Apostolos Pyrgelis

Security & Privacy Researcher

Personal Data

Place of Birth:	Marousi, Athens, Greece
Citizenship:	Greek
Address:	BC 202, CH 1015, EPFL, Lausanne, Switzerland
Phone:	+41 21 69 37548
Email:	apostolos.pyrgelis@epfl.ch
Homepage:	https://mex2meou.github.io

Research Interests

- Computer Security & Privacy Enhancing Technologies
- Privacy-Preserving Data Analytics & Machine Learning
- Privacy Measurement & Risk Assessment
- Applied Cryptography

Education

May 2015 - Nov 2018

PhD in Computer Science from the **Information Security Group** (InfoSec) at the **Department of Computer Science** (CS-UCL), University College London (UCL), United Kingdom

Thesis: Evaluating Privacy-Friendly Mobility Analytics on Aggregate Location Data | Advisor: Prof. Emiliano De Cristofaro | Co-Advisor: Dr. Gordon Ross

Oct 2009 - Mar 2012

Master's Degree in Computer Science and Engineering at the **Department of Computer Science and Engineering** (CEID), University of Patras, Greece

Thesis: Development of Cryptographic Algorithms for Heterogeneous Wireless Sensor Networks | Advisors: Prof. Paul Spirakis, Prof. Yannis Stamatiou, Dr. Ioannis Chatzigiannakis

Certificate Degree: "Excellent"

Jan 2009 - Jun 2009

Socrates/Erasmus Exchange Student at the **Department of Computer Science and Engineering** (CSE-TKK), Helsinki University of Technology, Finland

Sep 2003 - Sep 2009

Diploma in Computer Science and Engineering at the **Department of Computer Science and Engineering** (CEID), University of Patras, Greece

Thesis: Development of a Cryptographic Protocol Using Elliptic Curves for Wireless Sensor Networks | Advisors: Prof. Paul Spirakis, Dr. Ioannis Chatzigiannakis, Dr. Vasiliki Liagkou

Certificate Degree: 7,91 / 10

Sep 2000 - June 2003 | Anavrita Experimental Highschool, Marousi, Athens

Certificate Degree: 18,9 / 20

Employment

Dec 2018 - | Post-doctoral Researcher at the School of Computer and Communication Sciences (IC) of École Polytechnique Fédérale de Lausanne (EPFL)

I am currently working as a senior security and privacy researcher under the supervision of Prof. Jean-Pierre Hubaux and Prof. Carmela Troncoso. My role is to engage in cutting-edge research projects as well as supervise and mentor junior researchers towards their goals.

Sep 2017 - Dec 2017 | Research Intern at Telefonica Research Barcelona (TID)

Analysis of a large-scale mobility dataset derived from mobile network events. In particular, the project investigated the uniqueness of mobility patterns, their inherent characteristics, and their privacy implications.

Technologies Used: Python (numpy, numba)

Jun 2016 - Aug 2016 | Research Intern at the Alan Turing Institute (ATI)

Analysis of a broad dataset provided by a youth support charity in terms of topics, languages and peer-support as well as application of machine learning techniques for predictive tasks.

Technologies Used: Python (pandas, scikit-learn, NetworkX), MySQL

May 2014 - Mar 2015 | Analyst - Software Engineer at the Center of Information Technology Support of the Hellenic Army (KEPYES)

While fulfilling my military service at KEPYES - located at the Ministry of National Defense, I maintained and supported various military administrative applications.

Technologies Used: Java, JSP, Javascript, Hibernate, Oracle

Nov 2010 - May 2014 | Researcher at Computer Technology Institute and Press "Diophantus" (CTI), Patras, Greece

EU FP7 Project ABC4Trust: Attribute Based Credentials for Trust

Design of pilot scenarios for privacy protection of end users, implementation of web applications and integration of the ABC4Trust technology, development of cryptographic protocols for smart cards (Zeit Control Basic Card, MultOS), organization and administration of the project pilot at University of Patras, system maintenance and administration (Ubuntu Linux, Windows Server 2008), statistical evaluation of the pilot results using questionnaires, active participation in the writing of project deliverables, research papers.

Technologies Used: Java, REST-WS, Jetty, PHP, MySQL, Apache, Drupal

Sep 2010 - Oct 2010 | Researcher at Computer Technology Institute and Press "Diophantus" (CTI), Patras, Greece

EU FP7 Project VITRO: Virtualized Distributed Platforms of Smart Objects

Research on the integration of cryptographic algorithms at the project platform, development of cryptographic algorithms (AES, SHA-1, ECDH, ECIES, ECDSA) on the Wiselib library

Technologies Used: C, C++

Dec 2007 - Dec 2008 | Employee of the Hellenic Telecommunications Organization (OTE), Patras, Greece.

