CRYPI: Zero-Knowledge Identity Verification

Groupe 3

Clement BRUN, Lucas SIAUVE, Elsa François, Matthieu Tirloy

Sommaire

Introduction au Zero-Knowledge Identity Verification

Définition

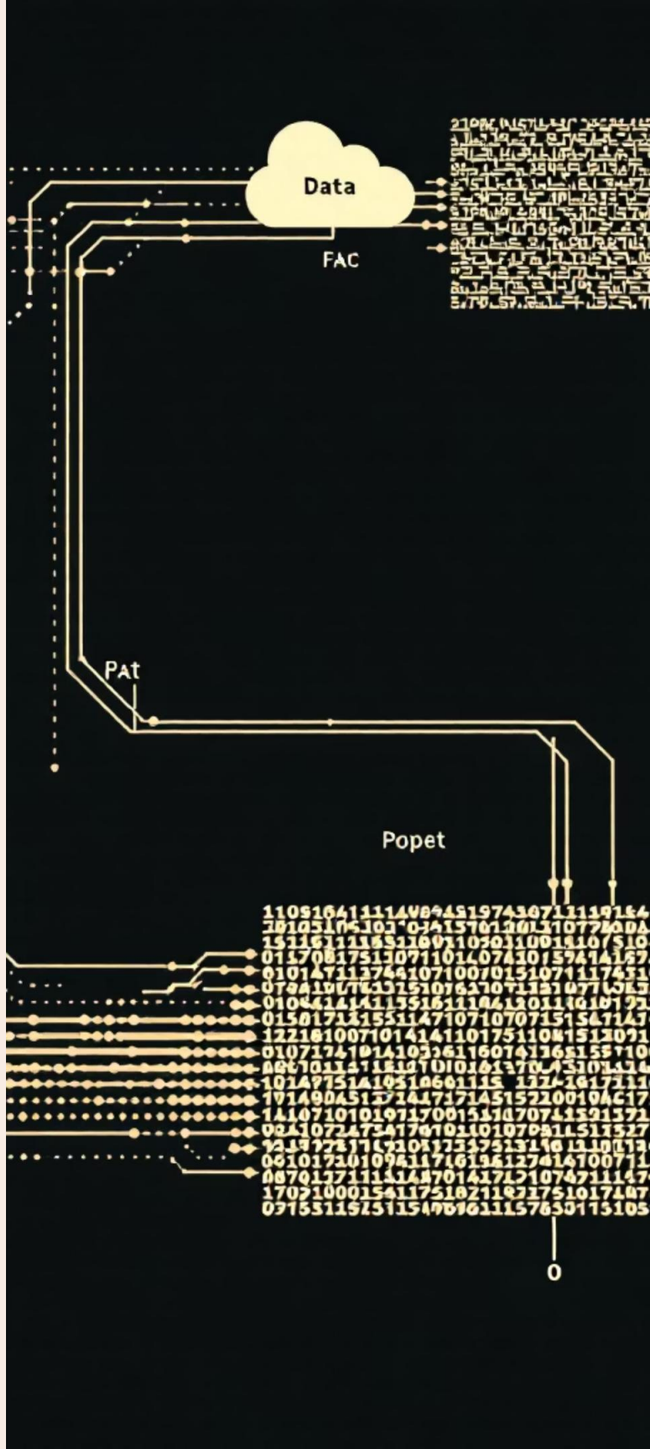
Permet de prouver une propriété d’une identité (comme être majeur, avoir un permis valide…) sans révéler d’information sensible comme le nom ou la date de naissance

Importance du ZKIV

- Protéger la vie privée dans les systèmes numériques- Limiter l’exposition inutile d’informations personnelles- Répondre aux exigences RGPD et aux enjeux de cybersécurité

Exemples d’usage concrets

- Accéder aux sites adultes sans donner sa date de naissance- Louer une voiture sans montrer son identité complète- Systèmes KYC (Know Your Customer) avec anonymat préservé



Implémentation des ZKP dans le projet

- Utilisation de la bibliothèque **Circom** pour la construction de circuits de preuve (majeur / permis valide)
- Hash des attributs personnels (nom, prénom, date de naissance, etc.) avec la fonction **Poseidon**
- Création d’un engagement cryptographique pour chaque utilisateur à partir de ses données et d’un **nonce aléatoire**
- Génération de preuves via le protocole **Groth16**, prouvant des propriétés sans révéler les données sources
- Intégration avec une interface Web pour la vérification en ligne des preuves ZKP
- Circuits séparés pour l’âge et le permis, avec tentative de fusion non aboutie dans le prototype

