# Yulliwas AMEUR

87 Quai de la Gare, 75013 Paris
ameur.yulliwas@gmail.com
06 42 45 25 86

**Enseignant-Chercheur en Cybersécurité**

Enseignant-chercheur en cybersécurité, spécialisé en cryptographie appliquée, sécurité des systèmes et investigation des menaces numériques. Responsable du programme *Réseaux et Sécurité* en alternance à Efrei Paris et membre de l'axe *Sécurité, Résilience et Confiance Numérique*. Activités de recherche, d'enseignement et d'encadrement académique à l'interface des approches techniques, criminologiques et institutionnelles de la sécurité numérique.

**Formations académiques**

**Executive MBA Management et Administration des Entreprises** – IAE Paris-Sorbonne (2026–2028)
Stratégie, management des SI, transformation digitale, finance, RH, gouvernance et mémoire.

**Diplôme Universitaire de Cybercriminologie (60h)** – Université Paris Nanterre, UFR DSP (2026, en cours)
Approche pluridisciplinaire de la cybercriminalité : droit du cyberespace, criminologie, sociologie des réseaux, économie criminelle, psychologie et forensique. Travail de recherche et soutenance orale.

**Master 2 Sécurité Informatique, Cybersécurité et Cybermenaces** – CNAM (FOAD) (2026–2028)
Sécurité offensive et défensive, audit, détection d'attaques, réponse à incident, OSINT, analyse post-incident et mémoire.

**Doctorat en Informatique**, CNAM Paris (2020-2023)
Thèse : Exploration de l'apprentissage automatique avec chiffrement homomorphe dans l'IoT/Cloud
Sous la direction de Samia BOUZEFRANE et Vincent AUDIGIER.

**Master 2 Mathématiques et Applications – parcours Arithmétique, Codage et Cryptologie (ACC)**, Université Paris 8 (2018–2019)
**UE majeures (M2) :**

- *Cryptographie post-quantique* : cryptographie asymétrique post-quantique ; cryptographie symétrique post-quantique.
- *Arithmétique avancée* : théorie des nombres ; courbes elliptiques et applications.
- *Interactions codes & cryptographie*

**Master 1 en Mathématiques et Applications : Cryptographie, Codage**, Université Paris VIII (2017-2018)
**Licence en Mathématiques**, Université Paris VIII (2014-2017)

**Formations courtes & certifications**

**16–18 février 2026 - PRINCE2® 7th Edition, Foundation – formation certifiante**
Groupe ORSYS
Préparation à l'examen PRINCE2 Foundation (7e édition) : concepts clés, principes, pratiques et processus PRINCE2 ; adaptation et gouvernance de projet

**18 juin 2025 IA générative en entreprise :** Outils et opportunités(interne).

**Février 2025 - "PARCOURS DÉCOUVERTE" du MOOC sur l'Intelligence Économique**
Ingénieurs et Scientifiques de France (IESF), Paris 8
Cours en ligne permettant d'appréhender l'intelligence économique à travers les "5 piliers de l'IE" développés par l'IESF. Validation par un badge numérique de certification (Open Badge).

**9–10 janvier 2025 - Rencontres "Sécurité Informatique et SHS" (CNRS)**
GDR Sécurité Informatique & GDR Internet, IA et Société — CNRS, Campus Paris Michel-Ange, Paris
Participation aux journées interdisciplinaires cybersécurité & SHS : exposés scientifiques, tables rondes et session "lightning talks".
`https://sishsjanv2025.sciencesconf.org/`

**9–13 décembre 2024 - Certified Ethical Hacker v13 (CEH) – Formation certifiante (35h)**
SysDream (EC-Council), Levallois-Perret
Formation intensive en hacking éthique : reconnaissance, scan/énumération, analyse de vulnérabilités, exploitation contrôlée, pentest web (incl. SQLi), réseaux, cloud, mobile, IoT/OT, et cryptographie.
Travaux pratiques (labs/CTF) et préparation à l'examen CEH (ANSI, 312-50).

**2020-2023 - Formation Doctorale**
Conservatoire National des Arts et Métiers (CNAM), Paris
Participation à plusieurs séminaires et formations interdisciplinaires, incluant les journées des doctorants, l'éthique scientifique, l'IA en astrophysique et l'innovation responsable. Accumulation de 118 heures de formation réparties sur 18 modules.

