Projeto de Formatura – 2025

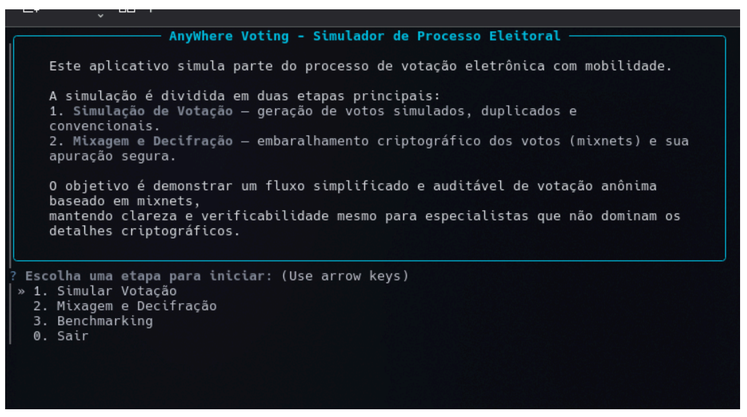
PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema: **Implementação e Avaliação de uma Solução Criptográfica para Mobilidade Segura em Eleições Brasileiras**

Contexto e Objetivos

A mobilidade permite votar em qualquer seção. O projeto explora como isso poderia ocorrer com privacidade, usando um token de voto móvel e uma mixnet para tratar votos possivelmente duplicados.

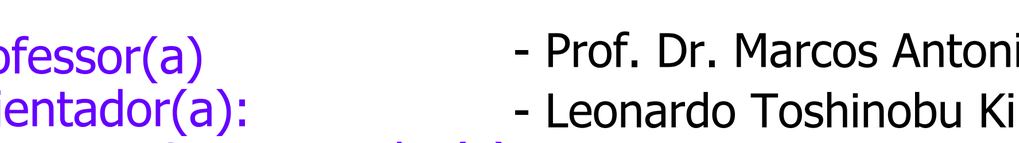


Arquitetura da Solução

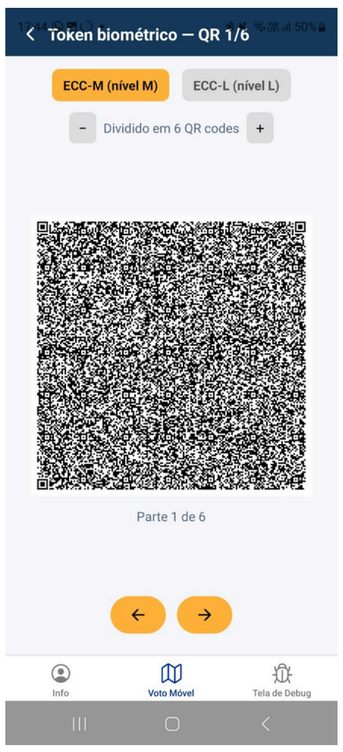
A solução possui duas frentes independentes.

(i) Aplicativo móvel: simula a experiência de mobilidade do eleitor e gera um token criptográfico em QR Code, demonstrando como um token de voto móvel poderia ser apresentado ao usuário.

(ii) Pipeline criptográfico: recebe votos já cifrados, identifica duplicatas pelo tokenID e aplica um processo de embaralhamento (mixnet) seguido de decifração limiar, produzindo um resultado final sem duplicatas, conforme ilustrado no fluxo abaixo.



O aplicativo móvel demonstra o fluxo de mobilidade do eleitor e gera o token biométrico em múltiplos QR Codes, ilustrando a experiência prática do voto móvel.



Conclusão

O protótipo de aplicativo combina tokenização móvel e mixnet para ilustrar como garantir privacidade e remover duplicatas na mobilidade de voto, explicitando o passo-a-passo do protocolo de maneira didática.

Resultados

O pipeline de mixnet foi desenvolvido com um frontend em CLI. Permite acompanhar o processamento criptográfico, incluindo a identificação de duplicatas e o uso da mixnet Verificatum com decifração limiar.

Integrantes:
- Jonas Gomes de Morais - 10893805
- Luis Enrique del Llano Risco - 6718450

Professor(a) Orientador(a):
- Prof. Dr. Marcos Antonio Simplicio Jr.
- Leonardo Toshinobu Kimura