# **C**ryptographie **I**ndustrielle **A**vancée // Projet

Création d'un système de vote électronique sécurisé

Loïc Rouquette

30 octobre 2025

## Objectif du projet

L'objectif de ce projet est de **concevoir et d'implémenter un prototype fonctionnel d'un système de vote électronique** sécurisé. Le projet mettra l'accent sur l'application correcte des principes et outils de la cryptographie pour adresser les défis spécifiques du vote en ligne.

## Livrables

Les livrables de ce projet sont doubles et seront évalués conjointement :

1. **Le Code Source et son environnement (Projet Logiciel) :**
   - Le code complet du système de vote électronique.
   - **Le système doit être rendu réalisable et déployable de manière autonome via une configuration Docker** (un ou plusieurs conteneurs).
   - Le code devra implémenter les mécanismes cryptographiques choisis pour la sécurité du vote.
2. **Le Rapport Technique & Scientifique :**
   - Un document structuré détaillant l'approche, la conception et l'analyse du système.

## Contenu du Rapport Technique et Scientifique

Le rapport doit être le reflet de la démarche de conception et de l'analyse des propriétés de sécurité. Il devra comporter les sections suivantes :

1. **Introduction & Choix de Conception**
   - Motivation et Contexte : Présentation des défis d'un système de vote électronique (fraude, intimidation, anonymat, etc.).
   - Architecture du Système : Description de l'architecture choisie (e.g., client/serveur, basé sur une blockchain, avec un ou plusieurs serveurs de scrutin/mixage). Justification des choix technologiques (langages, frameworks, base de données).
   - Processus de Vote : Description détaillée des étapes, de l'inscription de l'électeur à la publication des résultats.
2. **Analyse & Application Cryptographique**
   - Outils Cryptographiques Fondamentaux : Explication détaillée des outils cryptographiques utilisés et de leurs principes. Cela peut inclure :
   - Cryptographie Appliquée au Vote : Explicitation de la manière dont les outils cryptographiques sont appliqués pour garantir les propriétés que vous aurez définies.

3. **Propriétés & Analyse de Sécurité**
   - Propriétés Appliquées : Description des propriétés de sécurité du scrutin que le système vise à satisfaire.
   - Analyse des Menaces : Évaluation des vulnérabilités potentielles et de la façon dont les choix de conception (notamment cryptographiques) y répondent.

## Soutenance & Évaluation

L'évaluation portera sur les deux parties du projet. La soutenance sera un exercice de 15 minutes de questions uniquement, focalisées sur les aspects techniques et sécuritaires du projet (code et rapport).