**Juin - Août 2020 - Formation Consultant en Cybersécurité**
Fitec, Nanterre

- Introduction à la Cyberprotection
- Cryptographie en Cybersécurité
- Solutions Cyber Range
- Ethical Hacking
- Sécurisation des Réseaux

**Février - Mai 2020 - Formation Cloud et Virtualisation (VMware)**
Global Knowledge, Rueil-Malmaison, France

- Approche et réussite d'un projet de virtualisation
- VMware vSphere : Installation, Configuration et Administration (VSICM)
- VMware NSX : Installation, Configuration et Administration (VMNSXICM)
- Fondamentaux de la méthode Agile Scrum, DevOps Foundation

**Mai 2019 - 7e Atelier sur la Cryptographie Basée sur les Codes (CBC 2019) EUROCRYPT 2019**
Technische Universität (TU), Darmstadt, Allemagne
`https://cbc2019.dii.univpm.it/`

**Mars 2019 - École d'Hiver sur les Fondements Mathématiques de la Cryptographie Asymétrique**
CNRS, Aussois, France

- Introduction à la Cryptographie à Clé Publique
- Graphes d'Isogénies en Cryptographie
- Introduction à la Cryptographie Basée sur les Réseaux

`https://mathsofpkc.sciencesconf.org/`

**Août - Septembre 2018 - École d'Été de Recherche sur les Codes Algébriques**
Middle East Technical University, Ankara, Turquie

- Codes Quantiques issus des Codes Classiques de Type Cyclique
- Introduction à la Cryptographie Basée sur les Codes

`https://iam.metu.edu.tr/cimpa-2018`

**EXPÉRIENCE**

**Enseignant-Chercheur**, Efrei Paris - Université Panthéon-Assas (Depuis 2024)
Chercheur au sein de l'axe "Sécurité, Résilience et Confiance Numérique" à l'Efrei Research Lab
Responsable du programme "Réseaux et Sécurité en alternance"
Gestion pédagogique de la cyber range AIRBUS

**Cours dispensés:**

- Ethical Hacking (30h) - Niveau : Master/Fin de cycle ingénieur
- Sécurité Avancée Windows & Active Directory (30h) - Niveau : Master/Fin de cycle ingénieur
- Cryptographie (30h) - Niveau : Master/Fin de cycle ingénieur
- Cybersécurité (30h) - Niveau : Master/Fin de cycle ingénieur
- Projets Sécurité (Windows & Forensics) (30h) - Niveau : Master/Fin de cycle ingénieur
- Sécurité des Réseaux (30h) - Niveau : Master/Fin de cycle ingénieur

**Attaché Temporaire d'Enseignement et de Recherche**, Université Paris Panthéon-Assas (2023-2024)
**Cours dispensés (192h) :**

- Bureautique (Licence)
- Bases de Données (Licence)
- Programmation Python (Licence)
- Programmation VBA (Licence)

**Stage de fin d'études**, Inria Rennes - Bretagne Atlantique (2019)
Sujet : Attaques par canaux auxiliaires sur les cryptosystèmes post-quantiques
Encadrants : Martino Borello, Annelie Heuser, Tania Richmond, Benoit Gérard

**2011-2013 - Développeur d'Applications iOS**
Freelance, Paris
Développement et déploiement d'applications iOS, incluant études de faisabilité, rédaction de cahiers des charges, programmation et soumission sur l'App Store.
**Références Apple Store :** Magic Princess, Magic Money, VotOclic.

**AFFILIATIONS ACADÉMIQUES**

**Membre associé – Équipe ROC (Networks and IoT Systems)**
Laboratoire CEDRIC (EA 4629), Conservatoire National des Arts et Métiers (CNAM), Paris
Depuis novembre 2025
Participation aux activités de recherche de l'équipe ROC, incluant collaborations scientifiques, séminaires de recherche et contributions aux thématiques réseaux, cybersécurité, systèmes distribués et IoT.

**PUBLICATIONS**

**Articles de journaux**
- Y. Ameur, S. Bouzefrane, S. Banerjee, "Developing Adaptive Homomorphic Encryption through Exploration of Differential Privacy." *Journal of Cyber Security and Mobility*, 2024, pp. 863–886.
- Y. Ameur, S. Bouzefrane, "Enhancing Privacy in VANETs Through Homomorphic Encryption in Machine Learning Applications." *Procedia Computer Science*, vol. 238, pp. 151–158, 2024.

