Athanasiou Andreas

PhD candidate at INRIA and École Polytechnique

Profile

My research focuses on designing mechanisms that protect private and sensitive data. My work expands in a variety of privacy-requiring settings: machine learning, location data, internet and statistical analytics.

Moreover, I currently assist in teaching *Computer Programming* at École Polytechnique. Previously I have assisted in teaching *Computer Security* and *Introduction to Programming* at University of Athens.

Education

2022 - 2025 (expected)
PhD candidate in Computer Science
École polytechnique
Topic: Integration of Privacy Paradigms
Supervisor: Catuscia Palamidessi

2021
MSc. in Computer Science
National and Kapodistrian University of Athens
Thesis: Tor: Tree-based Vanguards
Supervisor: Konstantinos Chatzikokolakis

2019
BSc. in Computer Science and Telecommunications
National and Kapodistrian University of Athens

Work Experience

2022 - now
PhD Candidate, INRIA Saclay
Interests: Differential Privacy · Quantitive Information Flow · Federated Learning

2018 - 2019
Junior Developer, Gnosis Management
Implement BPM systems and web services (SOAP/REST)

2015 - 2018 (part time)
Junior IT, megamed.gr
Website Management · Format scientific books · Organize medical conferences

Teaching Experience (TA)

2024 - 2025 Computer Programming, École polytechnique

2023 - 2024 Computer Programming, École polytechnique

2021 - 2023 Computer Security, National and Kapodistrian University of Athens

2020 - 2021 Introduction to Programming, National and Kapodistrian University of Athens

Papers & Publications

IEEE CSF 2025	Self-Defense: Optimal QIF Solutions and Application to Website Fingerprinting
ACM CCS 2024	Protection against Source Inference Attacks in Federated Learning using Unary Encoding and Shuffling *(poster with proceedings)*

Talks & Presentations

IEEE CSF Santa Cruz, 2025	Self-Defense: Optimal QIF Solutions and Application to Website Fingerprinting (upcoming)
ACM CCS Salt Lake City, 2024	Protection against Source Inference Attacks in Federated Learning using Unary Encoding and Shuffling *(poster)*
CNRS APVP Vogüé, 2024	Enhancing Metric Privacy with a Shuffler
CNRS PEPR winter school Autran, 2024	Enhancing Metric Privacy with a Shuffler
INRIA Ethical AI workshop Paris, 2024	Enhancing Metric Privacy with a Shuffler
Bosch CRYPTECS workshop Stuttgart, 2023	Enhancing Metric Privacy with a Shuffler
EPFL SURI summer school Lausanne, 2023	Enhancing Metric Privacy with a Shuffler *(poster)*

Organisation of Conferences & Workshops

Bertinoro, 2025	Annual Workshop of ELSA: European Project on Safe & Secure AI
Paris, 2025	15ème Atelier sur la Protection de la Vie Privée

Attended Conferences & Workshops

Lancaster University et al. Windermere, 2024	Annual Workshop of ELSA: European Project on Safe & Secure AI
Max-Planck et al. Vodice, 2024	Summer School on Real-World Crypto and Privacy
Orange Caen, 2024	Annual Workshop of CRYPTECS: Lifting privacy-preserving techniques to the cloud
NTUA Athens, 2018	National Cybersecurity Exercise **"**Panoptis"
Open Technologies Alliance Athens, 2016	Workshop "Web Application, Active Response"

Languages

English	**Proficient** (C2, University of Michigan)
German	**Good** (B1, Goethe Institute)
French	**Basic**
Greek	**Mother Tongue**

Hobbies

Open-source software · Chess · Traveling · Hiking · Motorcycle · Basketball · Cooking