Dimitrios VASILOPOULOS

Dimitrios.Vasilopoulos@eurecom.fr | https://dimvasilopoulos.github.io
Residence: Madrid, Spain | Nationality: Hellenic

SUMMARY

Over the past three years, I was a post-doctoral researcher at IMDEA Software Institute in Madrid (Spain) under the direction of Pedro MORENO-SANCHEZ, where I worked on the design of provable secure and privacy-preserving cryptographic protocols for payments over blockchain technologies.

In 2019, I obtained my *Ph.D.* from Sorbonne University, which took place at EURECOM in Sophia Antipolis (France) under the direction of Refik MOLVA and Melek ÖNEN. During my *Ph.D.*, I worked on verifiable cloud storage designing cryptographic protocols that reconcile cloud storage functionalities with security. More specifically, I worked on the design of cryptographic protocols that succeed in verifying the reliable storage of outsourced data while enabling cloud storage providers to autonomously perform automatic data maintenance and data reduction operations.

I have published six (6) papers in international peer-reviewed conferences, workshops, and journals in the fields of blockchain security, cloud security, and applied cryptography. I have delivered five (5) public talks including three (3) presentations at international conferences. Moreover, I have participated in the program committee of seven (7) international conferences and workshops and served as a reviewer for five (5) international journals. Lastly, I have actively contributed to the preparation and instruction of a graduate-level course in cryptography and supervised a doctoral student and four (4) graduate students on their thesis work.

EDUCATION

EURECOM | Sorbonne University Sophia Antipolis, France
Ph.D. in Information Technology, Telecommunications and Electronics, July 2019
- *Dissertation:* "Reconciling Cloud Storage Functionalities with Security: Proofs of Storage with Data Reliability and Secure Deduplication."

Major Fields: Security Protocols and Applied Cryptography
Advisors: Professor Refik MOLVA, Professor Melek ÖNEN

EURECOM | Télécom ParisTech Sophia Antipolis, France
M.Sc. in Communications and Computer Security, January 2014
Advisor: Professor Refik MOLVA

Technical University of Crete Chania, Greece
Department of Electronic and Computing Engineering
Engineering Diploma (≈B.ENG. & M.ENG.) in Electronic and Computing Engineering, March 2010
- *Thesis:* "Design and Experimental Setup for High Speed Serial Communication with FPGA."

Advisor: Professor Apostolos DOLLAS

PUBLICATIONS

Publications in International Conferences and Journals:

1. Diego CASTEJON-MOLINA, Dimitrios VASILOPOULOS, Pedro MORENO-SANCHEZ.
"MixBuy: Contingent Payment in the Presence of Coin Mixers."
In Proceedings on Privacy Enhancing Technologies *(PoPETs)*, 2025.1, (To appear), https://eprint.iacr.org/2024/953.
2. Varun MADATHIL, Sri AravindaKrishan THYAGARAJAN, Dimitrios VASILOPOULOS, Lloyd FOURNIER, Giulio MALAVOLTA, Pedro MORENO-SANCHEZ.
"Cryptographic Oracle-based Conditional Payments."
In Proceedings of the 30th Annual Network and Distributed System Security Symposium *(NDSS)*, 2023, (Acceptance rate ~16.4%).
3. Dimitrios VASILOPOULOS, Melek ÖNEN, Refik MOLVA, Kaoutar ELKHIYAOUI.
"Proofs of Data Reliability: Verification of Reliable Data Storage with Automatic Maintenance."
Security and Privacy, 2020;e137 | *Special Issue Invited Submission*.