**Chapitres de livres**
- Y. Ameur, S. Bouzefrane, V. Audigier, "Application of Homomorphic Encryption in Machine Learning." *Emerging Trends in Cybersecurity Applications*, Springer, pp. 391–410, 2023.
- Y. Ameur, I. Taberkane, S. Bouzefrane, "Advancing Blockchain Privacy: The Role of Homomorphic Encryption." *Intelligent Cybersecurity and Resilience for Critical Industries: Challenges*, 2025.
- Y. Ameur, M. Kraiem, "Artificial Intelligence and Machine Learning: Revolutionizing Supply Chain Security." *Securing the Digital Supply Chain: Advances, Challenges, and Solutions*, pp. 183–201, 2026.

**Actes de conférence**
- Y. Ameur, R. Aziz, V. Audigier, S. Bouzefrane, "Secure k-means Clustering using Homomorphic Encryption." *17th International Conference on Ambient Systems, Networks and Technologies (ANT 2026)*, Istanbul, Türkiye, 14–16 avril 2026. (Full paper accepté ; à paraître dans *Procedia Computer Science*).
- Y. Ameur, S. Bouzefrane, L. V. Thinh, "Handling Security Issues by Using Homomorphic Encryption in Multi-Cloud Environment." *Procedia Computer Science*, vol. 220, pp. 390–397, 2023.
- Y. Ameur, R. Aziz, V. Audigier, S. Bouzefrane, "Secure and Non-Interactive k-NN Classifier Using Symmetric Fully Homomorphic Encryption." *International Conference on Privacy in Statistical Databases*, pp. 142–154, 2022.

**Jeux de données**
- Y. Ameur, S. Bouzefrane, "GovSecLLM++ SECAI 2026 Artifact Package." Zenodo, 2026. DOI : 10.5281/zenodo.20646702.

**ENCADREMENT Janvier – Juin 2026 - Encadrement de stage (Master 2) – IDS sur trafic chiffré (TLS/QUIC)**
Efrei Research Lab
Supervision de **KEFKEF Ahmed** sur le sujet : *"IDS intelligent sur trafic chiffré (TLS/QUIC) : benchmark CIC-IDS2017 et prototype SOC/SIEM."*
Co-encadré avec **Lyes Khoukhi**.

- Détection *payload-free* (features de flux + métadonnées TLS) sur TLS 1.3 / QUIC.
- Évaluation reproductible sur CIC-IDS2017 (baselines + analyse FP/FN).
- Prototype SOC/SIEM : Zeek/Suricata → scoring → alertes JSON ; explicabilité (feature importance / SHAP).

**Février – Août 2026 - Encadrement de stage (Ingénieur) – Optimisation PQC par apprentissage par renforcement**
Efrei Paris
Supervision de **LASLEDJ Insaf Imene** (Ingénieur d'État en Informatique, spécialité cybersécurité) sur le sujet : *"Apprentissage par renforcement pour l'optimisation d'algorithmes de cryptographie post-quantique."*

- Benchmark d'algorithmes PQC (Kyber, Dilithium, Falcon, BIKE) sur x86_64, ARM et IoT.
- Optimisation multi-objectif (temps, mémoire, énergie) via agents RL (PPO/DQN) sur paramètres de compilation/protocole.

**Janvier 2025 - Encadrement de stage de recherche – Cryptographie post-quantique**
Efrei Research Lab
Supervision d'**Abdoul Ahad Fall** sur le sujet : *"Analyse des approches hybrides pour la cryptographie post-quantique."*

- Étude des constructions hybrides (KEMs, signatures) et analyse sécurité/performance.

**Septembre 2023 – Juin 2024 - Encadrement d'alternants (Master)**
Université Paris Cité, Paris
Supervision et mentorat d'étudiants en apprentissage professionnel :

- Céline Djadel (Aéroport de Paris) ; Nouamane Bouihi (BNP Paribas) ; Mario El Dahdah (Potech Conseil SAS) ; Amel Khamoum (RandoriSec).

**Janvier 2023 – Juin 2023 - Encadrement de stage – Chiffrement homomorphe**
École Nationale Supérieure d'Informatique, Paris
Supervision d'**Aziz Rezak** sur le sujet : *"Clustering avec données manquantes dans le contexte du chiffrement homomorphe."*
Co-encadré avec **Samia Bouzefrane** et **Vincent Audigier**.

**Juin 2021 – Septembre 2021 - Encadrement de stage – k-NN sécurisé par chiffrement homomorphe**
École Nationale Supérieure de Cognitique (ENSC), Bordeaux
Supervision de **Corentin Lanusse-Malhéné** sur le sujet : *"Classification k-NN sécurisée basée sur le chiffrement homomorphe."*
Co-encadré avec **Samia Bouzefrane** et **Vincent Audigier**.

