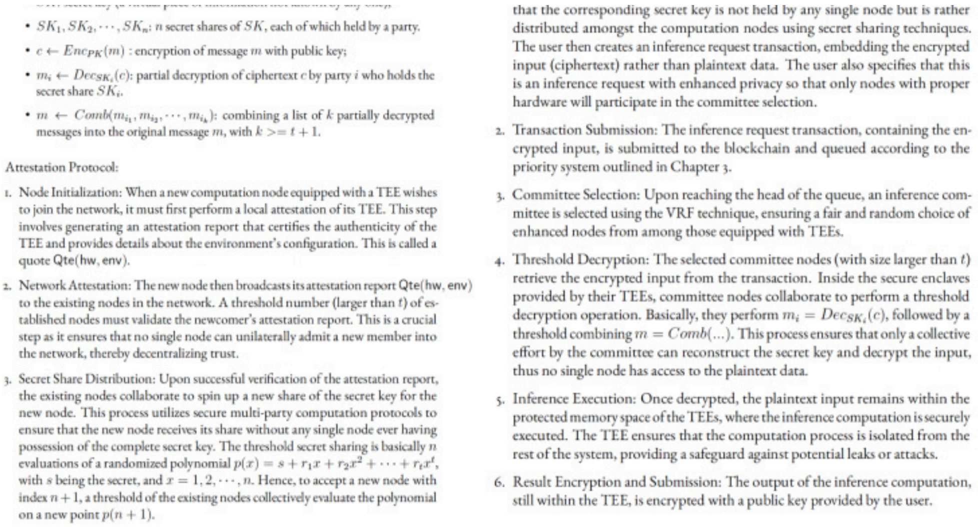
Playground Technology Research Token Docs Developers DNA X

# Nesa Research

Our proprietary research in cryptography and AI. A small selection of papers authored by Nesa's founders.



- $SK_1, SK_2, \cdots, SK_n$: $n$ secret shares of $SK$, each of which held by a party.
- $c \leftarrow Enc_{PK}(m)$ : encryption of message $m$ with public key;
- $m_i \leftarrow Dec_{SK_i}(c)$: partial decryption of ciphertext $c$ by party $i$ who holds the secret share $SK_i$.
- $m \leftarrow Comb(m_{i_1}, m_{i_2}, \cdots, m_{i_k})$: combining a list of $k$ partially decrypted messages into the original message $m$, with $k >= t + 1$.

Attestation Protocol:

1. Node Initialization: When a new computation node equipped with a TEE wishes to join the network, it must first perform a local attestation of its TEE. This step involves generating an attestation report that certifies the authenticity of the TEE and provides details about the environment's configuration. This is called a quote Qte(hw, env).
2. Network Attestation: The new node then broadcasts its attestation report Qte(hw, env) to the existing nodes in the network. A threshold number (larger than $t$) of established nodes must validate the newcomer's attestation report. This is a crucial step as it ensures that no single node can unilaterally admit a new member into the network, thereby decentralizing trust.
3. Secret Share Distribution: Upon successful verification of the attestation report, the existing nodes collaborate to spin up a new share of the secret key for the new node. This process utilizes secure multi-party computation protocols to ensure that the new node receives its share without any single node ever having possession of the complete secret key. The threshold secret sharing is basically $n$ evaluations of a randomized polynomial $p(x) = s + r_1x + r_2x^2 + \cdots + r_tx^t$, with $s$ being the secret, and $x = 1, 2, \cdots, n$. Hence, to accept a new node with index $n + 1$, a threshold of the existing nodes collectively evaluate the polynomial on a new point $p(n + 1)$.

that the corresponding secret key is not held by any single node but is rather distributed amongst the computation nodes using secret sharing techniques. The user then creates an inference request transaction, embedding the encrypted input (ciphertext) rather than plaintext data. The user also specifies that this is an inference request with enhanced privacy so that only nodes with proper hardware will participate in the committee selection.

2. Transaction Submission: The inference request transaction, containing the encrypted input, is submitted to the blockchain and queued according to the priority system outlined in Chapter 3.
3. Committee Selection: Upon reaching the head of the queue, an inference committee is selected using the VRF technique, ensuring a fair and random choice of enhanced nodes from among those equipped with TEEs.
4. Threshold Decryption: The selected committee nodes (with size larger than $t$) retrieve the encrypted input from the transaction. Inside the secure enclaves provided by their TEEs, committee nodes collaborate to perform a threshold decryption operation. Basically, they perform $m_i = Dec_{SK_i}(c)$, followed by a threshold combining $m = Comb(...)$. This process ensures that only a collective effort by the committee can reconstruct the secret key and decrypt the input, thus no single node has access to the plaintext data.
5. Inference Execution: Once decrypted, the plaintext input remains within the protected memory space of the TEEs, where the inference computation is securely executed. The TEE ensures that the computation process is isolated from the rest of the system, providing a safeguard against potential leaks or attacks.
6. Result Encryption and Submission: The output of the inference computation, still within the TEE, is encrypted with a public key provided by the user.

# Nesa Protocol Whitepaper

CORE TECHNOLOGY OVERVIEW

Playground Technology Research Token Docs Developers DNA X

Playground Technology Research Token Docs Developers DNA X

GITHUB CAREERS TEAM TERMS PRIVACY CONTACT