Key Derivation & Encryption Techniques

HKDF-SHA256

To do deterministic key generation inside the SGX enclave Secret Network leverages HDKF-SHA256[1] [2] . HDKF-SHA256 is a key derivation function for symmetric (private key) encryption. The function generates a 256-bit encryption key from a common public "salt" and a piece of Input Key Material (IKM). Thesalt [1] for the use in the Secret Network encryption schemes is chosen to be the Bitcoin's block halving hashhkdf_salt = 0x000000000000000000024bead8df69990852c202db0e0097c1a12ea637d7e96d

HDKF is commonly used to extract entropy from a larger source and deliver smaller output (eg. an encryption key) as well as expand already existing random output into a larger cryptographic-ally independent output. The deterministic keys coming from HDKF can be shared amongst network participants without revealing the underlying randomness. In the end this symmetric function is used to ensure safety for the pseudo-randomconsensus_seed and secure the shared secrets of the network participants.

The output of the HDKF is a curve25519 private key, which can be used to derive a public key as well.

Elliptic-curve Diffie-Hellman

Elliptic-curve Diffie-HellmanECDH (x25519) is a key derivation protocol designed to support assymetric encryption by returning a public-private key pair. ECDH allows for sharing secrets over public channels as one needs the private key to decrypt information while using the public key for sending the encrypted message. These Shared secrets can be used by both parties to then set up subsequent symmetric keys with functions like HDKF as mentioned above. ECDH delivers 256 bits Curve25519 encryption keys which have a probabilistic level of security of 2^128.

ECDH also allows for a special way of generating shared secrets which involves using the private and public key of both participants. Participant A and B can create a shared secret by doing:ecdh(Apriv, Bpub) == ecdh(Bpriv, Apub) , this feature is called "key-exchange" and is the basis of sharing information amongst network participants on Secret Network.

For additional explanation of Diffie-Hellman, check outthis video .

AES-128-SIV - "Rijndael"

Advanced Encyption Standard (AES) is an encryption algorithm slightly varying from the block cipher "Rijndael" set to a fixed 128 bits size block. The algorithm generates 256 bit encryption keys which offer very high security guarantees.

The AES-SIV encryption scheme is a perfect addition to the ECDH keypairs used in SGX enclaves. The combination allows for sharing encrypted data amongst nodes and protecting the private entropy of the protocol.AES-128-SIV was chosen to prevent IV misuse by client libraries. The algorithm does not pad ciphertext which leaks information about the plaintext, in particular its size.

Last updated1 year ago On this page *HKDF-SHA256 * Elliptic-curve Diffie-Hellman * AES-128-SIV - "Rijndael"

Was this helpful? Edit on GitHub Export as PDF