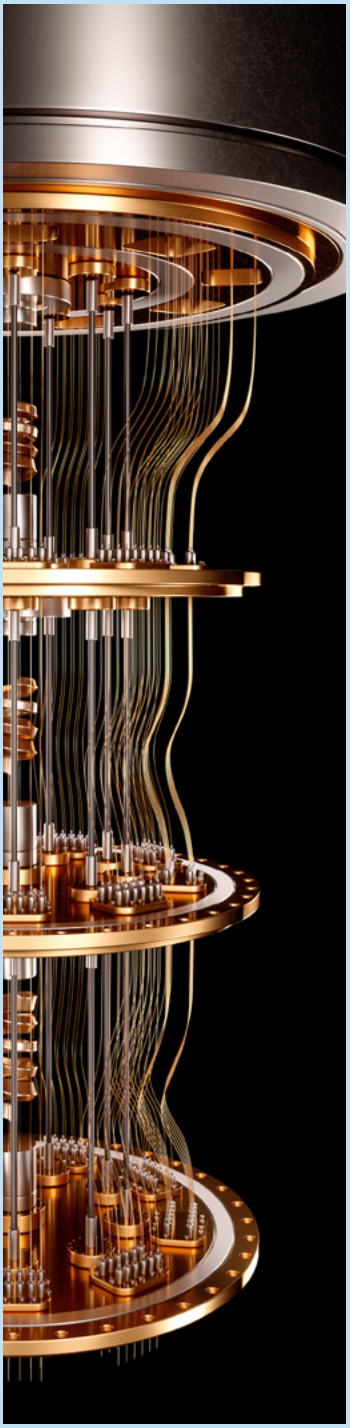
VIEW POINT



ROAD TO QUANTUM CRYPTOGRAPHY

Abstract

In this ever-evolving digital age, securing sensitive data has become a top priority for organizations across industries. From financial institutions to healthcare providers to national security, everyone strives to ensure their confidential information remains safe from prying eyes. Cryptography has been the go-to solution for data security for centuries, but since the dawn of quantum computing, classical cryptography methods are becoming increasingly susceptible to attacks. Enter quantum cryptography - a new era of security that comes with the promise to revolutionize the industry.

Infosys®
Navigate your next

What is Cryptography? – Definition!

The practice and study of techniques to secure information and communication through the use of mathematical algorithms is known as cryptography. It is done by taking the information and transforming it in a way that is unreadable to everyone except the one with the key that can transform it back to the readable form. These techniques have been used for a long time to protect messages from being read by unintended recipients, and their importance has risen in this modern digital age as the majority of communication takes place over electronic channels. The word Cryptography has Greek roots as the word 'kryptos' means 'hidden' and 'graphein' means 'to write'.

