Azevedo Oliveira Paco

Doctorant en cryptographie

Formation

2024- **Doctorant CIFRE en informatique**, *Thales DIS*, Université de Versailles Saint-Quentin
Dirigé par Louis Goubin et Benoît Cogliati

2022-2023 **M2-Algèbre Appliquée et cryptographie**, *Université de Versailles Saint-Quentin*, Versailles
Mention Bien

2021-2022 **M2-Préparation à l'agrégation**, *Université de Grenobles Alpes*, Grenoble
Admis 172ème à l'agrégation de mathématiques

2019-2021 **L3A-M1-Magistère**, *Université de Grenobles Alpes* , Grenoble
Mention Bien

2017-2019 **MPSI/MP**, *Lycée Camille Pissaro*, Pontoise
Admis au magistère de mathématiques de Grenoble

Experience professionnelle et de recherche

2023-2024 **Stage/CDD**, *Etude d'algorithmes de signatures post-quantique dans le modèle de la boite blanche*, Thales DIS, Meudon
Sous la direction de Benoit Cogliati et Louis Goubin

2020-2021 **Mémoire de magistère**, *Exposants critique pour la percolation plan*, Institut Fourier, Grenoble
Sous la direction de Vincent Beffara

Publications

2024 **Uncompressing Dilithium's public key**, *Paco Azevedo-Oliveira, Andersson Calle Viera, Benoît Cogliati et Louis Goubin.*
[preprint]

2024 **Finding a polytope : A practical fault attack against Dilithium**, *Paco Azevedo-Oliveira, Andersson Calle Viera, Benoît Cogliati et Louis Goubin.*
[preprint]

Enseignement

paco.azevedo-oliveira@thalesgroup.com
azevedopaco.github.io/azevedo_oliveira_paco • **in** *paco.azevedo-oliveira*

2024 **Jury academique pour les trophées NSI**
Les Trophées NSI est un concours qui récompensent des projets informatiques réalisés dans le cadre de l'enseignement de spécialité ≪ numérique et sciences informatiques ≫.

2023-2025 **Chargé de TD en M1-Algèbre Appliquée**, *30h heures de Travaux Dirigés pour le cours d'Introduction à la cryptographie*, Versailles

2024-2025 **Chargé de TD en L2-Physique**, *40h heures de Travaux Dirigés pour le cours "Analyse et algèbre linéaire" : Séries numériques, réduction des endomorphismes, fonction de plusieurs variables, équations différentielles résolues*, Versailles

2022-2024 **Colleur en MPSI**, *Lycée Camille Pissaro*, Pontoise

2020-2021 **Tutorat**, *Employé par l'Université de Grenoble*
- Cours d'aide aux élèves de L3 en topologie.
- Cours d'aide aux élèves de M1 à PolyTech Grenoble en Chaine de Markov.

2019-2022 **Animateur "Les maths autrement"**, *groupe IREM*, Institut Fourier, Grenoble
l'IREM anime un groupe d'élèves, de la primaire au lycée, qui font des mathématiques autrement dans une ambiance ludique et détendue.