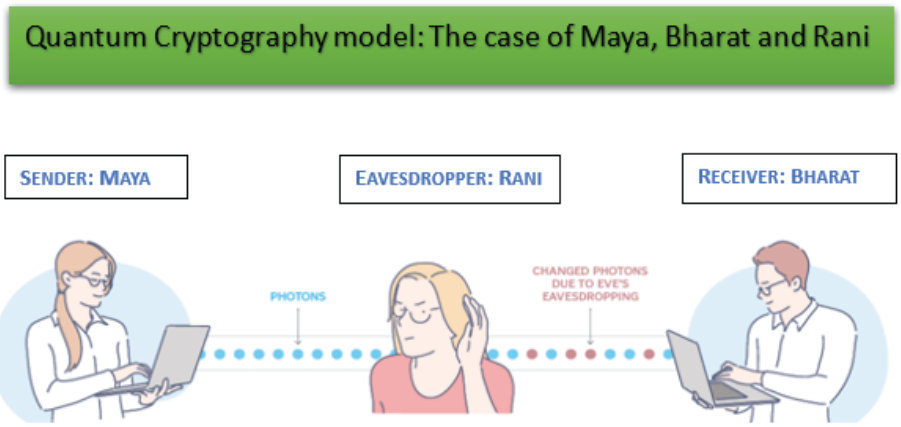
## QUANTUM CRYPTOGRAPHY

With Quantum Computing, Quantum Cryptography also come into picture for securing Data. Quantum Cryptography is the process of encrypting and protecting data so that only the person who has the secret key can decrypt it. Quantum cryptography is a method of encryption that uses the naturally occurring properties of quantum mechanics to secure and transmit data in a way that cannot be hacked. Quantum cryptography is different from traditional cryptographic systems, in that, it relies on quantum mechanics. Quantum cryptography uses a series of photons (light particles) to transmit data from one location to another over a fiber optic cable. By comparing measurements of the properties of a fraction of these photons, the two endpoints can determine what the key is and if it is safe to use.

### How Quantum Encryption works:

Considering the above diagram where you have two people, Maya and Bharat, who want to send a secret to each other that no one else can intercept. Maya sends Bharat a series of polarized photons over a fiber optic cable. This cable doesn't need to be secured because the photons have a randomized quantum state.

Maya initiates the message by sending Bharat a key. The key is a stream of photons that travel in one direction. Each photon represents a single bit of data -- either a 0 or 1. However, in addition to their linear travel, these photons are oscillating, or vibrating, in a certain manner. So, before Maya, the sender, initiates the message, the photons travel through a polarizer. The polarizer is a filter that enables certain photons to pass through it with the same vibrations and lets others pass through in a changed state of vibration. The polarized states could be vertical (1 bit), horizontal (0 bit), 45 degrees right (1 bit) or 45 degrees left (0 bit). The transmission has one of two polarizations representing a single bit, either 0 or 1, in either scheme she uses. The photons now travel across optical fiber from the polarizer toward the receiver, Bharat. This process



uses a beam splitter that reads the polarization of each photon. When receiving the photon key, Bharat does not know the correct polarization of the photons, so one polarization is chosen at random. Maya now compares what Bharat used to polarize the key and then lets Bharat know which polarizer she used to send each photon. Bharat then confirms if he used the correct polarizer. The photons read with the wrong splitter are then discarded, and the remaining sequence is considered the key.

Let's suppose there is an eavesdropper present, named Rani. Rani attempts to listen in and has the same tools as Bharat. But Bharat has the advantage of speaking to Maya to confirm which polarizer type was used for each photon; Rani doesn't. Rani ends up rendering the final key incorrectly. Maya and Bharat would also know if Rani was eavesdropping on them. Rani observing the flow of photons would then change the photon positions that Maya and Bharat expect to see.

