Quantum-Proof Cryptography
&
Its Role In Security

04/01/2020

AMBIKA CHOUDHURY

A Technical Journalist who loves writing about Machine Learning and…

Intro

- With almost all the tech giants and academia working for the advancement of quantum computing, the day is not far when researchers will be using quantum computers for their works. Quantum algorithms have been achieving a potential speed-up for quite a few years now.
- Also, interest in the areas of quantum computing and quantum-resistant cryptography has recently increased, this is because of the milestones in the development of quantum computing hardware. These advancements in quantum information processing and quantum computing have brought about fundamental challenges to cryptography. Cryptography plays a crucial role when it comes to security for applications such as digital signatures and communication protocols.
- In this article, we will take a deep dive into quantum-proof cryptography and its role in security.

What It Is

- Quantum-proof cryptography or post-quantum cryptography usually refers to the public-key cryptographic algorithms which are secured against an attack by quantum computers. In general words, post-quantum cryptography means cryptography which is resistant to attacks by quantum computers. In the present scenario, the researchers have been focussing on mainly six approaches in the domain of post-quantum cryptography, which are:
  1. **Code-based cryptography:** Code-based cryptosystem is one of the well-known post-quantum cryptosystems. Apart from quantum resistance, code-based post-quantum cryptography is also characterised by very high algorithmic efficiency, which makes them faster than many other solutions.
  2. **Hash-based cryptography:** Lamport signatures and the Merkle signature scheme are well-known examples of hash-based cryptography.
  3. **Lattice-based cryptography:** Lattice-based cryptography is said to be secure against quantum computers. Cryptosystems based on lattice problems have made applications like fully homomorphic encryption, code obfuscation, attribute-based encryption, and other such possible to secure complex systems.
  4. **Multivariate cryptography:** Multivariate (Public-Key) Cryptography is the study of PKCs where the trapdoor one-way function takes the form of a multivariate quadratic polynomial map over a finite field.
  5. **Supersingular elliptic curve isogeny cryptography:** This technique has short public keys compared to other post-quantum candidates, and has been studied for serving as a drop-in replacement to existing Internet protocols
  6. **Symmetric key quantum resistance:** This method is resistant to attack by a quantum computer. Symmetric key quantum resistance is used to encrypt messages, files, and drives, which becomes imbalance as the keys get larger.

How It Differs - Classical Cryptography and Quantum-Proof Cryptography

- Currently, the functionalities of the cryptographic system are implemented using the Diffie-Hellman key exchange, the RSA (RivestShamir-Adleman) cryptosystem, and the elliptic curve cryptosystems. These problems can be easily solved by the quantum-proof cryptography method and thus rendering all public-key cryptosystems. Quantum-proof cryptanalysis studies attacks which are allowed to take advantage of both conventional computers and quantum computers.

How It Differs - Quantum Cryptography and Quantum-Proof Cryptography

- According to the researchers of the University of Illinois, Chicago, there are three main differences between quantum cryptography and quantum-proof cryptography. They are mentioned below:
  - Post-quantum cryptography covers a wide range of secure-communication tasks, ranging from secret-key operations, public-key signatures, and public-key encryption to high-level operations such as secure electronic voting. While, quantum cryptography handles only one task, namely expanding a short shared secret into a long shared secret.
  - Post-quantum cryptography includes some systems proven to be secure but also includes many lower-cost systems that are conjectured to be secure, while quantum cryptography rejects conjectural systems.
  - Post-quantum cryptography includes many systems that can be used for a noticeable fraction of today's Internet communication. On the other hand, quantum cryptography requires new network hardware that is impossibly expensive for the vast majority of internet users.

Challenges

- According to the researchers, currently, the post-quantum cryptography is at an infant stage and consists of three major reasons which have been concerning the post-quantum cryptography researchers. They are mentioned below:

  - Time to improve the efficiency of post-quantum cryptography.
  - Time to build confidence in post-quantum cryptography.
  - Time to improve the usability of post-quantum cryptography.

Wrapping Up

- The goal of post-quantum cryptography (also known as quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and can be interoperated with existing communications protocols and networks. Though post-quantum cryptography is far to achieve from the current date yet, one definitely requires to take some measures which could help in preventing in getting attacked by the future implementation of quantum computers in cryptography.

END