Projet MiRitH

Maxime Coute Jules Magois

January 13, 2025

1 Explication générale de la signature

1.1 Problème MinRank

1.2 Authentification zero-knowledge utilisant MPC-in-the-head

1.3 Fiat-Shamir pour obtenir une signature

2 Proposition de structure du code

1. un fichier `matrix.c` pour gérer les opérations sur les matrices:
   - allocation de mémoire
   - libération de mémoire
   - addition de deux (ou une liste de) matrices
   - multiplication de deux matrices
2. un fichier `key_generation.c` pour générer la clé,
3. un fichier `party.c` qui implémente les calculs de chaque partie,
4. un fichier `main.c` qui implémente la signature.

3 Bibliothèques utilisées

1. `gmp` pour la génération de nombres aléatoires, et les calculs sur les grands entiers,
2. `openssl` pour l'utilisation du hash *Keccak*.