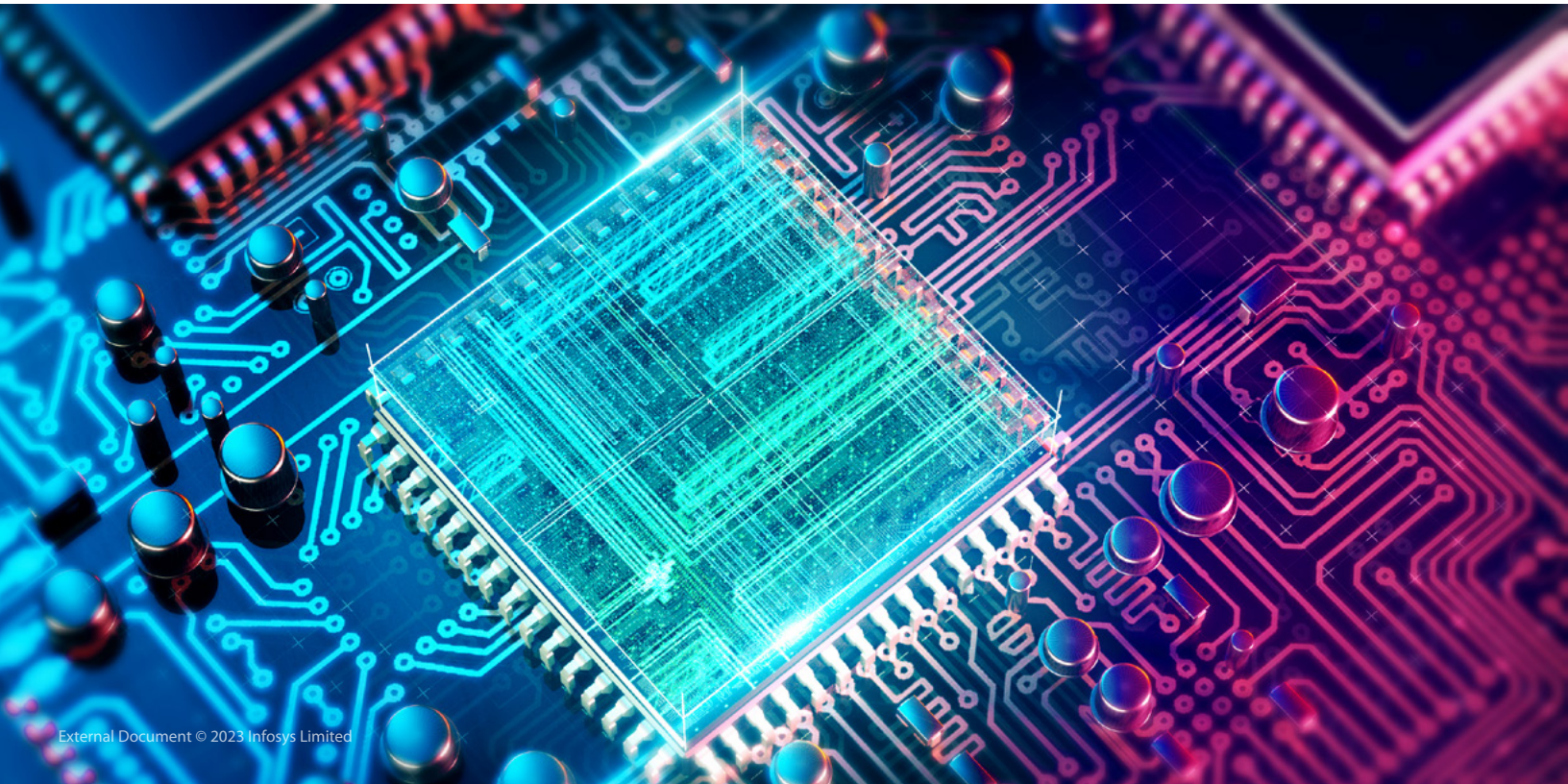
Cryptography Made Easy - Story Time!

Let's try to understand symmetric-key cryptography and public-key cryptography with the help of a short story.

Emma and Matt are two friends who often communicate online. One day, they want to share a secret document, but they're worried that someone might intercept it. They decide to use **encryption** to protect the document. They agreed on using a **symmetric encryption** technique, in which both will use a single secret key to encrypt as well as decrypt the shared document. They agree on a secret key and use a **cipher** to encrypt the document. Emma sends the document encrypted by cipher to Matt, and he uses the same key to decrypt the document and read it. However, they realize this method has a weakness - if anyone else gets hold of the key, they can also decrypt the document. After a bit of brainstorming, they decided to opt for **asymmetric encryption** where they would use a pair of keys – a public key and a private key.