4. Dimitrios Vasilopoulos, Melek Önen, Refik Molva.
"PORTOS: Proof of Data Reliability for Real-World Distributed Outsourced Storage."
In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications *(SECRYPT)*, 2019,
(Acceptance rate ~16%) | ***Best Student Paper Award***.
5. Dimitrios Vasilopoulos, Kaoutar ElKhiyaoui, Refik Molva, Melek Önen.
"POROS: Proof of Data Reliability for Outsourced Storage."
In Proceedings of the 6th International Workshop on Security in Cloud Computing *(ACM ASIACCS-SCC)*, 2018,
(Acceptance rate ~35%).
6. Dimitrios Vasilopoulos, Melek Önen, Kaoutar ElKhiyaoui, Refik Molva.
"Message-Locked Proofs of Retrievability with Secure Deduplication."
In Proceedings of the 2016 ACM on Cloud Computing Security Workshop *(ACM CCS-CCSW)*, 2016,
(Acceptance rate ~24%).

Submissions and Preprint:

- Javier Gomez-Martinez, Dimitrios Vasilopoulos, Pedro Moreno-Sanchez, Dario Fiore.
"Algebraic Zero Knowledge Contingent Payment."
- Erkan Tairi, Diego Castejon-Molina, Dimitrios Vasilopoulos, Pedro Moreno-Sanchez.
"Blind Adaptor Signatures and Blind Atomic Swaps."
- Diego Castejon-Molina, Alberto del Amo Pastelero, Dimitrios Vasilopoulos, Pedro Moreno-Sanchez.
"A Cryptographic Layer for the Interoperability of CBDC and Cryptocurrency Ledgers."
Cryptology ePrint Archive, Paper 2023/116, 2023, https://eprint.iacr.org/2023/116.

EMPLOYMENT

IMDEA Software Institute — Madrid, Spain
Post-doctoral Researcher — Jun. 2021 – May 2024

PRODIGY: Ensuring the Security, Scalability and Correctness of Digital Provenance Systems | Project: TED2021/132464B-I00, Spanish Research Agency (AEI).
BLOQUES: Scalable and Secure Smart Contracts and Blockchains through Verification and Analysis | Project: S2018/TCS-4339, Community of Madrid.

EURECOM — Sophia Antipolis, France
Doctoral Researcher at Digital Security Department — Mar. 2015 – Jul. 2019

TREDISEC: Trust-Aware, Reliable and Distributed Information Security in the Cloud | Project: H2020-ICT, EU.

- Protocol design on verifiable storage with secure deduplication and data reliability.
- Technical project management and reporting: Deliverables author.

SecludIT — Valbonne, France
Security Engineer (M.Sc. Internship) — Jul. 2013 – Jan. 2014

Internship Project: "Security Audit in Cloud Infrastructures."

- Studied the best practices for deploying and configuring the SSH and TLS protocols.
- Extended the Lynis audit tool to detect misconfigurations on OpenSSH, Postfix MTA, and Apache HTTP server.
Advisors: Professor Refik Molva, Sergio Loureiro

IT Support | Teaching Computer Skills — Athens, Greece
Freelancer — Jan. 2011 – Jul. 2012

- Providing technical support for small businesses and home users.
- Teaching basic computer skills to adults. Preparing students for the ECDL certification exam.

TEACHING EXPERIENCE

Teaching Assistant at Complutense University's *M.Sc.* in Formal Methods in Computer Science program.

- *Design and Analysis of Security Protocols* (Dario Fiore, Ignacio Cascudo, Pedro Moreno-Sanchez) — Fall 2022, 2023
I independently prepared, and delivered three course lectures on Hash Functions and Message Authentication Codes.

Teaching Assistant at EURECOM's *M.Eng.*, *M.Sc.*, and *Post Master's degree* programs.

- *Secure Communications* (Refik Molva, Melek Önen) Fall 2015 – 2019
  I instructed the lab sessions on RSA Encryption, RSA Signatures, and Public Key Infrastructure.
- *Security and Privacy for Big Data and Cloud* (Melek Önen) Fall 2018
- *Security Applications in Networking and Distributed Systems* (Refik Molva) Spring 2015 – 2018
  I designed, developed, and instructed the lab on Firewalls, and also instructed the lab session on IPSEC and Virtual Private Networks.

