eAddress

A representation of an encrypted address using Fully Homomorphic Encryption. It consists of 5 encrypted 32-bit unsigned integers (euint32).

struct Eaddress { euint32[5] values; }

ConfAddress

toEaddress

function toEaddress(address addr) internal pure returns (struct Eaddress) Encrypts a plaintext Ethereum address into its encrypted representation (eaddress).

Iterates over 5 chunks of the address, applying a bitmask to each, then encrypting withFHE .

Parameters

Name Type Description addr address The plain Ethereum address to encrypt

Return Values

Name Type Description [0] struct Eaddress eaddr The encrypted representation of the address

unsafeToAddress

function unsafeToAddress(struct Eaddress eaddr) internal pure returns (address) Decrypts aneaddress to retrieve the original plaintext Ethereum address.

This operation should be used with caution as it exposes the encrypted address.

Parameters

Name Type Description eaddr struct Eaddress The encrypted address to decrypt

Return Values

Name Type Description [0] address The decrypted plaintext Ethereum address

resestEaddress

function resestEaddress(struct Eaddress eaddr, euint32 ezero) internal pure Re-encrypts the encrypted values within aneaddress .

The re-encryption is done to change the encrypted representation without altering the underlying plaintext address, which can be useful for obfuscation purposes in storage.

Parameters

Name Type Description eaddr struct Eaddress The encrypted address to re-encrypt ezero euint32 An encrypted zero value that triggers the re-encryption

equals

function equals(struct Eaddress lhs, address payable addr) internal view returns (ebool) Determines if an encrypted address is equal to a given plaintext Ethereum address.

This operation encrypts the plaintext address and compares the encrypted representations.

Parameters

Name Type Description lhs struct Eaddress The encrypted address to compare addr address payable The plaintext Ethereum address to compare against

Return Values

Name Type Description [0] ebool res A boolean indicating if the encrypted and plaintext addresses are equal

conditionalUpdate

function conditionalUpdate(ebool condition, struct Eaddress eaddr, struct Eaddress newEaddr) internal pure returns (struct Eaddress) [Edit this page](#)