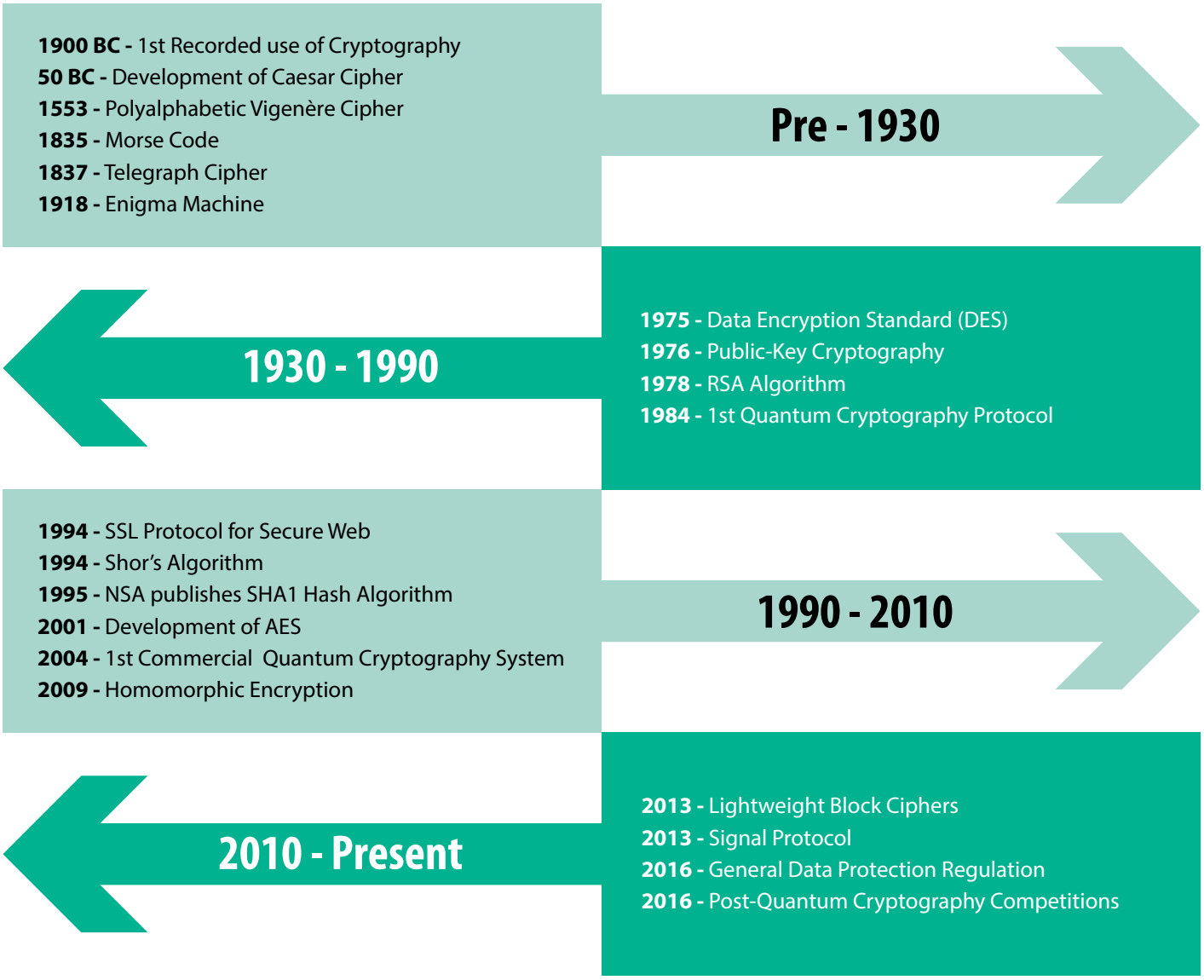
Matt comes up with a pair of keys - a **public key** and a **private key**. He sends Emma the public key, which she uses to encrypt the document. The encrypted document can only be decrypted using Matt's private key. This method ensures that only Matt can decrypt the document. Emma and Matt are now able to communicate securely using asymmetric encryption. They're both happy that their secret document is safe from prying eyes.

In summary, encryption is simply the process of utilizing a cipher to transform plain text into cipher text. The process of translating cipher text back into plain text is known as decryption. A set of instructions for encrypting and decrypting data is known as a cipher. Asymmetric encryption utilizes a pair of keys — a public key and a private key — in contrast to symmetric encryption, which uses the same secret key for both encryption and decryption. While the private key is required for decryption of the data, the public key is utilized for encryption of the data. The difficulty of the algorithm and the size of the key determine how secure a cryptographic system is.



