



Post-Quantum Cryptography

For Prelims: Post-Quantum Cryptography, [Quantum Computing](#), Rivest-Shamir-Adleman, ECC Elliptic Curves Cryptography, Diffie-Hellman, Quantum Bits.

For Mains: Post-Quantum Cryptography, Related Challenges and Way Forward.

[Source: TH](#)

Why in News?

Computation has transformed various facets of human civilization, from banking to warfare, however, the emergence of [Quantum Computing](#) has raised concerns about its impact on **Computer Security in the Future**.

What is Quantum Computing?

▪ About:

- Quantum computing is a **rapidly emerging technology** that harnesses the **laws of quantum mechanics** to solve problems that are too complex for classical computers.
- Quantum mechanics is a **subfield of physics that describes the behavior of particles** — atoms, electrons, photons, and almost everything in the molecular and sub molecular realm.
- It is an exciting new technology that will **shape our world tomorrow** by providing us with an edge and a myriad of possibilities.
- It is a fundamentally different way of processing information compared to today's classical computing systems.

▪ Features:

- While today's classical computers store information as **binary 0 and 1 states**, quantum computers draw on the fundamental laws of nature to carry out calculations using **quantum bits (Qubits)**.
- Unlike a bit that has to be a **0 or a 1**, a qubit can be in a combination of states, which allows for exponentially **larger calculations and gives them the potential to solve complex problems** which even the most powerful classical supercomputers are not capable of.

//

Bit

0

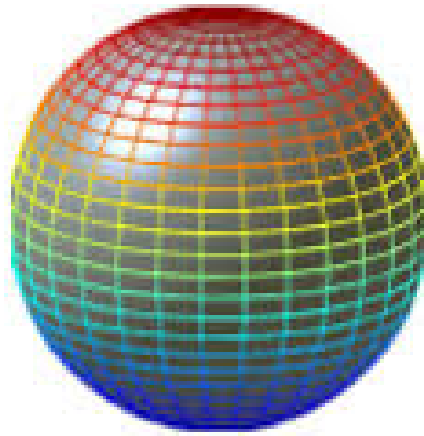


1



Qubit

0



1

▪ **Significance:**

- Quantum computers can tap **into the quantum mechanical phenomenon** to manipulate information and are **expected to shed light** on processes of molecular and chemical interactions, address difficult optimization problems, and boost the power of artificial intelligence.
- These could open the door to new scientific discoveries, life-saving drugs, and **improvements in supply chains**, logistics and the modeling of financial data.

What are the Post Quantum Concerns of Quantum Computing?

▪ **Vulnerabilities in Current Security Techniques:**

- Current security measures, such as **RSA (Rivest-Shamir-Adleman)**, **ECC (Elliptic Curves Cryptography)**, and Diffie-Hellman key exchange, rely on "hard" mathematical problems that could be broken with using **Shor's Quantum Algorithm**.
 - In 1994, **Peter Shor** developed a **quantum algorithm** that (with certain modifications) can break all of these security measures with ease.
- As quantum computing progresses, the security measures will eventually become **vulnerable, necessitating the exploration of alternative techniques**.

Note:

- **RSA** is a widely used cryptographic algorithm and **one of the fundamental building blocks of modern computer security**. RSA is primarily used for secure communication and data encryption, providing **confidentiality and authentication** in various applications.
- **Elliptic Curve Cryptography (ECC)** is a modern and widely used cryptographic technique that provides **security and efficiency for various computer security applications**.
- **Diffie-Hellman (DH)** is a key exchange algorithm used to establish a **shared secret key between two parties** over an insecure channel. It was introduced by **Whitfield Diffie** and **Martin Hellman** in 1976 and is considered one of the **fundamental building blocks of modern public-key cryptography**.

▪ **Scalability and Practicality:**

- Quantum Cryptography systems can be **challenging to implement and scale to large networks** due to the requirement for specialized hardware and tight environmental

constraints.

- **Quantum Key Distribution Over Long Distances:**

- Quantum Cryptography systems like QKD face limitations in terms of **the distance over which secure keys** can be distributed. Extending the range of secure key distribution is a significant challenge for **Quantum Cryptography researchers**.

- **Quantum Network Infrastructure:**

- Building a robust quantum network infrastructure to support Quantum Cryptography is a **complex task**.
- This involves developing reliable quantum repeaters, quantum routers, and quantum memory, among other components, to ensure the secure transmission of quantum information.

- **Quantum Cryptography in a Hybrid World:**

- As the transition to post-quantum cryptography progresses, hybrid communication scenarios will arise **where both classical and quantum communication systems coexist**.
- Ensuring seamless integration and secure communication between these systems presents a challenge.

Way Forward

- Post-quantum cryptography involves **researching alternative cryptographic techniques** to counter vulnerabilities against quantum attacks.
- The urgency in this area arises from attackers recording messages to exploit potential quantum weaknesses in the future.
- While practical and dangerous quantum computers might be decades away, preparing for a **quantum future is essential**. Governments, organizations, and individuals must transition to technologies secure against quantum attacks well in advance to safeguard sensitive data and digital infrastructure.
- The field of post-quantum cryptography continues to evolve rapidly, requiring ongoing research and collaborative efforts to **develop robust security measures that can withstand quantum attacks**. A proactive and carefully **planned transition to quantum-safe technologies will be crucial** to secure data and maintain the integrity of digital infrastructure in the quantum era.

PDF Reference URL: <https://www.drishtias.com/printpdf/post-quantum-cryptography>