I worked as an operator of administrative IT customer service applications.

Publications

David Froelicher, Hyunghoon Cho, Manaswitha Edupalli, Joao Sa Sousa, Jean-Philippe Bossuat, Apostolos Pyrgelis, Juan R. Troncoso-Pastoriza, Bonnie Berger, and Jean-Pierre Hubaux, **Scalable and Privacy-Preserving Federated Principal Component Analysis**, in IEEE Security and Privacy (S&P), San Francisco, California, USA, 2023 Details

Hyunghoon Cho, David Froelicher, Jeffrey Chen, Manaswitha Edupalli, Apostolos Pyrgelis, Juan R. Troncoso-Pastoriza, Jean-Pierre Hubaux, and Bonnie Berger, **Secure and Federated Genome-Wide Association Studies for Biobank-Scale Datasets**, in bioRxiv pre-print, 2022 Details

Sinem Sav, Abdularhman Diaa, Apostolos Pyrgelis, Jean-Philippe Bossuat, and Jean-Pierre Hubaux, **Privacy-Preserving Federated Recurrent Neural Networks**, arXiv pre-print, 2022 Details

Sylvain Chatel, Christian Knabenhans, Apostolos Pyrgelis, and Jean-Pierre Hubaux, **Verifiable Encodings for Secure Homomorphic Analytics**, arXiv pre-print, 2022 Details

Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda Gürses, Jean-Pierre Hubaux, Dennis Jackson, James R. Larus, Wouter Lueks, Rui Oliveira, Mathias Payer, Bart Preneel, Apostolos Pyrgelis, Marcel Salathé, Theresa Stadler, and Michael Veale, **Lessons from a Pandemic: Deploying Decentralized Privacy-Preserving Proximity Tracing**, in Communications of the ACM, September 2022 Details

Anisa Halimi, Leonard Dervishi, Erman Ayday, Apostolos Pyrgelis, Juan R. Troncoso-Pastoriza, Jean-Pierre Hubaux, Xiaoqian Jiang, and Jaideep Vaidya, **Privacy-Preserving and Efficient Verification of the Outcome in Genome-Wide Association Studies**, in Proceedings on Privacy Enhancing Technologies (PoPETS), Hybrid Event, 2022 Details

Ludovic Barman, Alexandre Dumur, Apostolos Pyrgelis, and Jean-Pierre Hubaux, **Every Byte Matters: Traffic Analysis of Bluetooth Wearable Devices**, in International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), Virtual Event, 2021 Details

Sylvain Chatel, Apostolos Pyrgelis, Juan R. Troncoso-Pastoriza, and Jean-Pierre Hubaux, **Privacy and Integrity Preserving Computations with CRISP**, in 30th Usenix Security Symposium, Virtual Event, 2021 Details

Sylvain Chatel, Apostolos Pyrgelis, Juan R. Troncoso-Pastoriza, and Jean-Pierre Hubaux, **SoK: Privacy-Preserving Collaborative Tree-based Model Learning**, in Proceedings on Privacy Enhancing Technologies (PoPETS), Virtual Event, 2021 Details

David Froelicher, Juan R. Troncoso-Pastoriza, Apostolos Pyrgelis, Sinem Sav, Joao Sa Sousa, Jean-Philippe Bossuat, and Jean-Pierre Hubaux, **Scalable Privacy-Preserving Distributed Learning**, in Proceedings on Privacy Enhancing Technologies (PoPETS), Virtual Event, 2021 Details

Sinem Sav, Apostolos Pyrgelis, Juan R. Troncoso-Pastoriza, David Froelicher, Jean-Philippe Bossuat, Joao Sa Sousa, and Jean-Pierre Hubaux, **POSEIDON: Privacy-Preserving Federated Neural Network Learning**, in Proceedings of the 28th Network and Distributed System Security Symposium (NDSS), Virtual Event, 2021 Details

Ludovic Barman, Italo Dacosta, Mahdi Zamani, Ennan Zhai, Apostolos Pyrgelis, Bryan Ford, Joan Feigenbaum, and Jean-Pierre Hubaux, **PriFi: Low-Latency Anonymity for Organizational Networks**, in Proceedings on Privacy Enhancing Technologies (PoPETS), Virtual Event, 2020 Details

Apostolos Pyrgelis, Carmela Troncoso, and Emiliano De Cristofaro, **Measuring Membership Privacy on Aggregate Location Time-Series**, in ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS), Virtual Event, 2020 Details

Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathe, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Capkun, David Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel Smart, Aysajan Abidin, Seda Gurses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, and Jose Pereira. **Decentralized Privacy-Preserving Proximity Tracing**, in IEEE Data Engineering Bulletin, Volume 43, 2020 Details

