

Samy HORCHANI

Jeune diplômé en Cryptographie, Cybersécurité et HPC

Paris, France | +33 7 67 07 54 94 | samyhorchani@gmail.com | [Github](#) | [Linkedin](#) | [Portfolio](#)

EXPÉRIENCES PROFESSIONNELLES

INGÉNIEUR STAGIAIRE – ORANGE, ARCUEIL

Février 2025 - Août 2025

- **Cryptographie post-quantique et Cybersécurité**
- Mise en place d'une plateforme répliquable de test en environnement conteneurisé (Docker) et de mesure des algorithmes cryptographiques post-quantiques (PQC) pour TLS, mTLS
- Intégration d'une pipeline CI/CD Gitlab
- Configuration et Déploiement de serveurs Nginx et Apache sur infrastructure Cloud
- Développement d'une PKI (génération et gestion)
- Identification des prérequis techniques nécessaires à la migration PQC et inventaire cryptographique (CBOM).
- **Outils:** GitLab, Docker, OpenSSL, Prometheus, Grafana, Linux, Python, TLS/mTLS, Bash, Liboqs (+OQSProvider), GoLang, Javascript/HTML/PHP, Nginx, Apache

ASSISTANT CHERCHEUR - UNIVERSITÉ D'OKAYAMA, JAPON

Juin 2024 - Août 2024

- **Sécurité des réseaux - (stage réalisé entièrement en anglais)**
- Développement d'une plateforme de simulations de problèmes réseaux en utilisant des outils d'Ingénierie du Chaos (Pumba)
- Génération de données synthétiques et analyses quantitatives et qualitatives de celles-ci.
- **Outils:** Docker, GoLang, Containerlab, Pumba, Dotnet, Linux, Bash

FORMATION

MASTER INFORMATIQUE - CRYPTOLOGIE, CALCUL HAUTE-PERFORMANCE ET ALGORITHMIQUE

Sorbonne Université | 2023-2025

LICENCE BIDISCIPLINAIRE - INFORMATIQUE & INGÉNIERIE MÉCANIQUE

Sorbonne Université | 2020-2023

PROJETS IT

CRYPTOGRAPHIE / SÉCURITÉ

- **Attaques par Canaux Auxiliaires**
- Sécurité embarquée et attaques matérielles, attaques par analyse de consommation, attaques par faute, attaques par analyse de timing, contre-mesures logicielles face aux attaques, évaluation de fuites secrètes.

CALCUL HAUTE PERFORMANCE - HPC / PROGRAMMATION PARALLÈLE

- **Performance des réseaux de neurones pour générer des distributions aléatoires standard**
- Parallélisation des algorithmes sur CPU et GPU pour évaluer l'efficacité lors de l'inférence des réseaux de neurones.
- **Outils:** Python (Numpy, PyTorch), C/C++ (CUDA, OpenMP, MPI), Réseaux de neurones, Méthode Monte Carlo

COMPÉTENCES

Cryptographie et Sécurité

- IAM, PKI, Recommandation ANSSI, Recommandation NIST
- ECC, ECDH, RSA, AES, PKCS (PKCS#11, PKCS#12)
- PQC Standard NIST (ML-KEM, ML-DSA, SLH-DSA)
- OpenSSL, LibOQS (+ OQSProvider)

Certification

- SecAnumacadémie (ANSSI)

Langages, Développement & Systèmes

- C/C++, Python, Go, SageMath, Matlab, Bash, SSH, Git, Nginx, Apache, Linux, Windows, Docker, CUDA, CI/CD (Github Actions et Gitlab), Prometheus, Grafana, Wireshark, Assembleur MIPS, JAVA

AUTRES

- **Langues:** Français (C2 - Langue maternelle), Anglais (C1 - confirmé)
- **Centres d'intérêt:** Course à pied, Escalade, Lecture (Dystopie et SF)