

Appétences — Je suis intéressé par de nombreux sujets que j'ai découvert au long de mon cursus : Implémentation sûr et sécurisé, Chiffrement homomorphe, Cryptanalyse, Sécurité des canaux auxiliaires, Sécurité des logiciels embarqués

Compétences

Algorithmique : Quantum Computing, algèbre, complexité
Cryptologie : McEliece, LWE, Kyber, Dilithium, AES, RSA, DES
Systèmes : Windows, Linux
Architectures : INTEL, ARM, RISC-V, shellcodes

Langage : Python, SageMath, C, Rust, LaTeX, OCaml, F*
Langues : Anglais et Espagnol - C1
Personnelles : Travail d'équipe, organisé, curieux, prise d'initiative sous supervision, autonome

Expériences professionnelles

Chercheur en Sécurité

INRIA Paris - Prosecco / CEA

2025

5 mois

- Recherche sur la sécurité des attaques par canaux auxiliaires. Travaux avec Binsec sur HACL*. Automatisation de l'analyse pour différentes versions de compilateurs et vers différentes architectures. Développement d'un outil pour la CI d'HACL*.

Présidences étudiantes

Association Alea - Université Champollion

2022 - 2023

12 mois

CFVU Université Champollion

12 mois

Conseil Etudiant Université Champollion

12 mois

Animation jeunesse - Directeur de centre

Éclaireuses et éclaireurs de France (EEDF, scoutisme laïque) - bénévole

2017 - 2024

Wakanga - direction de centre de vacances en 2024

7 ans

3 ans

Expériences laborales

2015 - 2024

Formations

Master Cryptologie et sécurité informatique

Option : Cryptographie Post-Quantique, Algorithmique arithmétique, Cryptanalyse, Cartes à puces, Sécurité des systèmes
Université de Bordeaux

2025

Licence Informatique, mention Intelligence Artificielle

Institut National Universitaire Jean-François Champollion

2022

Diplômes et certifications

- Certificat de langue anglaise, Cambridge Center - IHT
- Divers PSC1, BAFA, BSB
- Baccalauréat

Projets informatiques

Travaux de recherche, projets et stage

2019 - 2025

- Attaque par canal auxiliaire sur ECDSA et réduction de réseau, implémentation SageMath - [Présentation](#)
- Introduction complète aux Générateurs de nombres pseudo-aléatoires - [Article](#)
- Étude du cryptosystème de Paillier en application sur une application de messagerie, implémentation en C - [Archive](#)
- Logiciel d'étude des comportements humains pour dérouter une IA, programmation Python - [Restreint](#)
- Développement d'un compilateur C en OCaml - [Application fonctionnelle](#)

Global Game Jam - 2020/2021/2022/2023/2024

2020 - 2024

- Créativité, travail à distance et organisation avec les fuseaux horaires d'une équipe de huit personnes
- Développement de jeu vidéo durant cet événement mondial, sur 48h.

Nuit de l'info - Passage Python

2019 - 2021

- Programmation de site web sous forme de concours national avec des défis proposés par des entreprises
- Travail d'équipe, brainstorming, développement web et gestion de projets en ~14h.
- Récompensé pour les solutions de l'équipe

Loisirs

Gastronomie

Cinéma

Sports Tennis, Taekwondo, VTT

Lectures Hypérion, Belgariade, Les chevaliers d'émeraude