

Václav GREGOR

Toulouse, France
www.obludarium.fr
nationalité : slovaque
vaclav.gregor@aquilenet.fr

Éducation

Master Mathématiques et Applications
Parcours Cryptologie & Sécurité Informatique
2024 - 2026, *Université de Bordeaux*

Licence d'Informatique
2021 - 2024, *Université de Bordeaux*

Projets personnels / universitaires

A note on the Unsuitability of LIGA for Linkable Ring Signatures: The perils of non-commutativity
Université de Bordeaux (travail encadré de recherche)
Article de recherche en cryptographie centré sur une linkable ring signature post-quantique basée sur le problème d'isomorphisme de réseaux euclidiens (LIP). Pré-publié dans l'IACR (Internet Archive of Cryptographic Research).
Lien ici

Initiation à la Cryptographie Basée sur les Réseaux Euclidiens
Thales Alenia Space, Toulouse
Conception et présentation d'une formation interne introduisant les fondements de ce domaine de la cryptographie, axée sur les standards ML-KEM et ML-DSA, à destination d'une équipe technique amenée à les implémenter à terme.
Lien ici

On the MITM DNS-over-HTTPS downgrade attack
Université de Bordeaux (travail encadré de recherche)
Une étude des attaques actuelles sur le protocole DNS-over-HTTPS, et de la réaction des navigateurs modernes sous de telles attaques. Ce projet inclut un rapport et une implémentation des attaques dans un environnement virtuel.
Lien ici

Langues

🇸🇰 **Slovaque** (langue maternelle)
🇫🇷 **Français** (C2)
🇬🇧 **Anglais** (C2)
🇨🇿 **Tchèque** (C2)
🇪🇸 **Espagnol** (B1)

Expériences professionnelles

Stage en sécurité des communications spatiales
mars 2026 - sept. 2026, *Thales Alenia Space, Toulouse*
L'objectif principal de mon stage est la conception et implémentation d'un protocole d'établissement de clé pour un satellite géostationnaire et ses segments sol de contrôle, instancié avec ML-KEM. Cependant, j'ai aussi pu réaliser un travail pédagogique sur la cryptographie basée sur les réseaux euclidiens, sous forme d'une formation déstinée à une équipe technique en interne.

Tuteur pour la licence d'informatique
sept. 2024 - mars 2026, *Université de Bordeaux*
Accompagnement d'étudiants en licence, animation de séances de révision, avec certains étudiants un suivi tout au long de l'année.

Tuteur de maths, physique-chimie et informatique pour collège/lycée
janv. 2025 - mars 2026, *Complétude*

Compétences

Informatique générale
- programmation en Python, C, Java et OCaml
- assembleurs x86 et x64
- programmation système et admin. des réseaux sous Linux

Mathématiques
- algèbre
- théorie algorithmique des nombres
- théorie des probabilités et de l'information

Sécurité informatique
- bases de l'analyse (statique, dynamique, reverse) et exploitation de vulnérabilités logicielles
- sécurité des réseaux
- attaques sur DNS et DoH

Cryptologie
- cryptographie classique
- cryptographie post-quantique basée sur les réseaux euclidiens
- problème d'isomorphisme de réseaux euclidiens (LIP)
- (linkable) ring signatures post-quantiques
- cryptanalyse
- conception et construction d'un protocole cryptographique

Autres
- fonctionnement et sécurité des communications dans un système satellitaire