**ÉVALUATION & COMITÉS**

**Comités de programme (PC)** : ANT (2024, 2026) ; ARES / IWCC (2023, 2024) ; WISTP (2024) ; MSPN (2023) ; EMSICC (2026).

**Responsabilités dans des workshops** : Publicity Chair — IEEE/IFIP SRC-DAV 2025, workshop de la conférence NTMS 2025 (Paris, juin 2025).

**Évaluation d'artefacts / ouvrages** : DSN Artifact Evaluation (2025) ; CARDIS (2019) ; BWTS (2024).

**Relecteur pour conférences** : IEEE ICC (2024).

**Relecteur pour journaux** : *Annals of Telecommunications* (Springer) ; *JISA* (Elsevier) ; *Physical Communication* (Elsevier) ; *SN Computer Science* (Springer) ; *JDSIS* (Bon View Press) ; *Journal of Cyber Security and Mobility.*

**ENSEIGNEMENT**

**Université Paris Cité (2023-2024)**

- Analyse Forensique et Analyse Malware (15h, Master 1)
- Introduction à la Cryptographie (16h, Master 1)

**Université Paris 8 (2023-2024)**

- Programmation sur cartes à puces (30h, Master 1)

**École d'Ingénieurs ESILV (2023-2024)**

- Sécurité de l'information (18h, Bachelor 3)
- Cryptographie appliquée (18h, Bachelor 3)
- Politique de Sécurité des Systèmes d'Information (18h, Bachelor 3)
- Forensics (18h, Bachelor 3)

**Guardia Cyber School (2023-2024)**

- Fondamentaux des SI et de la cybersécurité (15h, Bachelor 1)
- Analyse du renseignement (15h, Bachelor 3)
- Techniques d'attaques web (15h, Bachelor 3)
- Sécurité et respect des libertés individuelles (15h, Master 1)
- Transition vers la cryptographie post-quantique (15h, Master 1)

**EPSI-PARIS (2023-2024)**

- SIEM - Security Information and Event Management (14h, Master 1)

**CNAM Paris (2021-2022)**

- Cryptographie avancée : Introduction rapide au chiffrement homomorphe (4h, Master)

**CONFÉRENCES INVITÉES & PRÉSENTATIONS**

**Septembre 2023 - Comment le chiffrement homomorphe révolutionne l'apprentissage automatique en protégeant les données**
Institut de Lutte contre la Criminalité Économique (ILCE), Neuchâtel, Suisse
Présentation des avantages du chiffrement homomorphe (HE) pour la sécurité des données dans le cloud et l'amélioration de la confidentialité en apprentissage automatique. Discussion sur les schémas HE, les outils actuels et les applications pratiques de l'apprentissage automatique préservant la vie privée (PPML).

**Mai 2022 - Machine Learning Sécurisé : Application du chiffrement homomorphe en apprentissage automatique**
Faculté d'Informatique, Célébration du 48e anniversaire de l'USTHB, Alger
Introduction au chiffrement homomorphe, présentation des schémas les plus prometteurs et des outils actuels. Discussion sur la protection de la vie privée en apprentissage automatique (PPML) et exploration des modèles d'apprentissage automatique les plus utilisés dans ce cadre.

**Avril 2021 - Chiffrement homomorphe et apprentissage automatique : Avancées et défis**
Séminaire CEDRIC : Axe "Confiance et Sécurité Numérique", Paris 3
Présentation des avancées du chiffrement homomorphe intégral, en mettant l'accent sur les fondements mathématiques, les améliorations récentes et les résultats d'implémentation. Discussion des défis ouverts liés à l'utilisation du chiffrement homomorphe dans l'apprentissage automatique.

**Missions**

**Avril 2024 - Expert en Cybersécurité**
Université Libre de Bruxelles, Belgique
Contribution au programme de Master en cybersécurité de l'Université de Bamenda (Cameroun) dans le cadre d'une coopération académique avec l'Université Libre de Bruxelles. Enseignement de modules spécialisés incluant "Calcul sur des Données Chiffrées" et "Sécurité des Cartes à Puce".

**Octobre 2023 - Membre du Comité d'Organisation Local**
MSPN 2023, Paris 3
Gestion de la communication de l'événement, recherche de sponsors et organisation administrative/logistique.
`https://mspn2023.roc.cnam.fr/`

**2021-2023 - Membre de la Commission des Locaux**
Laboratoire CEDRIC, CNAM, Paris
Rédaction de rapports et recommandations pour l'amélioration des conditions de travail, mise en place d'un système de réservation de salles de réunion et optimisation de l'aménagement des locaux.