Résultats obtenus

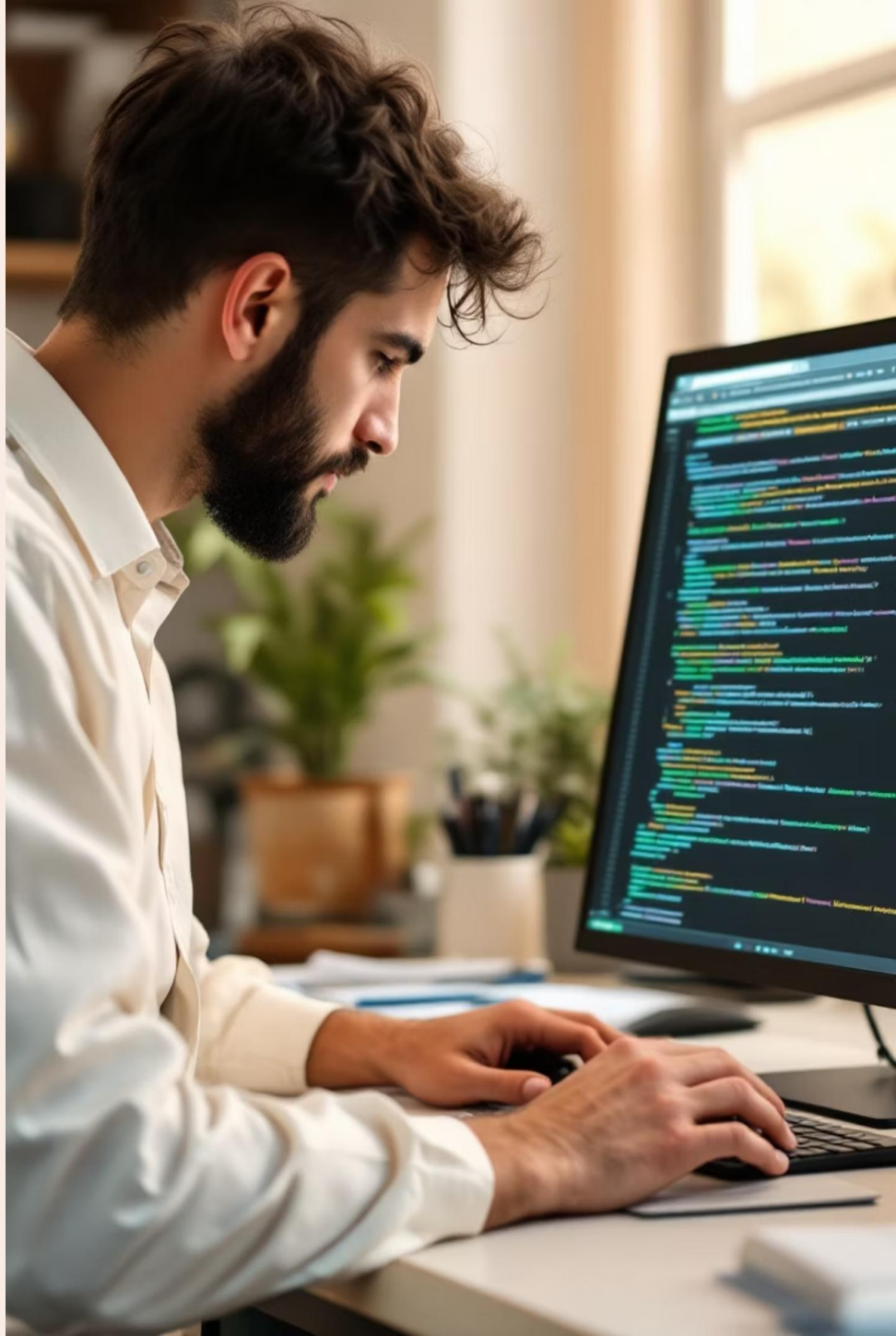
1 TEST EN LIVE

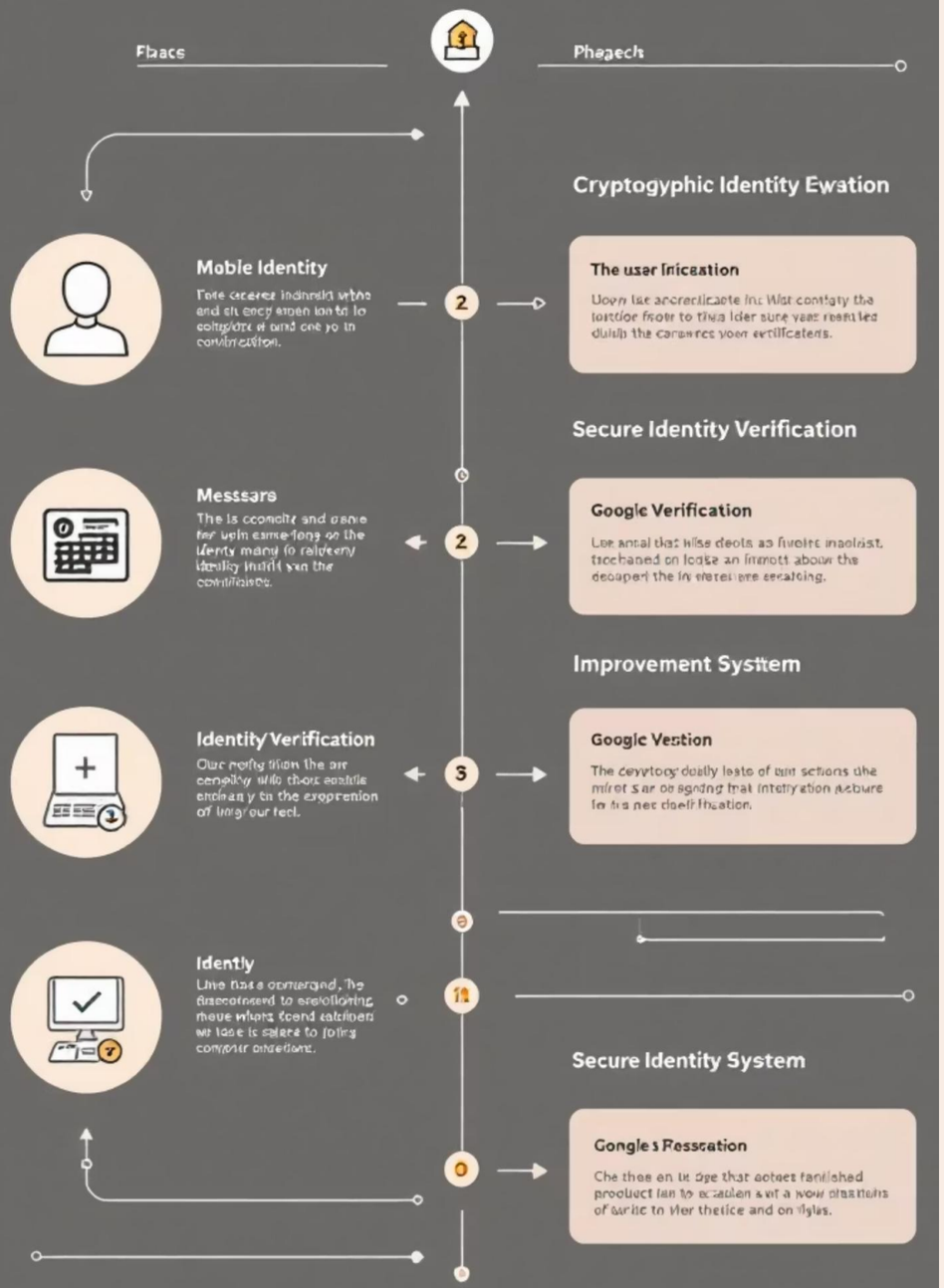
2 LIMITES

- Fusion difficile des circuits (âge et permis)- Dépendance critique à un nonce sécurisé- Confiance centralisée sur l’émetteur

3 AMÉLIORATION

- Créer un circuit unique regroupant tous les attributs- Renforcer la génération et la gestion du nonce- Améliorer l’intégration et l’interface utilisateur





Conclusion

Le système Zero-Knowledge Proof permet de prouver des attributs d'identité sans divulguer de données sensibles, assurant ainsi une forte confidentialité

Notre projet montre la faisabilité technique avec des preuves compactes et vérifiables rapidement grâce à l'utilisation de la bibliothèque CRICOM et du protocole Groth16

Malgré des résultats prometteurs, des défis subsistent, notamment la fusion des circuits et la gestion sécurisée des nonces, qui nécessitent des améliorations pour un déploiement à grande échelle

En combinant rigueur cryptographique et optimisation technique, ce type de solution peut révolutionner la vérification d'identité tout en respectant la vie privée des utilisateurs