Semaphore

Cedoor

Devcon 2024

Structure

- What is Semaphore?
- Semaphore V4
- Roadmap

What is Semaphore?

Semaphore is a **zero-knowledge protocol** that allows users to prove their **membership** in a **group** and send **messages** such as votes or feedback without revealing their **identity**.

It also provides a simple **nullifier** mechanism to prevent users to re-use existing proofs (i.e. to nullify proofs).

It works **off-chain** and on **EVM compatible-chains**.

Semaphore V4

Semaphore V4 introduces two significant protocol updates:

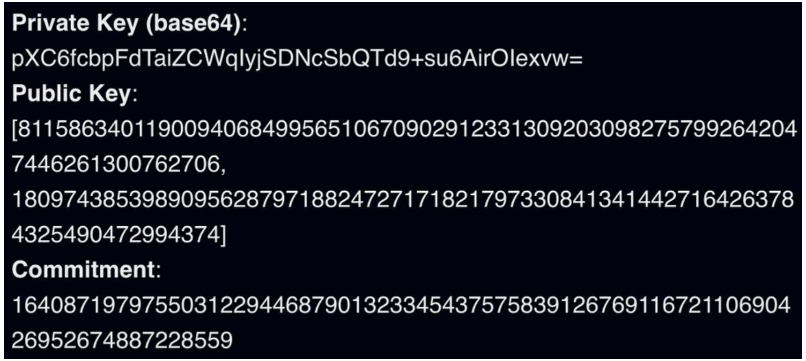
- EdDSA key pair -> New Identity schema (replaces Poseidon hash)
- LeanIMT -> New optimized Incremental Merkle tree for groups

github.com/semaphore-protocol/semaphore/releases/tag/v4.0.0

Identities

A Semaphore V4 identity consists of an **EdDSA** public/private key pair and a commitment.

Now with Semaphore v4 you can create and verify signatures out of the box.



```
Private Key (base64):
pXC6fcbpFdTaiZCWqIyjSDNcSbQTd9+su6AirOIexvw=
Public Key:
[8115863401190094068499565106709029123313092030982757992642047446261300762706,
18097438539890956287971882472717182179733084134144271642637843254904729943374]
Commitment:
16408719797550312294468790132334543757583912676911672110690426952674887228559
```

docs.semaphore.pse.dev/guides/identities

LeanIMT

Semaphore V4 uses the LeanIMT data structure for group operations, an improvement over the IMT used in v3.

Two key improvements of the LeanIMT over the IMT:

- **Zero hashes** are no longer required.
- **Dynamic depth** is now supported.

Learn More

GitHub

semaphore.pse.dev/github

Docs

docs.semaphore.pse.dev

Telegram

semaphore.pse.dev/telegram

Website

semaphore.pse.dev