STUDENT ADVISING

- Diego Castejon-Molina (IMDEA | Technical University of Madrid) | *Ph.D.* candidate: Oct. 2021 – Present
  "Cryptographic Protocols for Secure and Privacy-preserving Payments in a Digital Economy."
- Javier Gomez Martinez (IMDEA | Complutense University of Madrid) | *M.Sc.* internship: Feb. 2023 – Jul. 2023
  "Algebraic Contingent Payments and Applications."
- Alberto del Amo Pastelero (IMDEA | Technical University of Madrid) | *M.Sc.* internship: Feb. 2023 – Jul. 2023
  "Cryptographic Protocols for Interoperability of Payment Channels."
- Ana-Marija Eres (IMDEA | University of Zagreb) | *M.Sc.* internship: Nov. 2021 – May 2022
  "Analysis of the Impact of Collateral Funds in Payment Channel Networks."
- Cedric Osornio-Gleanson (EURECOM) | *M.Eng.* semester project: Spring 2018
  "Advanced Proofs of Data Reliability."
- Ahmed Souissi, Azim Hamadi (EURECOM) | *M.Eng.* semester project: Fall 2017
  "Locally Recoverable Codes for Proofs of Data Reliability."
- Arsham Aryaman, Meru Prabhat (EURECOM) | *M.Eng.* semester project: Fall 2017
  "Firewall Laboratory."
- Hamdi Ammar (EURECOM) | *M.Eng.* semester project: Spring 2017
  "Proofs of Data Reliability."
- Linxia Gong, Yiyi Zhang (EURECOM) | *M.Eng.* semester project: Fall 2016
  "Secure Deduplication."
- Duc Trinh (EURECOM) | *M.Eng.* internship: Jul. 2016 – Feb. 2017
  "Proofs of Retrievability with Secure Deduplication."

TALKS

Talks at International Conferences:

- *SECRYPT '19*, Prague, Czech Republic. Jul. 2019
  "PORTOS: Proof of Data Reliability for Real-World Distributed Outsourced Storage."
- *ACM ASIACCS-SCC '18*, Incheon, Republic of Korea. Jun. 2018
  "POROS: Proof of Data Reliability for Outsourced Storage."
- *ACM CCS-CCSW '16*, Vienna, Austria. Oct. 2016
  "Message-Locked Proofs of Retrievability with Secure Deduplication."

Invited Talks:

- The Lightning Network developers: Discreet Log Contracts (DLC) specification working group, (Virtual). Jun. 2022
  "Practical Decentralized Oracle Contracts."
- Technical University of Crete, Department of Electronic and Computing Engineering, Chania, Greece. Sep. 2017
  "Privacy and Integrity Mechanisms for Cloud Storage."

ACADEMIC SERVICE

Participation in Program Committees:

- Applied Cryptography and Network Security *(ACNS)* 2024
- Workshop on Cryptocurrencies and Blockchain Technology *(CBT)* 2022 – 2024
- *Tokenomics* 2022, 2023
- *ESORICS* Poster Program 2022

Reviewer for International Journals:
Journal of Parallel and Distributed Computing, IEEE Transactions on Dependable and Secure Computing, Journal of Cloud Computing, International Journal of Information Security, IEEE Transactions on Information Forensics & Security.

External Reviewer for International Conferences:
Usenix (2023), SECRYPT (2023, 2017, 2016), CFS (2023), NDSS (2022), FC (2022), AFT (2022), IFIP SEC (2022, 2017), PST (2019), ACNS (2018), IEEE CNS (2018), ACM CCS (2017), ESORICS (2017), CANS (2017, 2016), ICDS (2016), ISC (2016), DPM (2015).

LANGUAGE SKILLS

English (Full professional proficiency), **French** (Fluent), **Greek** (Native speaker).