Zero-knowledge proofs

A zero-knowledge proof is a cryptographic mechanism to prove you know a secret without revealing the secret. This is possible through the use of complex math under the hood. Thanks to the cryptographers who worked on the moonmath for us.

A simple example of a ZKP is that you can cryptographically prove you are above 18 years of age without revealing your date of birth, actual age or any other information.

A ZKP should have the following properties:

- Completeness: If you are above 18, verifier will be convinced with a high probability.
- Soundness: Very low probability of cheating.
- Zero knowledge: Your exact age is not shared.

Why does World ID use ZKPs?

After the orb verifies you are a unique human, your identity commitment is added to a public list of verified humans. Everytime you want to prove you are a unique person, your World app generates a ZKP that proves you know the secret toan identity commitment, without revealing which one. Holistically, World ID ZKPs prove these three things:

- Membership: "I'm a member of this group". You prove you are a member of the verified identities list.
- One-shot: "I haven't done this beforein this context
- ". This is achieved throughnullifiers
- . Nullifiers are random numbers, unique to each user for each context (i.e. for each action ID).
- Signal: "I want to include this message". This allows the user to add extra data to the request. It could be a receiver address when claiming an airdrop, or a vote when participating in governance. This mitigates an attack where an attacker could intercept a transaction with a proof and change the vote.

How does it work?

A user's World ID lives in their device, and only in their device. The user installs a compatible identity wallet (such as theWorld App). A unique and random private key is generated on-device, where it is securely stored. Identity wallets may incorporate their own recovery mechanisms, however Protocol-level recovery is being implemented soon.

From the user's private key, a publicidentity commitment is generated and published on-chain (currently Ethereum Mainnet), which acts as the source of truth for the protocol. An identity commitment is analogous to a public key in an asymmetric key-pair, or a wallet address, but in the World ID protocol this value is not broadly shared. The private key is used as input to each World ID verification, specifically as part of theZKP .

The user's wallet (e.g. World App) generates a ZKP for every verification a user makes. Verifications cannot be linked across applications or actions, which means that the user's privacy is cryptographically protected.

After a user verifies, anullifier hash is returned to the application. The nullifier hash is the user's unique identifier for the application (and the action, if usingIncognito Actions). Nullifiers are unique to the application, and cannot be linked to other nullifiers from the same person, even resistant to colluding applications.

If you want to learn more about ZKPs, here is a great resourcehttps://github.com/ingonyama-zk/ingopedia .