# Dr. Andreas Athanasiou

Google Scholar ORCID andathan.github.io

My research focuses on designing mechanisms to protect private and sensitive data, seeking to provide users with strong privacy guarantees while preserving the utility of the data. In my PhD thesis, I proposed new probabilistic mechanisms for privacy amplification, in both cooperative and non-cooperative settings. My work covers various privacy-sensitive settings: machine learning, location data, private browsing, federated analytics and private set intersection. I have presented my work at ICLR, PETS, ACM CCS and IEEE CSF. Passionate about solving challenging problems with societal impact and disseminating complex ideas.

## 1 Education

**2025 PhD in Computer Science**
École Polytechnique (France)
Supervisors: *Catuscia Palamidessi and Konstantinos Chatzikokolakis*
Thesis: *Advanced Probabilistic Methods for Privacy Amplification: Cooperative and Non-Cooperative Approaches*

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

**2019 BSc in Computer Science and Telecommunications**
National and Kapodistrian University of Athens (Greece)

## 2 Work Experience

**2025-... Postdoctoral Researcher**, TU Delft (Netherlands)

- Conducting research on securing digital identities using distributed privacy-preserving technologies.
- Developing protocols for private fuzzy matching of sensitive data.
- Investigating the privacy-utility trade-off of defenses against inference attacks on ML models.
- Supervising 3 Master's students.

**2022-2025 Doctoral Researcher**, INRIA (France)

- Proposed advanced approaches for privacy amplification, resulting in 4 publications in top-tier international conferences.
- Developed a novel privacy mechanism for location data that combines shuffling with metric privacy, achieving one order-of-magnitude improvement in accuracy; this work was subsequently followed up by researchers at Google.
- Collaborated with Orange S.A., improving the accuracy of data analytics pipelines by 15%.
- Designed provably optimal mechanisms to protect users from web profiling, achieving 20% stronger protection compared to existing approaches.
- Proposed the first formal defense against an emerging inference threat on ML models, fully mitigating the attack without affecting the model's accuracy.

**2018-2019 Junior Developer**, Gnosis Management (Greece)

- Implemented 3 Business Process Management systems for major Greek companies in the banking and insurance sectors.

- Evaluated the data warehouse architecture of a leading Greek insurance company, delivering a report with 20 actionable improvement recommendations.
- Developed over 100 BI scripts to enhance data visualization and business reporting.

**2015-2018 Junior Web Developer** (part-time), MegaMed.gr (Greece)

- During my undergraduate studies, I co-developed and maintained a website for a Greek medical conference company.

## 3 Teaching Experience

**2026 Privacy-Enhancing Technologies**, Lectures and Teaching Assistant, TU Delft

**2024-2025 Computer Programming (introduction)**, Lab Teacher, École Polytechnique

**2023-2024 Computer Programming (advanced)**, Lab Teacher, École Polytechnique

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

**2020-2021 Intro to Programming**, Teaching Assistant, National and Kapodistrian University of Athens

## 4 Publications (Peer-Reviewed)

In my field, the primary publication venues are international conferences, rather than journals. ACM CCS is widely regarded as the leading conference in computer security (acceptance rate 16%). In privacy-enhancing technologies, PETS is the flagship venue of the community (acceptance rate 22%). For the theoretical foundations of computer security, IEEE CSF is considered the premier conference (acceptance rate 25%). Finally, in machine learning, ICLR is one of the three most prominent international conferences and a top-tier venue in the field (with acceptance rate of 30%).

**ICLR 2026** **[1] Protection against Source Inference Attacks in Federated Learning**
*A. Athanasiou, K. Chatzikokolakis, C. Palamidessi*
Protected against Source Inference Attacks in Federated Learning by employing a trusted shuffler with enhanced granularity. The proposed solution completely mitigates the attack, reducing its accuracy to random guessing.

**CSF 2026** **[2] Optimizing Differential Privacy in Federated Analytics under Known Input Distributions**
Collaboration with Orange S.A. and University of Stuttgart
*F. Escobar, A. Athanasiou, R. Küsters, C. Palamidessi, P. Reisert*
Provided Differential Privacy mechanisms for Federated Analytics. We proposed a novel distributed noise obfuscation mechanism that delivers superior accuracy while maintaining the same rigorous Differential Privacy guarantees.

**PETS 2025** **[3] Enhancing Metric Privacy With a Shuffler**
*A. Athanasiou, K. Chatzikokolakis, C. Palamidessi*
Improved metric privacy (a generalization of standard Differential Privacy) for location data by combining it with a trusted shuffler. The resulting framework offers the same privacy guarantees as the current state of the art but enjoys a better (by one order-of-magnitude) accuracy.

**CSF 2025** **[4] Self-Defense: optimal QIF solutions and application to Website Fingerprinting**
*A. Athanasiou, K. Chatzikokolakis, C. Palamidessi*
Provided optimal defenses against Website Fingerprinting using the framework of Quantitative Information Flow (QIF). Experiments on real-world websites show that the QIF-based solutions notably outperform other conventional defensive approaches.

**CCS 2024** **[5] Protection against Source Inference Attacks in Federated Learning using Unary Encoding and Shuffling**
*A. Athanasiou, K. Jung, C. Palamidessi*
Showed that Source Inference Attacks can be prevented via enhanced shuffling. Published as a poster (mini-paper).

**under review** **[6] Metric privacy in Federated Learning for Medical Imaging**
Collaboration with the University of Cantabria
*J. Díaz, A. Athanasiou, K. Jung, C. Palamidessi, A. García*
Improved the privacy-utility trade-off in Federated Learning with metric privacy.

### 4.1 Citations

Despite the recency of my publications, I have already received **7** citations to my work. The most notable follow-up to my work [3] came from researchers at Google. In [3], we introduced a novel analysis for the Geometric Mechanism, one of the most widely used approaches in achieving privacy. Harrison et al. from Google followed up on this work, adapting our approach in use cases which demand small noise.

### 4.2 Highlighted Talks

**2025** **Enhancing Metric Privacy With a Shuffler**, PETS 2025 (Washington D.C., USA)

**2025** **Self-Defense: optimal QIF solutions and application to Website Fingerprinting**, IEEE CSF 2025 (Santa Cruz, USA)

**2025** **Blending into the crowd: Exploring Shuffling across Different Granularities**, TU Delft (Delft, Netherlands)

**2025** **Improving privacy by increasing Shuffling Granularity**, University of Lille (Lille, France)

**2025** **Shuffling Granularity: From Location Data to Federated Learning**, IPOP: French National Consortium on Privacy (Virtual)

**2024** **How to improve Metric Privacy with Shuffling**, Ethical AI workshop (Paris, France)

**2024** **Protection against SIAs in FL using Unary Encoding and Shuffling**, ACM CCS 2024 (Salt Lake City, USA)

## 5 Service

#### Reviewing

- ACM REP 2026
- ACM CCS 2026
- ACM Transactions on Privacy and Security
- Transactions on Dependable and Secure Computing Journal
- Tsinghua Science and Technology Journal
- 14ème and 15ème Atelier sur la Protection de la Vie Privée

#### Organization

- Workshop “Safe and Secure AI” 2025, Bertinoro, Italy
- 15ème Atelier sur la Protection de la Vie Privée, Poitiers, France

## 6 Awards and Fellowships

**2025** **E4H BME Conference Fellowship Program** from École Polytechnique for my work [5].

**2023** **EPFL SURI** PhD Summer School Student Fellowship from EPFL for my work [3].