How We Reached and Where We Are – History!

The history of cryptography dates back thousands of years, with early civilizations developing methods to disguise the meaning of messages using simple codes and ciphers. The Caesar Cipher, which was used by Julius Caesar to communicate with his generals via secret messages, is among the most well-known examples. Over time, more complex and sophisticated cryptographic techniques were discovered and experimented with, such as the Vigenère Cipher and the Enigma Machine, both of which the Germans famously employed during the Second World War.



Cryptography Timeline

Today, cryptography is considered an indispensable component of cybersecurity, providing the necessary tools and techniques to maintain confidentiality, integrity, and authenticity in digital systems and information exchange. It is utilized to ensure secure communication, safeguard online banking transactions, and protect sensitive government and military data. The development of new and more robust cryptographic techniques is essential and become a top priority for organizations across the globe to address and tackle the growing threat of cyber-attacks. Now, cryptography has become a highly specialized field where experts are working continuously to create new techniques, algorithms, and protocols resistant to attacks from highly sophisticated criminals.

What Popular Techniques Are Being Used Currently? – Types!

There are a variety of cryptographic techniques and methods used in the industry nowadays to ensure that their information and communications are secure.

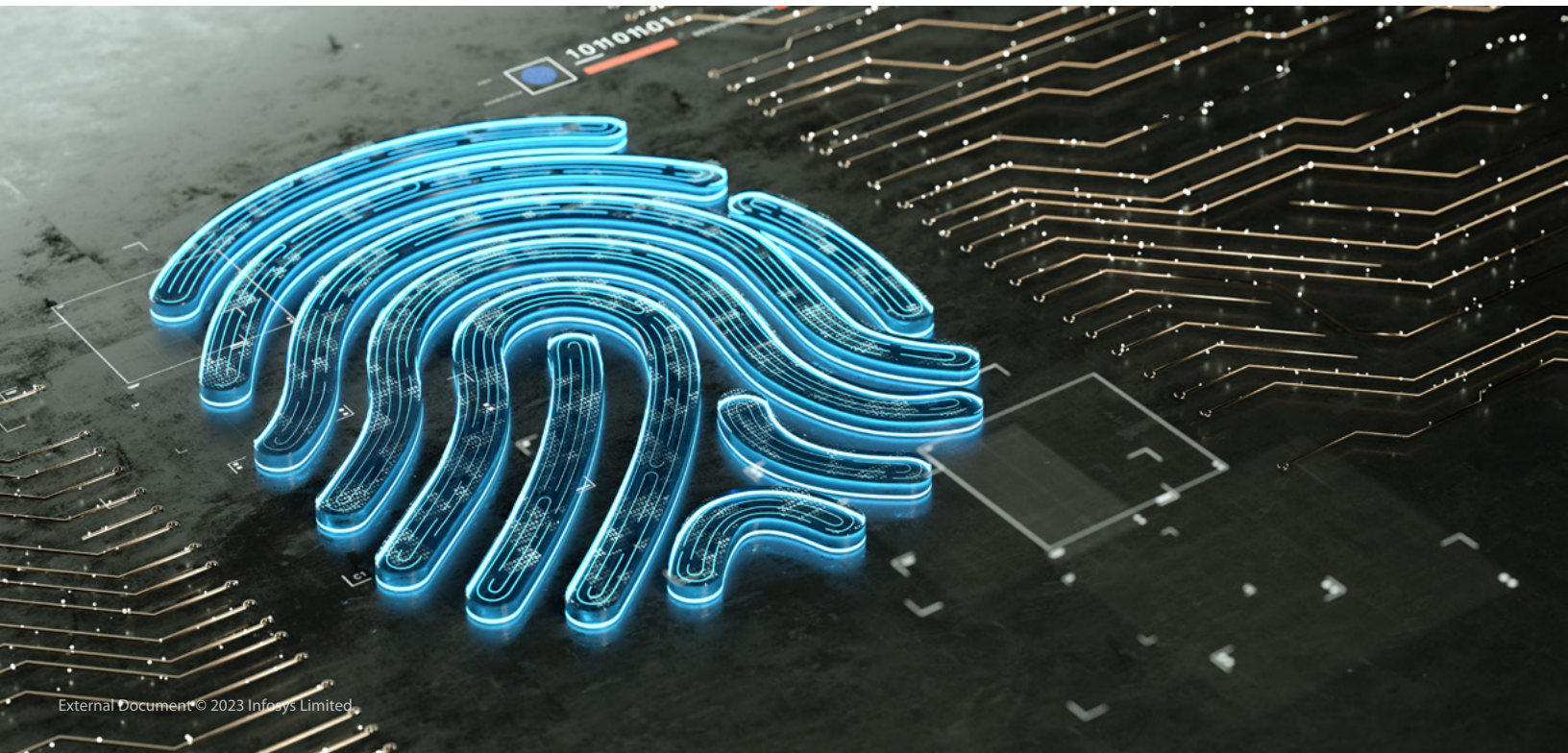
One of the well-known techniques is the **Advanced Encryption Standard (AES)**, invented in the year 1997. It is a symmetric key algorithm that uses a 128-bit block size and key sizes of 128, 192, or 256 bits. AES is widely used to encrypt sensitive data in transit or at rest, including financial transactions, sensitive documents, and communication between devices. The AES-265 algorithm is considered so secure that even for the most powerful supercomputer currently in use, it would take the classical computer billions of years to break the encryption with a brute-force attack. Due to this complexity, it is regarded as being extremely safe.

