

# Nugzari Uzoevi

 [nougzar.uzoev@hotmail.fr](mailto:nougzar.uzoev@hotmail.fr) |  +33 6 40 24 09 91  
 [github.com/nougzarm](https://github.com/nougzarm) |  Paris

## À la recherche d'opportunités dans le domaine de la cryptographie

### Compétences

**Langages de programmation :** Rust (expertise principale), Python, C,  
**Outils :** SageMath, Linux/Bash, Git, Virtualisation, Programmation embarquée

### Formation

**Master 2 Mathématiques, Informatique, Cryptologie (MIC)** à Université Paris Cité **2024 - 2025**

- Cours majeurs : Cryptologie symétrique/asymétrique, Réseaux sécurisés, Informatique embarquée, sécurité des protocoles, Services internet, Codes correcteurs d'erreurs, Méthodes formelles

**Master 2 Mathématiques fondamentales** à Université Paris Cité **2022 - 2023**

- Cours majeurs : Géométrie algébrique (Variétés algébriques, Théorie des schémas), Théorie des catégories, Topologie algébrique

**Licence 3 - Master 1 Maths fondamentales et appliquées** à Université Paris Cité **2020 - 2022**

**CPGE Mathématiques (MPSI-MP)** au Lycée Jacques Amyot **2018 - 2020**

### Expériences Professionnelles

**Stage de fin d'études en cryptographie - UVSQ** **mai - octobre 2025**  
sous la direction de Michele Orrù et Balthazar Bauer

**Domaine :** Preuves à divulgation nulle de connaissance (**ZKP**)

- Contribution significative au développement de la librairie open source [sigma-proofs](#) (Rust).
- Travaux ayant mené à la standardisation IETF et à son intégration dans le projet **Tor**.
- Développement et intégration de briques cryptographiques essentielles dans une architecture modulaire (Implémentation des protocoles Sigma, conception du code permettant la composition de protocoles complexes (AND/OR), etc.).
- Rédaction de la documentation, revues de code et tests unitaires.

### Projets

**kyber-nz | Librairie de Cryptographie Post-Quantique (PQC) haute performance (Rust)** (novembre 2025) : [[Lien GitHub](#)]

- **Implémentation FIPS 203** : Développement en **Rust** pur du standard ML-KEM (Kyber), validé par les vecteurs de tests officiels du **NIST (KATs)** pour les niveaux 512, 768 et 1024.
- **Sécurité Offensive** : Conception résistance aux attaques par canaux auxiliaires (timing attacks) via des opérations en **temps constant** et nettoyage automatique de la mémoire (zeroize).
- **Optimisation Système** : Refactoring complet pour éliminer les allocations dynamiques.
- **Qualité & CI/CD** : Mise en place d'une chaîne d'intégration continue complète (Tests, Audit de sécurité), **benchmarking** statistique (criterion) et **fuzzing** pour la robustesse.
- **Python** : Une autre librairie développée en Python également disponible : [[Lien Github](#)].

**Informatique embarquée (M2 MIC)** :

Implémentation d'un authentificateur sur le microcontrôleur Arduino ATmega328P [[Lien GitHub](#)].

**Cryptographie asymétrique (M2 MIC)** :

- Implémentation en C de primitives et attaques cryptographiques classiques (p.ex : corps finis [[Lien](#)])
- Attaque sur RSA par révélation partielle de la clé privée [[Lien](#)].

**Cryptographie symétrique (M2 MIC)** :

Chiffrement AES (cryptanalyse différentielle, attaque intégrale), LFSR et chiffrement à flot (attaque algébrique) [[Lien GitHub](#)].

**Chiffrement RSA et attaque de Coppersmith** (mai 2024)

Cryptanalyse à l'aide de l'algorithme LLL [[Lien](#)].

## Centres d'intérêts

---

**Bricolage** : Restauration de voiture de collection