RAPPORT

Sujet : CRYPI
Groupe3

Groupe N°3

Lucas SIAUVE
Clément BRUN
Elsa FRANCOIS
Matthieu TIRLOY

Table des matières

1 Introduction

Ce rapport présente ce que nous avons réalisé pour la conception et l'implémentation de notre un mécanisme de vérification de preuve à divulgation nulle de connaissance (ZKP). C'est un mécanisme qui permet de faire de la vérification d'identité, d'âge, et autres caractéristique personelles, tout en ne dévoilant aucune connaissance à l'acteur qui souhaite les vérifier. Dans notre société où la divulgation de données personelles et sensibles est devenue un point d'intérêt pour la majorité des utilisateurs, nous proposons une implémentation de cette méthode où les attributs d'identité, engagés par une autorité de confiance via un hachage cryptographique, peuvent être prouvés sans révéler d'informations suplémentaires. Ce projet nous permet finalement d'explorer les fondements de la cryptographie, de réaliser une mise en œuvre pratique à l'aide d'une bibliothèque ZKP, et d'analyser ensuite les forces et limites de notre système.

2 Le modèle d'engagement d'identité

2.1 Définition

Le modèle d'engagement d'identité consiste à représenter de manière sécurisée et confidentielle les attributs personnels d'un individu sous forme d'un engagement cryptographique. Cet engagement sert de preuve immuable des données d'identité sans nécessiter leur divulgation directe.

Une autorité de confiance (le plus souvent une organisation apparentée au gouvernement) collecte les attributs d'identité d'un utilisateur. Dans notre cas, les attributs sont définis : le nom, le prénom, la date de naissance, la catégorie du permis de conduire, la date d'expiration et un nonce qui est aléatoire. Ces données sont ensuite concaténées et soumises à un algorithme de hachage selon le format prédéfini suivant :

$$H(\texttt{name} \parallel \texttt{surname} \parallel \texttt{date\_of\_birth} \parallel \texttt{expiration\_date} \parallel \texttt{nonce})$$

Ce modèle d'engagement présente plusieurs propriétés intéressantes et essentielles :

- **Confidentialité :** La fonction de hachage étant à sens unique, il est impossible de retrouver les données originales à partir de l'engagement seul, protégeant ainsi directement les données de l'utilisateur.
- **Intégrité :** Toute modification des attributs d'identité entraînerait une modification du hash final, garantissant ainsi une intégrité des données fournies.
- **Non reproductible :** L'ajout d'un nonce comme une valeur aléatoire non divulguée évite que deux utilisateurs avec des données similaires produisent le même engagement, ou même qu'un attaquant parvienne à retrouver les données de l'utilisateur en brute forçant le hash en essayant plusieurs combinaisons de données en entrée.

2.2 Réflexions sur les impacts la publication publique de l'engagement

Quels sont les avantages pour la protection de la vie privée d'une telle publication ?

- **Protection des données personnelles :** Le hachage agit comme une preuve numérique non réversible et non altérable (intégrité conservée). Il permet de prouver que des données existent, sont vérifiables par une preuve, tout en n'étant pas dévoilées au public.
- **Vérification décentralisée :** Toute entité disposant du hachage peut vérifier une preuve sans avoir accès aux données originales. La confiance qu'elle accorde à la preuve vient directement de l'autorité de vérification, qui est la seule à recevoir les données sensibles dans le processus de vérification.
- **Transparence et auditabilité :** L'engagement étant public, il est vérifiable par des tiers sans compromission de la vie privée. Cela permet une transparence quasi totale dans la gestion des identités, et surtout dans le respect des données personelles et sensibles.

Quels en sont les risques ?

- **Corrélation entre engagements :** Sans l'ajout d'un nonce unique, aléatoire et suffisament grand, deux engagements issus de données identiques généreraient le même hash. Cela rendrait possibles des corrélations entre utilisateurs, dévoilant ainsi à certains utilisateurs les données personelles d'autres utilisateurs.
- **Attaques par dictionnaire ou force brute :** Si certaines données (comme le nom ou la date de naissance) sont prévisibles voire connues, un attaquant pourrait tenter de reconstituer l'engagement en testant toutes ou une série de combinaisons possibles. À nouveau, sans l'utilisation d'un hash suffisamment robuste, cela compromettrait dangereusement les engagements publiés, qui pourraient être "brisés" par calculs de hash en série par exemple.
- **Fuite d'information par méta-données :** Cette hypothèse, moins probable mais tout de même envisageable, suppose que des informations sur les utilisateurs pourraient être divulgués lors des processsus et manipulation des données de l'autorité de confiance. Elle deviendrait le maillon faible de la chaîne et la cible privilégiée des attaquants. Le moment de la publication, la structure des engagements ou l'ordre d'insertion dans la base publique sont autant d'éléments qui pourraient potentiellement révéler des indices sur les utilisateurs.

Sous quelles conditions ce modèle peut-il être considéré comme sûr ?

Pour que ce modèle soit considéré comme sécurisé, plusieurs conditions doivent être réunies :

- **Fonction de hachage robuste :** La confidentialité des données repose premièrement sur la robustesse du hash publié. La fonction de hachage utilisée doit donc nécessairement être résistante aux collisions, aux attaques de type "pré-images" et à toutes les attaques suscpetibles d'être utilisées pour briser les hashs publiés. Sans cette condition, ce modèle est tout simplement inenvisageable.
- **Utilisation d'un nonce cryptographiquement sécurisé :** Le nonce doit être aléatoire et de taille suffisante, de manière à ce qu'il soit différent pour chaque engagement, permettant ainsi de garantir l'unicité et empêcher les attaques par *rainbow table*.
- **Canal sécurisé pour la transmission des données privées :** Bien que l'engagement soit public, les éléments utilisés dans les preuves doivent rester strictement confidentielles et côté utilisateur. Ainsi, il est nécessaire que n'importe quel utilisateur pouisse établir une connexion sécurisée avec l'autorité de confiance lors de l'envoi des données privées.

