# **Athanasiou** Andreas

**PhD candidate** at INRIA and École Polytechnique

## *Profile*

My research focuses on designing mechanisms to protect private and sensitive data, using the frameworks of Differential Privacy and Quantitative Information Flow. My work covers various privacy-sensitive settings: machine learning, location data, website fingerprinting and federated analytics.

I am currently a teaching assistant for Computer Programming at École Polytechnique. Previously, I assisted in teaching Computer Security and Introduction to Programming at the University of Athens.

## *Education*

*2022 - 2025 (expected)*
PhD 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 Researcher, INRIA Saclay
Interests: Differential Privacy · Quantitative Information Flow · Federated Learning

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

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

## *Teaching Experience (TA)*

*2024 - 2025* Computer Programming (introduction), École polytechnique

*2023 - 2024* Computer Programming (advanced), École polytechnique

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

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

## *Publications*

PETS 2025
Enhancing Metric Privacy With a Shuffler
**A. Athanasiou**, K. Chatzikokolakis, C. Palamidessi

| | |
|---|---|
| IEEE CSF 2025 | Self-Defense: Optimal QIF Solutions and Application to Website Fingerprinting<br>**A. Athanasiou**, K. Chatzikokolakis, C. Palamidessi |
| ACM CCS 2024 | Protection against Source Inference Attacks in Federated Learning using Unary Encoding and Shuffling<br>**A. Athanasiou**, K. Jung, C. Palamidessi |

### *Talks & Presentations*

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

### *Awards & Fellowships*

| | |
|---|---|
| École Polytechnique, 2025 | E4H BME Conference Fellowships Program |
| EPFL SURI, 2023 | Phd Student Fellowship |
| Municipality of Marousi Athens, 2014 | Outstanding Student Award |