ð Threshold Network

In principle, a Threshold Network is a cryptographic system designed to enhance security and trust by distributing control and decision-making across multiple parties. In such a network, sensitive operations, such as decryption or signing, require collaboration among a subset of participants, rather than relying on a single entity.

Conceptâ

In Fhenixâs Nitrogen testnet, the Threshold Network performs decryption operations. The Threshold Network is currently initialized by a Trusted Dealer (in the future, we plan to eliminate the Trusted Dealer). The Trusted Dealer initially generates a key. Then, the Dealer uses Shamir's Secret Sharing cryptographic algorithm to generate Secret Shares of the key to share among individual members. Each member holds exactly one secret share. To perform a decryption, the secret shares are used to perform partial decryptions through a multiparty computation (MPC) protocol. These partial decryptions are then combined into the final plaintext. The protocol uses a T-out-f-N scheme, meaning that T parties out of a total of N existing parties need to agree and work together to perform a decryption. The benefit of this approach is that a single entity (Threshold Network âmemberâ) cannot decrypt the ciphertext, since it is necessary to have a consensus in order to decrypt, which provides the end user with additional protection from malicious actors.

Note The Threshold Network in Nitrogen requires 3 out of 4 parties to decrypt ciphertexts.

Authenticationâ

A Threshold Network authentication mechanism is important to differentiate between valid and invalid (or malicious) decryption requests. The authentication mechanism ensures that no party can decrypt data that is not supposed to be decrypted. Authentication is currently under development and not yet included in this testnet. It will be added in future Fhenix versions.

Threshold Network in Nitrogenâ

In Nitrogen, the Threshold Network is used bySecurity Zone 0 (which is the default). Edit this page

Previous ð§® FHE Schemes Overview Next Details