Apostolos Pyrgelis, Nicolas Kourtellis, Ilias Leontiadis, Joan Serrà, and Claudio Soriente, **There goes Wally: Anonymously sharing your location gives you away**, in IEEE International Conference on Big Data, Seattle, WA, USA, 2018 Details

Luca Melis, Apostolos Pyrgelis, and Emiliano De Cristofaro, **On Collaborative Predictive Blacklisting**, in ACM SIGCOMM's Computer Communication Review (Volume 48, Issue 5, October 2018) Details

Apostolos Pyrgelis, Carmela Troncoso, and Emiliano De Cristofaro, **Knock Knock, Who's There? Membership Inference on Aggregate Location Data**, in Proceedings of the 25th Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, 2018 Details

Apostolos Pyrgelis, Carmela Troncoso and Emiliano De Cristofaro, **What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy**, in Proceedings of the 17th Privacy Enhancing Technologies Symposium (PoPETS), Minneapolis, Minnesota, USA, 2017 Details

Apostolos Pyrgelis, Emiliano De Cristofaro, and Gordon Ross, **Privacy-Friendly Mobility Analytics using Aggregate Location Data**, in 24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, Burlingame, California, USA, 2016 Details

Ioannis Chatzigiannakis, Andrea Vitaletti, and Apostolos Pyrgelis, **A privacy-preserving smart parking system using an IoT elliptic curve based security platform**, in Journal of Computer Communications, 2016 Details

Vasiliki Liagkou, George Metakides, Apostolos Pyrgelis, Christoforos Raptopoulos, and Yannis Stamatiou, **Privacy Preserving Course Evaluations in Greek Higher Education Institutes: an eParticipation case study with the empowerment of Attribute Based Credentials**, in Annual Privacy Forum, Limassol, Cyprus, 2012 Details

Ioannis Chatzigiannakis, Apostolos Pyrgelis, Paul Spirakis, and Yannis Stamatiou, **Elliptic Curve Based Zero Knowledge Proofs and their Applicability on Resource Constrained Devices**, in Mobile Adhoc and Sensor Systems (MASS), Valencia, Spain, 2011 Details

Dimitrios Amaxilatis, Ioannis Chatzigiannakis, Shlomi Dolev, Christos Koninis, Apostolos Pyrgelis, and Paul Spirakis, **Adaptive Hierarchical Network Structures for Wireless Sensor Networks**, in 3rd ICST International Conference on Ad Hoc Networks, Paris, France, 2011

Details

Tobias Baumgartner, Ioannis Chatzigiannakis, Sandor Fekete, Christos Koninis, Alexander Kröller, and Apostolos Pyrgelis, **Wiselib: A Generic Algorithm Library for Heterogeneous Sensor Networks**, in 7th European Conference on Wireless Sensor Networks (EWSN), Coimbra, Portugal, 2010 Details

Technical Reports

Souheil Bcheri, Norbert Goetze, Vasiliki Liagkou, Apostolos Pyrgelis, Christoforos Raptopoulos, Yannis Stamatiou, Katalin Storf, Peder Wängmark, and Harald Zwingelberg, **EU FP7 ABC4TRUST - D5.1: Scenario Definition for both Pilots**, Details

Souheil Bcheri, Kasper L. Damgaard, Daniel Deibler, Norbert Goetze, Hans G. Knudsen, Maksym Moneta, Apostolos Pyrgelis, Eva Schlehahn, Michael B. Stausholm, and Harald Zwingelberg, **EU FP7 ABC4TRUST - D5.3: Experiences and Feedback of the Pilots** Details

Joerg Abendroth, Vasiliki Liagkou, Apostolos Pyrgelis, Christoforos Raptopoulos, Ahmad Sabouri, Eva Schlehahn, Yannis Stamatiou, and Harald Zwingelberg, **EU FP7 ABC4TRUST - D7.1: Application Description for Students** Details

Kasper Damgaard, Hamza Ghani, Norbert Goetze, Anja Lehmann, Vasiliki Liagkou, Jesus Luna, Gert Læssøe Mikkelsen, Apostolos Pyrgelis, and Yannis Stamatiou, **EU FP7 ABC4TRUST - D7.2: Necessary hardware and software package for the student pilot deployment** Details

Daniel Deibler, Malte Engeler, Ioannis Krontiris, Anja Lehmann, Vasiliki Liagkou, Apostolos Pyrgelis, Eva Schlehahn, Yannis Stamatiou, Welderufael Tesfay, and Harald Zwingelberg, **EU FP7 ABC4TRUST - D7.3: Evaluation of the Student Pilot** Details

Patents

Apr 2022 **System and method for privacy-preserving distributed training of neural network models on distributed datasets**, based on the paper titled *POSEIDON: Privacy-Preserving Federated Neural Network Learning (NDSS'21)*.