Public key cryptography, which we previously covered, is another popular method of cryptography today. It makes use of two keys—a public key and a private key—to encrypt and decrypt messages. This method has many applications, which include securing email, SSL/TLS, and digital signatures. Public key cryptography enables two parties to communicate securely without having to share a secret key. **RSA** and **Elliptic Curve Cryptography** both rely on the difficulty of factoring huge prime numbers and resolving the discrete logarithm problem associated with elliptic curves. The size of the keys used directly impacts how strong these algorithms are. For example, a 2048-bit RSA key is currently considered secure against classical attacks, while a 256-bit elliptic curve key is considered equivalent in strength.

Another important cryptographic technique is the **hash function**, primarily used to ensure data integrity. A hash function takes a message of any length and generates a fixed-size, unique hash value. Any changes in the message will result in a different hash value, making it difficult for an attacker to alter the data without detection. Hash functions, such as **SHA-256**, are used to ensure the integrity of data and are resistant to collisions. The strength of hash functions is measured in terms of their collision resistance or the ability to generate unique hash values for different input data.

If These Methods Are So Good, Why Quantum Cryptography?

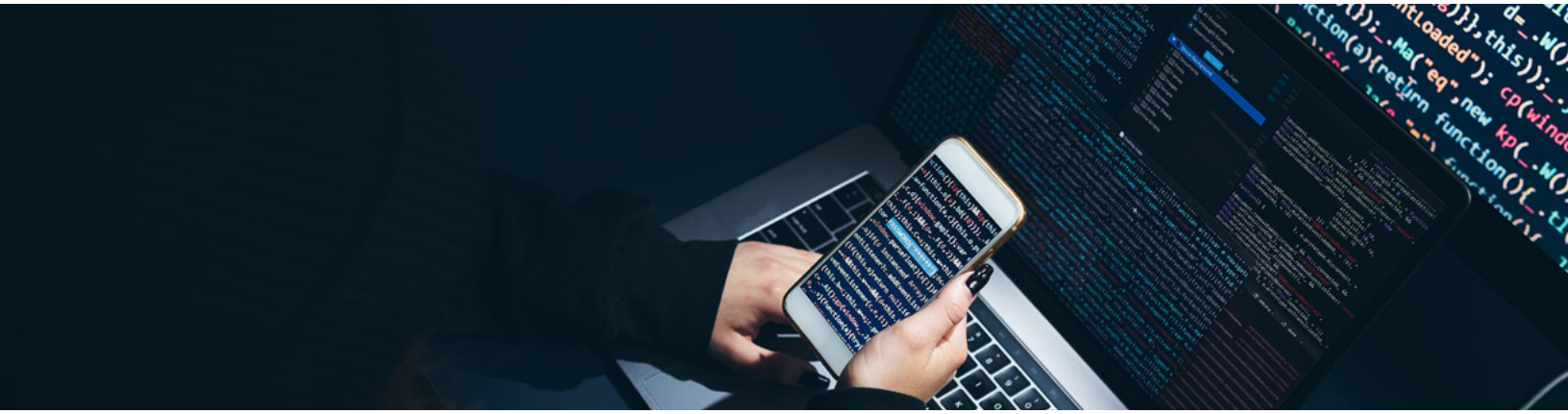
Even though hash functions, public key cryptography, and traditional cryptographic methods like AES are very good at protecting data and communications, they are all based on mathematical equations. And existing mathematical equations can be cracked/solved given enough computing power. Contrarily, quantum cryptography takes advantage of the ideas behind quantum mechanics to produce cryptographic keys that are impenetrable even in the presence of infinite computing power. More advantages and reasons will be covered after we understand quantum cryptography.



What is Quantum Cryptography? – Definition!

Definition: Quantum Cryptography is a branch of cryptography that uses the principles of quantum mechanics to ensure private and secure communication and exchange of information. It is highly secure and can detect any attempt to eavesdrop or alter the message.