## QUANTUM CRYPTOGRAPHY BENEFITS

Today's modern Cryptographic algorithms derive their strength from the difficulty of solving certain math problems using classical computers or the difficulty of searching for the right secret key or message. Quantum computers, however, work in a fundamentally different way. Solving a problem that might take millions of years on a classical computer could take hours or minutes on a sufficiently large quantum computer, which will have a significant impact on the encryption performed using hashing and public key algorithms we use today. This is where quantum-safe cryptography comes in.

**"Quantum-safe cryptography that refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built."**
**Quantum-safe cryptography benefits includes:**

- Quantum Cryptography Provides secure communication. Instead of difficult-to-crack numbers, Quantum Cryptography is based on the laws of physics, which is a more sophisticated and secure method of encryption.

- Quantum Cryptography helps in detects eavesdropping. If a third-party attempts to read the encoded data, then the quantum state changes, modifying the expected outcome for the users.

- Quantum Cryptography offers multiple methods for security. There are numerous quantum cryptography protocols that may used for enhancing security. Some, like QKD, for example, can combine with classical encryption methods to increase security.

## HOW QUANTUM COMPUTING IS BENEFICIAL FOR THE FINANCIAL INDUSTRY

Some specific use cases for Quantum computing in financial services are

- **Targeting and prediction**

Today's financial services customers demand personalized products and services that rapidly anticipate their evolving needs and behaviors. 25% of small and medium-sized financial institutions lose customers due to offerings that don't prioritize customer experience. It's difficult to create analytical models that sift through mounds of behavioral data quickly and accurately enough to target which products are needed by specific customers in near real-time. This constrains financial institutions from providing preemptive product recommendations with optimal feature selection in an agile manner. As a solution, the data modeling capabilities of quantum computers are superior in finding patterns, performing classifications, and making predictions enabling financial institutions to cater to their customer's dynamic demands. This whole process is not possible by using a classical computer because of the challenges of complex data structures.

- **Trading optimization**

Complexity in financial markets trading activity is skyrocketing. Due to greater transparency requirements from regulations, strict validation processes are applied to trading. Hence, In this complicated trading landscape, investment managers struggle to incorporate real-life constraints, such as market volatility and customer life-event changes, into portfolio optimization. Quantum technology could help cut through the complexity of today's trading environments. Quantum computing's optimization capabilities may enable investment managers to improve portfolio diversification, rebalance portfolio investments to precisely respond to market conditions and investor goals.

## CHALLENGES IN QUANTUM COMPUTING

While there are clear advantages to Quantum Computing, it's crucial to acknowledge the potential challenges as well. There are three broad categories of challenges to realize the true potential of quantum computing.

- First, and perhaps most fundamental is the quest for the 'application/s' to demonstrate the advantages of quantum computers over conventional technology.

- Second more difficult challenge is design and engineering of devices and hardware. Specifically, thermal and vibrational noise disturbs the quantum entangled state of qubits and leads to erroneous computation.

- Finally, nurturing professionals to work with quantum computers is also challenging.

**CONCLUSION:**

In the near term, classical computers will continue to dominate the marketplace. Given the specialized equipment, space, and expertise required for building and using them, quantum computers will be limited to specific institutions and uses. Technology companies are beginning to address this limitation by making quantum capabilities and services available through the cloud, thereby making these capabilities broadly available to government, academia, and industry and ensuring continued interest and development.

With available Quantum Computing capabilities an enhanced Security is the need of every organization. From security perspective ability for quantum computers to quickly factor large numbers of calculations will be disruptive to the field of security. This change will require a shift from current encryption methodology standards to systems that are challenging for quantum computers to break such as quantum cryptography.


NUCLEUS SOFTWARE

SALES@NUCLEUSSOFTWARE.COM
WWW.NUCLEUSSOFTWARE.COM



GLOBAL OFFICES: AMSTERDAM | CHENNAI | DUBAI | JAIPUR | JOHANNESBURG | LONDON | MANILA | MUMBAI | NEW DELHI | NEW JERSEY | NOIDA | SINGAPORE | SYDNEY | TOKYO.