3 Critères et processus de sélection de la bibliothèque ZKP

Le choix de la bibliothèque ZKP s'est porté sur CRICOM, en fonction des critères suivants :

- **Simplicité d'utilisation** : interface claire, bonne documentation, adaptée à un contexte pédagogique.
- **Fonctionnalités adaptées** : prise en charge des opérations nécessaires (comparaison d'âge, égalité de catégories, recalcul de hash).
- **Compatibilité avec Poseidon** : fonction de hachage efficace et optimisée pour les circuits ZKP.
- **Pipeline intégré** : compilation, génération et vérification de preuve simples, sans configuration complexe.
- **Preuves efficaces** : protocoles comme Groth16 pour produire des preuves courtes et rapides à vérifier.
- **Facilité d'expérimentation** : permet un prototypage rapide et une bonne intégration dans notre architecture.

4 Résultats des expériences menées

Nous avons rencontré un souci lié à la licence et au permis à cause de la fusion des deux circuits. Sinon, pour le résultat indiquant si la personne est majeure, nous avons ceci :

- 1 si elle est majeure,
- 0 si elle est mineure,
- 2 si le hash ne correspond pas.

5 Défis rencontrés au cours du projet

Le passage où nous vérifions si le hash est correct a été compliqué. Nous avions d'abord commencé par réaliser des tableaux pour les chaînes de caractères, que nous avons ensuite transformés en un hachage de nombres avec Poseidon. Nous avons essayé de fusionner deux circuits différents : un pour l'âge, l'autre pour le permis. Nous n'avons pas réussi, mais nous avons laissé le circuit circom à l'intérieur du projet. Nous avons aussi rencontré des problèmes pour fusionner l'interface web avec le circuit.

6 Regard critique sur notre projet

Quelle est la robustesse de la garantie de confidentialité offerte par votre système ZKP ?

La preuve à divulgation nulle de connaissance (ZKP) permet de confirmer la validité d'un attribut (par exemple, être majeur ou posséder un permis valide) sans jamais révéler d'informations sensibles telles que la date de naissance, le nom complet ou le nonce utilisé. Tant que la fonction cryptographique Poseidon demeure résistante aux attaques par préimages et collisions, aucun tiers ne peut extraire les données originales à partir de l'engagement public, ni recouper plusieurs sessions pour identifier l'utilisateur.

Quelles sont les limites des engagements basés sur un hash pour la vérification d'identité ?

Les engagements hachés peinent à gérer naturellement des plages ou intervalles complexes (comme « entre 18 et 25 ans ») sans recourir à des circuits cryptographiques plus lourds. Leur sécurité dépend également de la qualité du nonce : un nonce faible ou prévisible expose à des attaques par force brute. Par ailleurs, la confiance repose entièrement sur l'émetteur ; en cas de compromission de sa clé ou de son processus de génération, l'intégrité du système est compromise.

Ce système peut-il être déployé à l'échelle d'une infrastructure nationale ou de grande ampleur ?

Sur le plan technique, oui : les engagements, qui pèsent quelques centaines d'octets, ainsi que les preuves Groth16, relativement compactes (quelques kilo-octets), permettent une vérification rapide. Cependant, pour un déploiement à grande échelle, il sera nécessaire d'industrialiser la gestion des clés du *trusted setup*, d'assurer la distribution régulière des circuits mis à jour, et de fournir un service d'API fiable pour la publication et la consultation des engagements publics.

Existe-t-il des alternatives cryptographiques mieux adaptées ?

Oui, plusieurs options complémentaires ou alternatives existent :

- Les certificats d'attributs signés, où une autorité (par exemple, l'État) délivre un jeton numérique attestant d'un attribut spécifique (comme la majorité).
- Les identifiants sélectifs, tels que les wallets d'identité, qui permettent de détenir plusieurs badges (âge, permis, diplôme) tout en n'activant que celui nécessaire.

— Les signatures aveugles, qui permettent à l'émetteur de signer un document sans en connaître le contenu, validant ainsi uniquement l'attribut demandé.

7 Pistes d'amélioration et étapes futures

L'intégration des différents circuits de preuve a été pour nous un véritable défi au cours du projet. Jusqu'à présent, nous avons conçu plusieurs circuits distincts, chacun dédié à une propriété spécifique (comme l'âge ou la catégorie de permis). Une piste d'amélioration consisterait à regrouper ces fonctionnalités dans un circuit unique et plus complet, capable de vérifier plusieurs attributs d'identité en même temps. Cette approche permettrait de se rapprocher davantage du fonctionnement d'une pièce d'identité numérique tout-en-un, et de simplifier à la fois la génération et la vérification des preuves.

8 Conclusion

Ce projet a démontré la faisabilité d'un système de vérification d'identité respectueux de la vie privée grâce aux preuves à divulgation nulle de connaissance. En s'appuyant sur un modèle d'engagement cryptographique sécurisé et des circuits ZKP adaptés, nous sommes parvenus à mettre en place de la validation d'attributs sensibles (comme l'âge ou la catégorie de permis) sans révéler les données personnelles sous-jacentes. Cette approche offre une réelle avancée en matière de protection des données dans les systèmes d'identification numérique, tout en posant des défis techniques liés à la gestion des engagements, à la confiance dans l'autorité émettrice et à la scalabilité de ce modèle. L'intégration de ce type de solution dans des infrastructures réelles nécessitera une mise en œuvre rigoureuse, mais ouvre des perspectives prometteuses pour des identités numériques plus sûres et souveraines.