Mar 2021 **System and method for privacy-preserving distributed training of machine learning models on distributed datasets**, based on the paper titled *Scalable Privacy-Preserving Distributed Learning (PoPETS'21)*.

Talks & Articles

Measuring Membership Privacy on Aggregate Location Time-Series, 9 June 2020, ACM SIGMETRICS, Virtual Event Details

On Location, Time, and Membership: Studying How Aggregate Location Data Can Harm Users' Privacy, 2 Oct 2018 Details

Building and Evaluating Privacy-Friendly Mobility Analytics on Aggregate Location Data, 29 June 2018, PrivaSec Seminar, EPFL, Switzerland Details

Knock Knock, Who's There? Membership Inference on Aggregate Location Data, 20 Feb 2018, NDSS, San Diego, California, USA Details

What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy, 19 Jul 2017, PETS, Minneapolis, Minnesota, USA Details

Privacy-Friendly Mobility Analytics using Aggregate Location Data, 3 Nov 2016, ACM SIGSPATIAL, Burlingame, California, USA Details

Ioannis Krontiris and Apostolos Pyrgelis, **Menschen vergessen – Systeme nicht, Mehr Datenschutz für den Einzelnen mit ABC4Trust**, PHP Magazine Vol. 5/12. PHP Magazine, 2012.

Cryptography and Security in Wireless Sensor Networks, 14 Oct 2009, FRONTS 2nd Winterschool, Braunschweig, Germany Details

Service

PC Member: USENIX Security Symposium (2023), Privacy Enhancing Technologies Symposium - PETS (2023, 2022).

Reviewer: PoPETS, NDSS, ACM CCS, IEEE S&P, WWW, ACM ASIACCS, ACM WISEC, ICWSM, Elsevier Ad Hoc Networks, Elsevier Computers and Security, IEEE Pervasive Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Network Science and Engineering, IEEE Internet of Things, Journal of Computer Security, Nature Communications, Nature Machine Intelligence.

Teaching

Instructor at EPFL: Information Security and Privacy (2022, 2021)

Teaching Assistant: Introduction to Cryptography (UCL, 2016), Computer Security I (UCL, 2015), Distributed Systems I (CEID, 2011), Operating Systems I (CEID, 2010)

Honors & Awards

Sep 2022 **IMWUT Distinguished Paper Award**, for the paper titled *Every Byte Matters: Traffic Analysis of Bluetooth Wearable Devices (UbiComp'21)*.

Jul 2022 **Top Reviewer Award**, for the service performed for the Privacy Enhancing Technologies Symposium (PETS) of 2022.

Nov 2021 **CSAW'21 Applied Research Competition Europe 1st Place**, for the paper titled *POSEIDON: Privacy-Preserving Federated Neural Network Learning (NDSS'21)*.

Jan 2021 **Huawei Bug Bounty & Responsible Disclosure Award**, for the paper titled *Every Byte Matters: Traffic Analysis of Bluetooth Wearable Devices (UbiComp'21)*.

Jan 2020 **INRIA-CNIL Privacy Protection Award Runner-up**, for the paper titled *Knock Knock, Who's There? Membership Inference on Aggregate Location Data (NDSS'18)*.

May 2018 **Hall of Famer**, for our linkability attack on the Aircloak Attack Challenge.

Feb 2018 **NDSS 2018 Distinguished Paper Award**, for the paper titled *Knock Knock, Who's There? Membership Inference on Aggregate Location Data*.

Jul 2017 **PETS 2017 Stipend Award**, for attending the Privacy Enhancing Technologies Symposium (PETS), Minneapolis, Minnesota, USA.

Nov 2016 **ACM SIGSPATIAL 2016 Travel Award**, for attending the International Conference on Advances in Geographic Information Systems, ACM SIGSPATIAL, Burlingame, California, USA.

May 2016 **TPMPC Travel Award**, for attending the workshop on Theory and Practice of Multi-Party Computation (TPMPC), Aarhus, Denmark.

Computer Skills

Programming: C, C++, C#, Java, Python, PHP, JSP, Hibernate, MySQL, Oracle, Matlab, HTML, Javascript, Ajax, CSS, Xml

Operating Systems: Microsoft Windows, Linux, Unix, Mac Os X

Foreign Languages

English: Michigan Certificate of Proficiency in English, year 2001
IELTS Cambridge English Language Assessment (7,5 / 9), year 2015

French: Delf A1, A2, A3, A4, year 2000

Interests & Activities

Sports: Basketball, Football, Swimming, Hiking, Mountain Running, Climbing, Table Tennis, Cycling

Hobbies: Music, Cinema, Literature, Technology

Last Update: January 4, 2023