Last updated on September 15, 2022

Dimitrios (Dimitris) Mouris

3514 Spring Garden St. Apt. A21, Philadelphia, PA 19104, USA

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

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

Research & Work Experience

University of Delaware — *Newark, DE, USA*

Research Assistant — *February 2019 – Now*

Applied Cryptography • Zero-knowledge Proofs • Homomorphic Encryption • Secure Multi-party Computation

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

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

Research Engineer Intern — *June 2022 – August 2022*

Privacy-enhancing solutions that solve real-world problems such as private set intersection (PSI) and multi-party private matching protocols with the Statistics & Privacy Team.

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: Developed 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 – Now*

- Research Topic: *Private and trustworthy 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 multi-party 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)

Articles

A4 — D. Mouris, C. Gouert and N.G. Tsoutsos. **"Privacy-Preserving IP Verification"** in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)* — *2021*

A3 — D. Mouris and N.G. Tsoutsos. **"Zilch: A Framework for Deploying Transparent Zero-Knowledge Proofs"** in *IEEE Transactions on Information Forensics and Security (TIFS)* 16, (pp. 3269–3284) — *2021*

A2 — D. Mouris, C. Gouert, N. Gupta, and N.G. Tsoutsos. **"Peak Your Frequency: Advanced Search of 3D CAD Files in the Fourier Domain"** in *IEEE Access, 8, (pp. 141481–141496)* 8, (pp. 141481-141496) — *2020*

A1 — D. Mouris, N.G. Tsoutsos, and M. Maniatakos. **"TERMinator suite: Benchmarking Privacy-Preserving Architectures"** in *IEEE Computer Architecture Letters* 17(2), (pp. 122–125) — *2018*

Proceedings

P3 — D. Mouris, C. Gouert and N.G. Tsoutsos. **"zk-Sherlock: Exposing Hardware Trojans in Zero-Knowledge"** in *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (pp. 1–6) — *2022*

P2 — D. Mouris and N.G. Tsoutsos. **"Pythia: Intellectual Property Verification in Zero-Knowledge"** in *57th Design Automation Conference (DAC)* (pp. 1–6). ACM/EDAC/IEEE — *2020*

P1 — P. Cronin, C. Gouert, D. Mouris, N.G. Tsoutsos, and C. Yang. **"Covert Data Exfiltration Using Light and Power Channels."** in *37th International Conference on Computer Design (ICCD)* (pp. 301–304). — *2019*

Open-access Archives

O2 C. Gouert, D. Mouris and N.G. Tsoutsos. **"New Insights into Fully Homomorphic Encryption Libraries via Standardized Benchmarks"** in *Cryptology ePrint Archive* Report 2022/425 — *2022*

O1 D. Mouris and N.G. Tsoutsos. **"Masquerade: Verifiable Multi-Party Aggregation with Secure Multiplicative Commitments"** in *Cryptology ePrint Archive* Report 2021/1370 — *2021*

Theses

T1 A. Giannopoulos and D. Mouris. **"Privacy preserving medical data analytics using secure multi party computation. An end-to-end use case"** in *Master's Thesis, National and Kapodistrian University of Athens.* Supervisors: Y. Ioannidis and M. Garofalakis — *2018*

Technical Skills

Programming Paradigms	Procedural ☰, Object Oriented ☰, Logic ☰, Functional ☰
Programming Languages	C ☰, C++ ☰, Java ☰, Rust 〓, Python 〓, Go 〓, Haskell ☰
Parallel Programming	POSIX processes & threads ☰, MPI ☰, Open MP ☰
Assembly Languages	x86/x64 ☰, MIPS 〓
Markup & Web Languages	NodeJS 〓, JS ☰, HTML ☰
Scripting	Z shell ☰, Bash ☰
Database Systems	SQL 〓, MySQL 〓
Version Control	Git ☰, Mercurial ☰
Languages	Greek (native), English (fluent)

Teaching Assistant

University of Delaware

Reverse Engineering & Penetration Testing (Fall 2021), Microprocessor Systems (Fall 2020), Applied Cryptography (Spring 2020, 2021), Secure Software Design (Spring 2020, 2021), Embedded Systems Security (Fall 2019 – 2021)

University of Athens

System Programming (Spring 2017), Logic Programming (Spring 2017), Introduction to Programming (Fall 2014 – 2017), Operating Systems (Fall 2016)

Honors & Awards

2021 **Student Conference Grant**, Registration for ACM Symp. on Computer and Com. Security (CCS) — *ACM CCS*

2021 **1st Place for outstanding research presentation**, Reliable and Resilient Digital Manufacturing — *IEEE Workshop*

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*

Professional Service

Reviewer

CSAW Applied Research Competition (2019 – 2022), IEEE Access (2020), Elsevier FGCS (2020)

External/Sub-Reviewer

AIHC (2019), ACM TACO (2021 – 2022), AsianHOST (2020), ACM/ESDA/IEEE DAC (2020 – 2021), IEEE/IFIP DSN (2020), IEEE ESL (2019), IEEE HOST (2019), IEEE ICCD (2019), IEEE Access (2019), IEEE Computer (2019), IEEE ISVLSI (2019), IEEE MICRO (2019 – 2022), Springer JETT (2019), IEEE TCAD (2019), IEEE TETC (2019), IEEE TIFS (2019), IFIP/IEEE VLSI-SoC (2019)

Community Service

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

Global Co-lead — *2021*

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*

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

CTF Mentoring — *Newark, DE, USA*

Mentor — *2019 – Now*

Cryptography, binary exploitation, and reverse engineering mentoring for the University of Delaware's *Blue Hens* team.