One of the important characteristic of quantum cryptography is the fact that it is impossible to measure and calculate the state of a quantum system without disturbing the initial state of it. Quantum cryptography uses photons (individual particles of light) to transmit the data, as their behavior is well understood and can carry information in optical fiber cables. Photons can also demonstrate quantum behavior, specifically **quantum entanglement**, which means two particles are linked to each other even after being light-years apart. This means if two photons are entangled, then the change in one photon will reflect in the other as well.



What is the impact of that? Advantages!

1. **Eavesdrop Detection:** Any attempt to intercept or measure the quantum state of a photon will result in a change to the state of the photon, which can be detected by the receiver. Therefore, any attempt to eavesdrop on a quantum communication or information channel would necessarily leave detectable traces, alerting the legitimate parties to the presence of an eavesdropper.
2. **Information-Theoretic Security:** It makes sure that the privacy of the encrypted message/ data is based on the fundamental laws of physics. Any intruder with unlimited computational resources and time will not be able to uncover the message/data, and it will remain secure.
3. Quantum States are continuously changing hence making it impossible for the intruder to crack the key.
4. **Multiple Methods for Security:** Numerous quantum cryptography protocols can be used. A few of them are:
   i. **Quantum Key Distribution (QKD)** protocol establishes a shared secret key between two parties without the possibility of interception or tampering by an eavesdropper.
   ii. **Quantum Coin Flipping** protocol resolves any disagreement between two parties about the outcome of a coin flip. The protocol ensures that neither party can cheat and that the outcome of the coin flip is truly random.
   iii. **Quantum Oblivious Transfer** protocol is used to securely transfer one of two possible values from a sender to a receiver without revealing which value was transferred.
   iv. **Quantum Digital Signatures** are cryptographic protocols that allow a sender to digitally sign a message and ensure that the signature is authentic and cannot be forged.
   v. **Quantum Secret Sharing** operates on a protocol that shares a secret among several parties, and only when a specific number of parties collaborate the secret can be reconstructed.

In summary, while traditional cryptographic techniques are highly effective, they are vulnerable to attacks by quantum computers. Quantum cryptography, on the other hand, offers provably secure communication and detection capabilities that are not possible with traditional cryptographic techniques and has the potential to enable new forms of secure communication and computation.

