As of November 2024

Dimitrios (Dimitris) Mouris

400 Walnut St. Apt. 10E, Philadelphia, PA 19106, USA

(+1) (302) 407-2887 | jimouris@udel.edu | jimouris.github.io | jimouris | jimouris | @jimouris | FaHg3QoAAAAJ

Applied cryptography researcher motivated by the impact of cryptography in contemporary society and in humanity.

Research & Work Experience

Nillion (Nilogy Inc.) — *Remote*

Senior Cryptography Researcher — *January 2024 – Now*

Research and development of an MPC compiler and protocols for Nillion's secure and distributed computing platform.

University of Delaware — *Newark, DE, USA*

Research & Teaching Assistant — *February 2019 – December 2023*

Applied Cryptography • Secure Multiparty Computation • Homomorphic Encryption • Zero-knowledge Proofs

Meta Inc. — *Bellevue, WA, USA & Remote*

Part-Time Student Researcher (Remote) — *September 2022 – December 2022*

Research Engineer Intern — *June 2022 – August 2022*

Development of privacy-enhancing solutions that solve real-world problems such as private attribution and privacy-preserving personalization. Research and implementation of *Delegated Private Matching for Compute*. *Blogpost*, *Private-ID*

Amazon Web Services (AWS) — *Palo Alto, CA, USA*

Software Development Engineer (SDE) Intern — *June 2021 – August 2021*

Development of Role-Based Access Control (RBAC) for Amazon Redshift to manage permissions and security privileges.

Athena Research & Innovation Center — *Athens, Greece*

Research Assistant & Software Engineer — *September 2017 – December 2018*

My Health My Data (MHMD) project: Design and implementation of an end-to-end framework for privacy-preserving medical data analytics (i.e., histograms and decision trees) using secure multi-party computation (MPC). *smpc-analytics*

Education

Department of Electrical & Computer Engineering, University of Delaware — *Newark, DE, USA*

Doctor of Philosophy (PhD) in Electrical and Computer Engineering — *February 2019 – December 2023*

- Research Topic: *Private and Verifiable Computation* — Advisor: Nektarios G. Tsoutsos
- My research focuses on privacy-preserving technologies and on building efficient solutions that respect data privacy using cryptographic techniques such as *zero-knowledge proofs*, *homomorphic encryption*, and *secure multiparty computation*.

Department of Informatics & Telecommunications, University of Athens — *Athens, Greece*

Master of Science (MSc) in Computer Science — *October 2016 – September 2018*

The *Computer Systems (Software and Hardware)* specialization covers advanced topics in areas such as computer security & architecture, operating & distributed systems, programming languages, algorithms & data structures.

Department of Informatics & Telecommunications, University of Athens — *Athens, Greece*

Bachelor of Science (BSc) in Computer Science — *October 2012 – September 2016*

Publications (Selected)

Journal Articles

- D. Mouris, C. Patton, H. Davis, P. Sarkar, and N. Tsoutsos. **"Mastic: Private Weighted Heavy-Hitters and Attribute-Based Metrics"** in *Proc. Priv. Enhancing Technol. (PoPETs)*, vol. 2025, no. 1, *IETF - CFRG*, — *2025*
- C. Gouert, D. Mouris, and N. Tsoutsos. **"Juliet: A Configurable Processor for Computing on Encrypted Data"** in *IEEE Trans. on Computers*, vol. 73, no. 9, — *2024*
- D. Mouris, P. Sarkar, and N. Tsoutsos. **"PLASMA: Private, Lightweight Aggregated Statistics against Malicious Adversaries"** in *Proc. Priv. Enhancing Technol. (PoPETs)*, vol. 2024, no. 3, *IETF - CFRG*, — *2024*
- D. Mouris, D. Masny, N. Trieu, S. Sengupta, P. Buddhavarapu, and B. Case. **"Delegated Private Matching for Compute"** in *Proc. Priv. Enhancing Technol. (PoPETs)*, vol. 2024, no. 2, *Blogpost*, — *2024*
- C. Gouert, D. Mouris, and N. Tsoutsos. **"SoK: New Insights into Fully Homomorphic Encryption Libraries via Standardized Benchmarks"** in *Proc. Priv. Enhancing Technol. (PoPETs)*, vol. 2023, no. 3, pp. 154–172, , — *2023*
- D. Mouris, C. Gouert, and N. Tsoutsos. **"Privacy-Preserving IP Verification"** in *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, vol. 41, no. 7, pp. 2010–2023 — *2021*
- D. Mouris and N. Tsoutsos. **"Zilch: A Framework for Deploying Transparent Zero-Knowledge Proofs"** in *IEEE Trans. on Information Forensics and Security (TIFS)*, vol. 16, pp. 3269–3284, — *2021*

- D. Mouris, N. Tsoutsos, and M. Maniatakos. **"TERMinator suite: Benchmarking Privacy-Preserving Architectures"** in *IEEE Computer Architecture Letters,* vol. 17, no. 2, pp. 122–125, *2018*

