Zero-Knowledge Identity Verification

Térence Miralves

Ugo Majer

Christophe de Pontac

Alban Naulin

Sommaire

- Objectifs
- Choix d'implementation
- Architecture technique
- Securite cryptographique

Objectifs

Maintenir la **confidentialité** des données personnelles

Vérifier cette preuve sans révéler d'informations sensibles

Prouver qu'une personne possède un permis de conduire d'un certain type

Rapidite de verification et de generation de la preuve

Garantir **l'intégrité** grâce aux zk-SNARKs (non-interactive ZKP)

Introduction aux preuves ZK

- Prouver une information sans la révéler
- Types : zk-SNARKs, zk-STARKs, Bulletproofs
- Applications : Zcash, vote électronique, contrôle d'accès privé

Introduction aux preuves ZK - Commitments

Commitments {*commit*, *open*, *verify*}

A prover $\mathcal{P}$ hides a secret in the commit phase
and opens it to a verifier $\mathcal{V}$ in the open phase.

Commit phase

$\mathcal{P}$ computes and sends *com* to $\mathcal{V}$:
r = *random*()
com = *commit*(*secret*, *r*)

Hiding

$\mathcal{V}$ cannot find clues of (*secret*, *r*) from *com* at the commit phase.

After some confirmations...

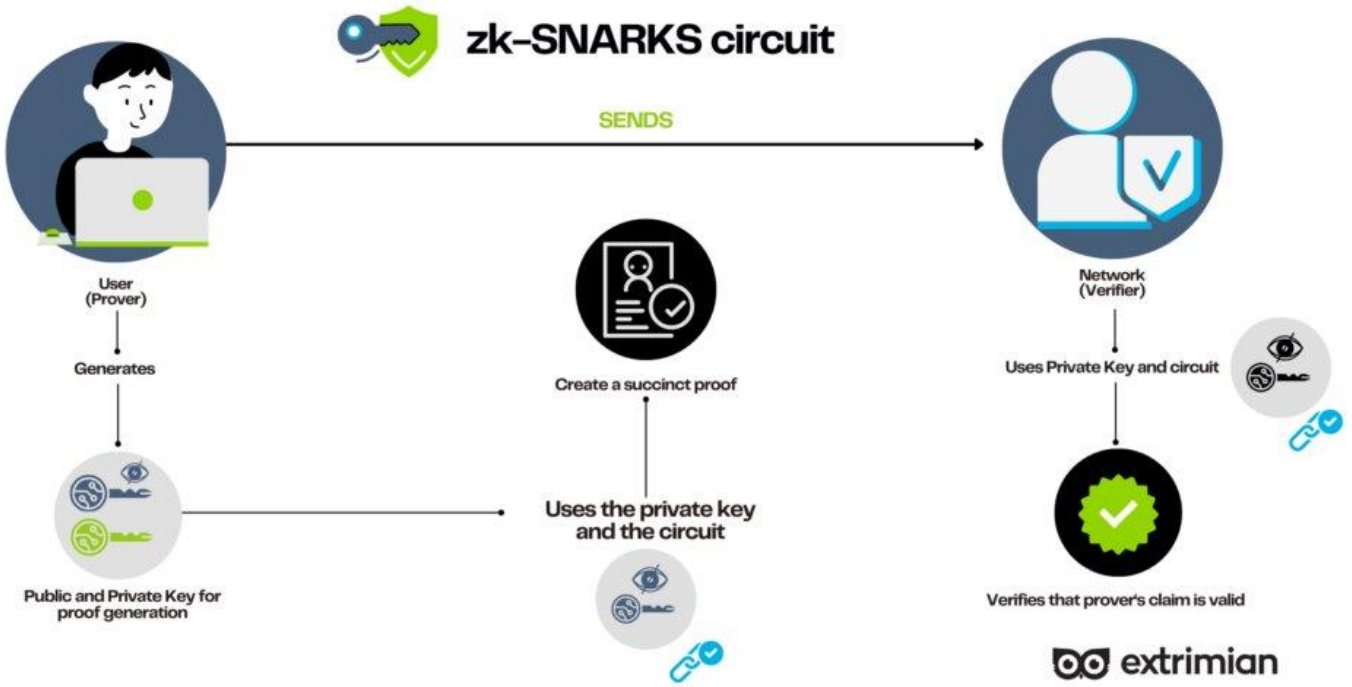
Open phase

$\mathcal{P}$ *open* *secret* and r to $\mathcal{V}$.
$\mathcal{V}$ *verify*(*com*, *secret*, *r*) = *T* / *F*

Binding

$\mathcal{P}$ cannnot open (*secret'*, *r'*) =/= (*secret*, *r*) such that
T = *verify*(*com*, *secret'*, *r'*)

Choix d'implémentation



==> circom
CIRCUIT COMPILER

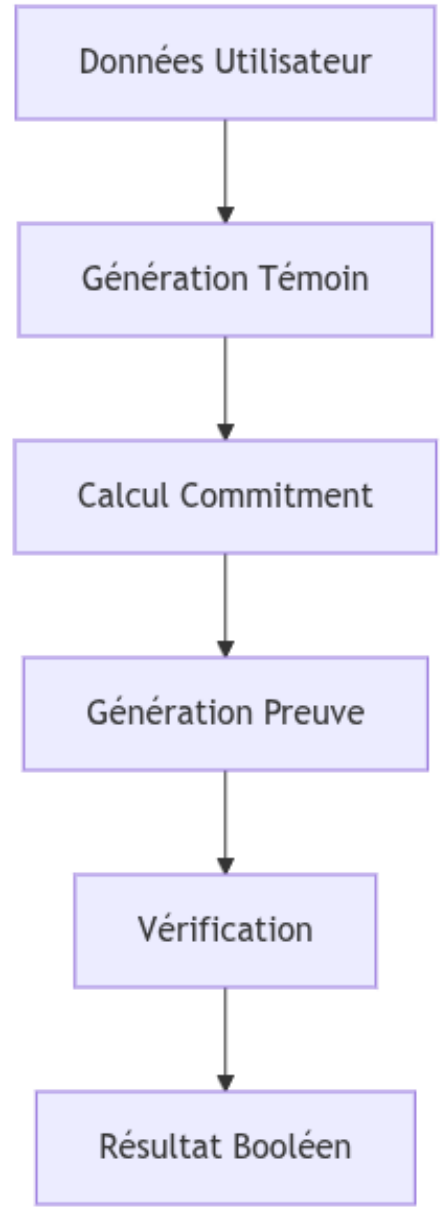
snarkjs

Architecture technique

Circuit Circom

- Concaténation : Assemble toutes les données
(nom + prénom + date de naissance + type de permis + date d'expiration + nonce)
- Hash SHA256 : Calcule le hash des données concaténées
- Vérification : Le verificateur de confiance Compare avec le commitment public
- Contrainte ZK : Vérifie que le permis est de type 'A' et prouver l'age >= 18

Trusted setup (powers of tau)
- génération et vérification de preuve



Flux de données

Sécurité cryptographique

Nonce : Évite les attaques par rejeu et permet l'unicite

zk-SNARKs Groth16 : Preuve zero-knowledge

Hash SHA256 : Garantit **l'intégrité** des données

Trusted Setup : Cérémonie Powers of Tau

Conclusion