An Introductory Report on

Threshold Cryptography as an Effective Tool in Post-Quantum Security

by:

Micheal Tadese

August 2024

Quantum Computers

Quantum Computers rely on quantum level operations to function. They perform computations differently from the classical computers used today. They can also solve a lot of problems that are hard to solve by classical computers. Such big computers are also able to break the standard asymmetric cryptography encryptions existing today. These quantum computers have therefore created a need for advanced cryptography techniques.

Threshold Cryptography

Threshold Cryptography is a branch of cryptography that enables the protection of assets by sharing encryption keys among multiple computer servers. It is a method where an encryption key is splitted and distributed among multiple parties, and a subset of these parties (known as the "threshold") is able to reconstruct or decrypt the encryption and perform the required cryptographic operation. This distribution of encryption keys among a cluster of fault-tolerant systems increases the protection and security of information (or computation). Sensitive data encryption is performed so that decrypting or digital signing can be done by a group of cooperating servers such that no minority of servers is able to perform the decryption by themselves, nor will these minority be able to prevent other servers from operating as required (Goldwasser).

Post-Quantum Security

According to Thales Cloud Security (2024), Post-Quantum Cryptography (PQC), or Resistant Cryptography develops cryptographic systems that are secure against quantum and classical computers. It interoperates with existing communication protocols and networks. PQC algorithms have been undergoing development for some years now, however, NIST (National Institute of Standards and Technology) commenced the standardization of PQC algorithms in 2016. Post-quantum security, therefore entails the cryptographic techniques designed to withstand attacks from quantum computers

Use Case Scenario - Threshold Cryptography

A typical application is the storage of secrets. The secret key material of public key cryptography or a digital signature scheme are split and shared among a number (N) of computers such that a minimum of (K) numbers out of the N computers must combine their secret bits before access can be granted (Panther Academy, 2022).

Application of Threshold Cryptography to Post-Quantum Security

1. **Secret Sharing:** Secret sharing schemes like Shamir's Secret Sharing can withstand classical adversaries and is also effective for managing post-quantum encryption keys. These schemes can protect the encryption keys used in post-quantum algorithms.
2. **Distributed Key Management:** Threshold cryptography can be used to distribute the encryption keys for post-quantum algorithms among the involved parties. In simple terms, the private key of a post-quantum public-key algorithm can be divided into shares and distributed among a number of parties. Hence, only a subset of the parties can reconstruct the private key required for the decryption
3. **Fault Tolerance:** Combining threshold scheme with post-quantum algorithms ensures that even if some parties are compromised, the system remains secure and operational.
4. **Secure Multi-Party Computation (MPC):** Threshold cryptography also supports multi-party computations whereby multiple parties cooperatively compute a function while keeping their imputed data private to themselves. When combined with post-quantum techniques, the privacy and security of the computation are maintained, even when quantum adversaries are involved.
5. **Mitigating Risks:** Incorporating threshold cryptography into post-quantum cryptography increases the security layers of the system. This makes it difficult for an attacker to decrypt data without compromising multiple parties

A Use-case Scenario of MPC

A group of individuals decide to compute the average of their salary. Each individual submits his own figure without knowing the figures of the other. MPC can be used to output the average of all these salaries (Safe-DEED, 2021)

References

Thales (2020). Understanding Post-Quantum Cryptography (PQC). Thales Cloud Security. Available at: https://www.youtube.com/watch?v=vTSbeL0q530

Goldwasser S. (). Threshold Cryptography. MIT CSAIL Theory of Computation Available at: https://toc.csail.mit.edu/node/217

Panther Academy (2022). Threshold Cryptography, MPC, and MultiSigs: A Complete Overview. Available at: https://blog.pantherprotocol.io/threshold-cryptography-an-overview/

Safe-DEED (2021). Introduction to Multi-Party Computation (MPC or SMPC). Available at: https://www.youtube.com/watch?v=90jcXCHsBF0