Are There Only Good Things? – Disadvantages!

Quantum cryptography is not the ideal solution, and as it is still at its nascent and developing stage, we see some shortcomings that are worth mentioning.

1. **Limited Range & Sensitive to Environmental Noise:** Its range is limited due to photon loss over long distances as photons are sensitive toward the environment (such as temperature fluctuations, vibrations, etc.) and interact with it causing their polarization states to change. This usually results in errors and loss of quantum information. While specialized techniques such as quantum repeaters, error correction codes, and quantum memories have been proposed to address this issue, they are still in the experimental phase.
2. **Complexity and High Cost:** To successfully achieve quantum cryptography requires specialized equipment such as single-photon detectors, quantum sources, and quantum channel emulators, which can be challenging and expensive to manufacture, operate, and maintain. The specialized components required, such as single-photon detectors, are typically more expensive than those used in classical cryptography systems. Moreover, knowledge of quantum mechanics, quantum information theory, and information security are necessary for its successful implementation. This complexity can make it difficult to deploy on a large scale, especially in comparison to classical cryptography.

Where Can It Be Utilized? – Use Cases!

Quantum cryptography can be used in multiple applications where secure communication is essential. Below are a few potential use cases:

- **Financial Services:** The cost of cyberattacks in the banking industry has reached $18.3M annually per company. Quantum cryptography can be used to safeguard financial transactions, including stock trading, internet banking, and electronic fund transfers. It will provide a level of security that can aid in preventing fraud and illegal access to financial data.
- **Government and Military:** Secure communication offered by quantum cryptography can be utilized by government and military organizations for intelligence gathering, diplomatic communications, and military command and control. With such a high level of security information, leaks and espionage would drastically drop in count.
- **Healthcare:** According to reports, the healthcare sector suffers a loss of $10M per data breach. Patient data and medical records, including electronic health records and medical imaging, can be easily secured with quantum cryptography. It will be able to prevent unauthorized access and safeguard sensitive personal data from getting into the wrong hands.
- **Critical Infrastructure:** Average data breach due to lack of proper strategies cost $5.4M and has seen a steady rise. Quantum cryptography can help secure power grids, transportation systems, communication networks, and other such critical infrastructures. The security offered can help prevent cyberattacks and protect against disruptions to essential services.
- **Cloud Computing:** Loss of data lost due to cloud security breaches cannot be quantified as personal data is priceless to its owner. Quantum cryptography can protect data storage, processing, and transmission and can be used to secure cloud computing as a whole. The security offered by quantum cryptography can help protect sensitive information and prevent data breaches.
- **IoT and Smart Devices:** Personal smart devices usually track personal details, and it would be ideal to have them protected. IoT devices and smart devices, such as smart homes, wearables, and industrial IoT devices, can all be secured with the help of quantum cryptography. The security offered by quantum cryptography can help prevent hacking and protect against unauthorized access to the devices.

