

# Plan de l'oral

- Introduction — contexte et objectifs
- Méthodes de protection et limitations
- Outils de vérifications
- Érysichthon
  - Conception générale
  - Andhrímnir
- Résultats
- Conclusion

## Introduction

- Attaquer sur la sécurité et le besoin d'avoir des libs cryptographiques
- Présenter HACL\*
- Historique timing attacks
- Introduction de la problématique

## Méthodes de protection et limitations

- compilateurs

- CompCert => garanties formelles // retard sur les standards
- Jasmine => annotations de codes, execute toutes les branches // pas employable sur un projet industriel, artefact de recherche
- Raccoon => annotations de codes // pas le temps constants
- Constantine => linéarisation // 16.36x taille binaire & 27.1x temps

- assembleur

- programmation en temps constant

- présentation
- détails et exemple

*transition*

## Outils de vérifications

- tableau

- **Binsec** / présentation

## Automatismes

- Démo de Binsec et comment ça fonctionne
- adaptation cas d'étude
- automatisation **tableaux**
- cahier des charges

## Érysichthon

- graphes de fonctionnements
- spécialisation x86\_64
- construction en modules

### Focus sur Andhrímnir

- standardisation de la construction des tests
- graphe de fonctionnements

## Résultats

- graphes
  - discuter des **unknown**
- détail sur les plus importants** : KO - error

## Conclusion

Retour sur la présentation :

**Questions de recherches** QR1 : propagation des garanties de sécurité

QR2 : automat détect° faille

QR3 : application sur biblio

- outil fonctionnel - corrections pour Binsec - modification de HACL\* - ajout à une intégration continue