**Janvier - Avril 2021 - Community Manager**
MOOC "Bases de Données Relationnelles : Apprendre pour Utiliser" (Fun-Mooc), Paris
Création et gestion d'une communauté en ligne de plus de 500 participants, animation de discussions et organisation de webinaires.

**2017-2018 - Tuteur en Mathématiques**
Université Paris VIII Vincennes - Saint-Denis
Assistance aux étudiants de L1 en mathématiques et informatique sur l'algèbre, l'analyse et l'introduction à la programmation.

**COMPÉTENCES** **Cybersécurité et investigation numérique :** cyberdéfense, sécurité des systèmes et des réseaux, ethical hacking, sécurité avancée Windows/Active Directory, analyse forensique et post-incident, détection des attaques et SIEM, sécurité des environnements cloud, cartes à puce (dont cartes SIM), gestion de crise cyber et continuité d'activité.

**Méthodologies, cadres et référentiels :** MITRE ATT&CK (Enterprise / ICS), OWASP, référentiels de compétences ANSSI, European Cybersecurity Skills Framework (ECSF), méthodologie URSID pour la conception de scénarios cyber.

**Cryptographie et sécurité des données :** cryptographie appliquée et avancée, cryptographie post-quantique, chiffrement homomorphe (applications IoT/Cloud), protocoles cryptographiques, protection des données sensibles, analyses d'impact et notions DPO, blockchain et applications.

**Intelligence artificielle et confidentialité :** IA sécurisée, privacy-preserving machine learning (PPML), protection de la vie privée dans les systèmes d'apprentissage automatique, connaissance des usages de l'IA générative en contexte organisationnel.

**Ingénierie et environnements techniques :** Python, C++, LaTeX, VBA ; outils de sécurité et d'analyse (OpenSSL, liboqs, Wireshark, Burp Suite, Metasploit) ; virtualisation (VMware vSphere, NSX) ; compétences en statistiques.

**Pilotage, projets et appels d'offres :** gestion de projet complexe (PRINCE2® Foundation, Agile/Scrum, cycle en V), conduite du changement (Kotter, Lewin, ADKAR), intégration de la cybersécurité dans les projets et les appels d'offres, analyse de faisabilité, évaluation des risques, conformité (ISO 27001, RGPD).

**Pédagogie, expertise et accompagnement :** responsabilité et ingénierie de programmes académiques, conception de référentiels de compétences (RNCP/RS, VAE, CTI), innovation pédagogique (gamification, Open Badges), expertise et accompagnement en recrutement et consulting cyber, compétences en communication, leadership et gestion de la complexité.

**ENGAGEMENT COMMUNAUTAIRE**

**Depuis Septembre 2025 - Aidant cyber (MonAideCyber / ANSSI) – Diagnostic "CyberDépart"**
Membre de la communauté des Aidants cyber (tiers de confiance formés et outillés par l'ANSSI) : réalisation de diagnostics cyber de premier niveau (CyberDépart) et restitution de 6 recommandations prioritaires pour améliorer la cybersécurité des organisations.
`https://messervices.cyber.gouv.fr/cyberdepart`

**2025 -2026 Médiation scientifique – Programme Inria "1 scientifique, 1 classe : chiche !"**
5 interventions en lycées (SNT) : sensibilisation aux sciences du numérique, métiers de la recherche et cybersécurité.
`https://www.inria.fr/fr/programme-chiche-sensibilisation-numerique`

**Depuis Novembre 2023 - Membre du CEFCYS**
CEFCYS, Paris
Le CEFCYS (Cercle des Femmes de la Cybersécurité) est une association ayant pour objectif de promouvoir et renforcer la présence et le leadership des femmes dans les métiers de la cybersécurité.
`https://cefcys.fr/`

**Depuis Septembre 2023 - Membre de l'AFSIN**
AFSIN, Paris
L'Association Francophone des Spécialistes de l'Investigation Numérique rassemble enquêteurs, experts judiciaires et magistrats travaillant dans le domaine de l'investigation numérique.
`https://new.afsin.org/`

**Depuis Octobre 2020 - Membre de l'ARCSI**
ARCSI, Paris
L'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI) est une organisation majeure en France, faisant le lien entre les aspects historiques et modernes de la cryptographie et de la sécurité numérique.
`https://www.arcsi.fr/`