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

Outils de vérifications

Érysichthon

Résultats

Conclusion