Attaque par canal auxiliaire sur la signature ECDSA et réduction de réseau

Capgrand Paul - Chauveau Paul - Duzes Florian

Master Cryptologie et Sécurité Informatique

université de BORDEAUX

June 15, 2025

Introduction

Introduction

Outils développés en *SageMath* :

1. Un générateur de paramètres DSA
2. Un générateur de signatures et de traces pour tous les protocoles étudiés
3. Les fonctions de l'attaque de notre référence
4. Un programme pour filtrer et agréger les résultats avant de les tracer avec *numpy*, *pandas*, *matplotlib* et *seaborn*

Sommaire

Annexe