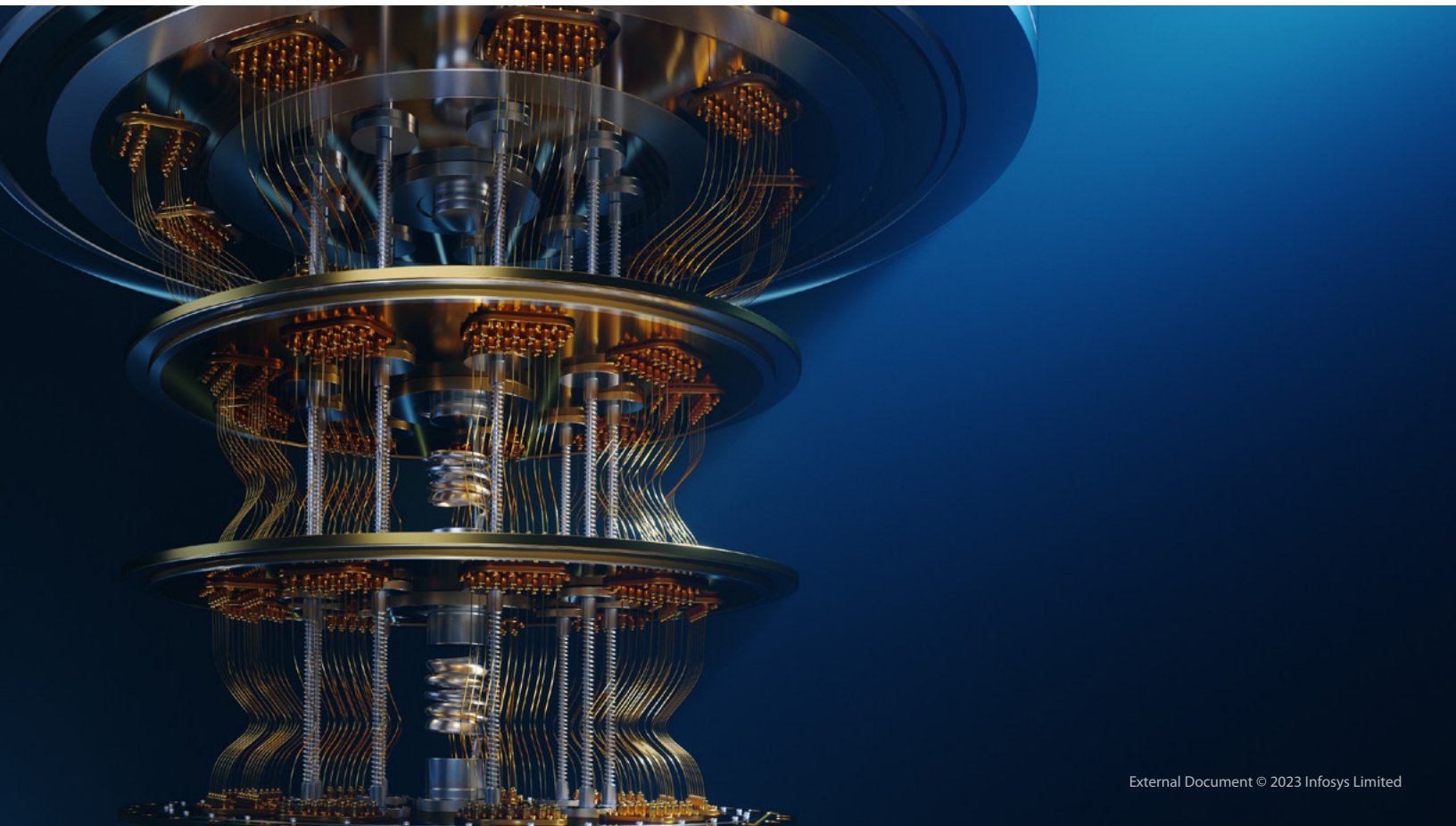
Reference

- https://www.sangfor.com/blog/cybersecurity/cyber-attacks-on-banks-devastate-financial-sector
- https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-attacks-against-critical-infrastructure-quietly-increase
- https://www.linkedin.com/pulse/encryption-vs-hashing-amr-saafan
- https://arxiv.org/pdf/1804.00200.pdf
- https://www.sciencedirect.com/topics/engineering/cryptography
- https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html
- https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

Authors

Aseem Rajvanshi is a Senior Associate Consultant working in iCETS. His main objective revolves around researching various industries for trends and emerging technologies like Quantum Computing, AI, Blockchain, etc. as well their impact in several industries. He is a technology enthusiast who enjoys exploring and learning about new & emerging technologies.

Vittal Setty is working as a Product Line Manager in iCETS. Vittal is the Head of Quantum COE and has created multiple working prototypes to demo quantum computing applications in different verticals. Vittal has created multiple IP solutions based on AI/ML while working on generative AI solutions. Vittal is a technocrat with over 20 years of experience delivering large transformation projects.



For more information, contact askus@infosys.com

Navigate your next