Conference Papers

- C. Gouert, M. Ugurbil, D. Mouris, M. de Vega, and N. Tsoutsos. **"Ripple: Accelerating Programmable Bootstraps for FHE with Wavelet Approximations"** in *27th Information Security Conference (ISC),* *FHE Summit*, *2024*
- M.B. Santos, D. Mouris, M. Ugurbil, S. Jarecki, J. Reis, S. Sengupta, and M. de Vega. **"Curl: Private LLMs through Wavelet-Encoded Look-Up Tables"** in *Conference on Applied Machine Learning in Information Security (CAMLIS),* *2024*
- D. Mouris, C. Gouert, and N. Tsoutsos. **"MPloC: Privacy-Preserving IP Verification using Logic Locking and Secure Multiparty Computation"** in *IEEE 29th Int. Symp. on On-Line Testing and Robust System Design (IOLTS),* *2023*
- D. Mouris, C. Gouert, and N. Tsoutsos. **"zk-Sherlock: Exposing Hardware Trojans in Zero-Knowledge"** in *IEEE Computer Society Annual Symposium on VLSI (ISVLSI),* pp. 170-175 *2022*
- D. Mouris and N. Tsoutsos. **"Pythia: Intellectual Property Verification in Zero-Knowledge"** in *ACM/IEEE 57th Design Automation Conference (DAC),* pp. 1–6 *2020*

Open-access Archives

- C. Gouert, D. Mouris, and N. Tsoutsos. **"HELM: Navigating Homomorphic Encryption through Gates and Lookup Tables"** in *Cryptology ePrint Arch.,* 2023/1382, *2023*

Theses

- D. Mouris. **"Private And Verifiable Computation"** in *Ph.D. Thesis,* Advisor: N.G Tsoutsos, *2024*
- A. Giannopoulos and D. Mouris. **"Privacy preserving medical data analytics using secure multi party computation. An end-to-end use case"** in *M.Sc. Thesis,* Supervisors: Y. Ioannidis and M. Garofalakis, *2018*

Technical Skills

Programming Paradigms	Procedural, Object Oriented, Logic, Functional		
Programming Languages	Rust, C, C++, Java, Python, Go, Haskell		
Parallel Programming	POSIX processes & threads, MPI, Open MP		
Assembly Languages	x86/x64, MIPS	**Database Systems**	SQL, MySQL
Version Control	Git, Mercurial	**Languages**	Greek (native), English (fluent)

Teaching Assistant

U. of Delaware	Reverse Eng. & Pen. Testing (Fall '21, '22), Microprocessor Sys. (Fall '20), Applied Cryptography (Spr. '20, '21), Secure Soft. Design (Spr. '20, '21), Embedded Systems Sec. (Fall '19 – '21)
U. of Athens	Sys. Prog. (Spr. '17), Logic Prog. (Spr. '17), Intro to Prog. (Fall '14 – '17), Operating Systems (Fall '16)

Honors & Awards

2023	**Conference Stipend**, Travel stipend for Privacy Enhancing Technologies Symposium (PETS)	*Lausanne*
2021	**Student Conference Grant**, Registration for ACM Symp. on Computer and Com. Security (CCS)	*Virtual*
2021	**1st for outstanding research presentation**, IEEE Reliable and Resilient Digital Manufacturing	*Virtual*
2020	**Scholarship**, Outstanding Academic Performance Scholarship, from the Gerondelis Foundation	*Grant $5,000*
2020	**DAC Young Fellow Program**, 57th Design Automation Conference, July 20-24	*Virtual*
2016	**Scholarship**, Programming Languages Mentoring Workshop (PLMW) at SPLASH 2016, 10/30-11/4	*Amsterdam*

Professional Service

Reviewer	FHE.org (2025), PETS (2023), CSAW Applied Research (2019 – 2024), IEEE Access (2020, 2022), Elsevier FGCS (2020)
External	ACM TACO (2021 – 2022), DAC (2020 – 2021), AIHC (2019), AsianHOST (2020), GLSVLSI (2023), IEEE Access (2019), IEEE Computer (2019), IEEE ESL (2019), IEEE HOST (2019, 2023), IEEE ICCD (2019), IEEE IOLTS (2023), IEEE ISVLSI (2019), IEEE MICRO (2019 – 2023), IEEE TCAD (2019, 2022, 2023), IEEE TETC (2019), IEEE TIFS (2019), IEEE DSN (2020), VLSI-SoC (2019) Springer JETT (2019)

Community Service

BlueHens Capture The Flag (CTF) Competition - UDCTF *Global Event*

Global Co-lead *2021, 2022*

Challenge developer and organizer for research and educational oriented CTF competition. *Event on ctftime.org/event/1298*

CSAW Cybersecurity Games & Conference – Embedded Security Challenge *Global Event*

Global Co-lead *2020, 2021, 2022, 2023*

Challenge developer and organizer for research-oriented embedded systems hacking competition.