Anonymous signaling on Ethereum

Why we need anonymity, and how we can achieve it

Cedoor Software engineer, Privacy and Scaling Explorations

Invisibility is a superpower

"I don't know why people are so keen to put the details of their private life in public; they forget that invisibility is a superpower."

-Banksy

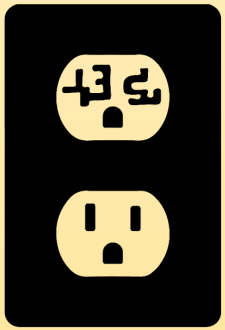
Anonymity can help us to:

- **Limit power**: knowledge is power, protecting it makes us stronger.
- **Promote freedom of speech**: knowing that our data and identity are safe encourages us to think freely.
- **Safeguard reputation**: our ideas should not be judged based on who we are, but rather on what we have to say.

Drawbacks

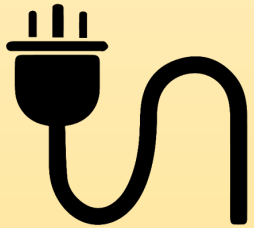
Complexity

- Still too niche technologies
- Lack of practical development tools



Indifference

- Lack of awareness
- Still few education resources



Solutions

Privacy by default

Privacy and cryptography should be the backbone of the Internet infrastructure.

Education

People should be more aware of the technological and social complexity of the world we live in.

Developer experience

Developers need to be able to rely on robust, easy-to-use tools.

Semaphore

Semaphore is a zero-knowledge protocol that lets users prove their membership in a **group** and send **signals** such as votes or endorsements without revealing the user's original **identity**.

And additionally, it provides a simple mechanism to prevent **double-signaling**.

Identities

Each identity is made up of:

- Two secret values: **Trapdoor** and **Nullifier**
- One public value: **Commitment**

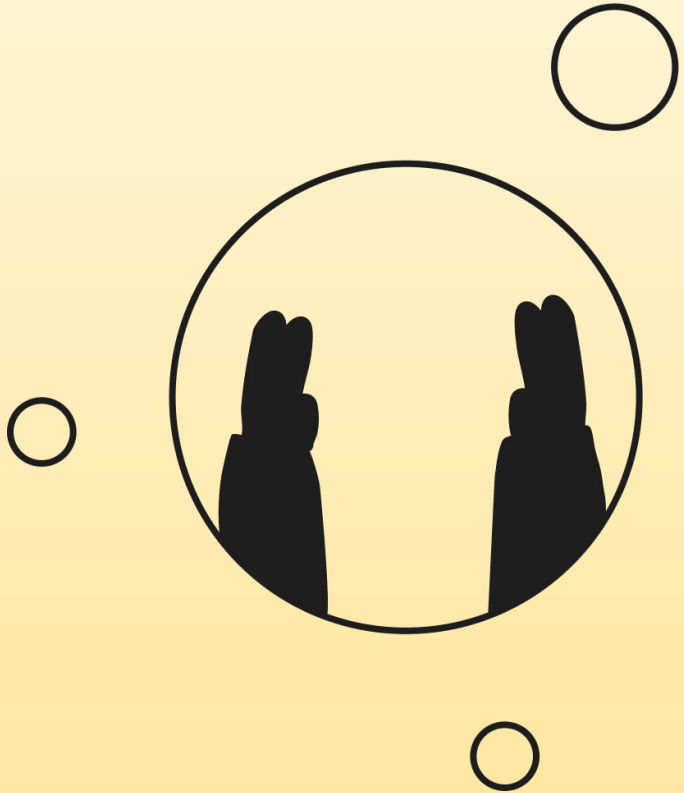
```
import { Identity } from "@semaphore-protocol/identity"

// Random
const { trapdoor, nullifier, commitment } = new Identity()

// Deterministic
const identity = new Identity("secret-message")
```

https://semaphore.appliedzkp.org/docs/guides/identities

Groups

Groups can be thought of as **anonymity sets**. They are a way to establish necessary **trust** among participants.

Semaphore groups are **binary Merkle trees**, in which the leaves are identity commitments and all the other nodes in the tree are hashes of their two child nodes.



Groups

Semaphore groups can be created off-chain with a JavaScript library, or on-chain with the Semaphore contracts.

```
import { Group } from "@semaphore-protocol/group"

const group = new Group()

group.addMember(commitment)
```

```
contract Greeter {
    ISemaphore public semaphore;
    uint256 public groupId;

    constructor(address semaphoreAddress, uint256 _groupId) {
        semaphore = ISemaphore(semaphoreAddress);
        groupId = _groupId;

        semaphore.createGroup(groupId, 20, 0, address(this));
    }
}
```

https://semaphore.appliedzkp.org/docs/guides/groups

ZK-Proofs

After creating their identity and joining a group users can anonymously prove that they are members of that group and send **signals**, such as votes, endorsements or any message.

To generate a valid proof we also need an **external nullifier**. The hash of this value and the identity nullifier is the **nullifier hash**, which can be used to avoid double-signaling.

ZK-Proofs

Zero-knowledge proofs can be generated off-chain with a JavaScript library. They can then be verified both on-chain and off-chain.

```
import { generateProof, verifyProof } from "@semaphore-protocol/proof"

const externalNullifier = 42n
const greeting = "Hello world"

const fullProof = await generateProof(identity, group, externalNullifier, greeting)

await verifyProof(fullProof, group.)
```

```
contract Greeter {

    function greet(
        bytes32 greeting,
        uint256 merkleTreeRoot,
        uint256 nullifierHash,
        uint256[8] calldata proof
    ) external {
            semaphore.verifyProof(
                    groupId,
                    merkleTreeRoot,
                    greeting,
                    nullifierHash,
                    groupId,
                    proof
            );
}
```

https://semaphore.appliedzkp.org/docs/guides/proofs

Semaphore in use today

Unirep

Unirep is a protocol which allows anonymous members of a group to give, receive, and prove reputation without revealing their identity.

https://docs.unirep.io

ZKitter

Anonymous social network where people can post and chat without losing their real-life reputation.

https://zkitter.com

TAZ apps

Experimental Semaphore applications to learn through experience about privacy and anonymity at Devcon VI.

https://taz.appliedzkp.org

Future plans

Semaphore will continue to be developed and improved over time. Some potential future directions include:

- Create an infrastructure to manage groups
- Create attestation contracts for decentralized groups
- Investigate other zero-knowledge technologies and proving systems
- Continue improving the developer experience and documentation
- Create a strong community

Thank you!

Semaphore grants

Semaphore website

Cedoor Software engineer, Privacy and Scaling Explorations me@cedoor.org @cedoor_