# Stefanos Chaliasos

✉ stefanos@chaliasos.com | 🏠 stefanoschaliasos.github.io | StefanosChaliasos

## Research Interests

My main research interests involve Computer Security, Blockchain, Software Engineering, Programming Languages, Software Testing, and Zero Knowledge Proofs.

## Education

**Ph.D. in Computing Research** — *London, UK*

Imperial College London — *2021 - 2025 (expected)*

- Ph.D. Thesis: *"Security and Adoption of Zero-Knowledge Proofs"*
- Academic Advisors: Ben Livshits, Alaister Donaldson

**M.Sc. in Computer Science (GPA 9.57/10)** — *Athens, Greece*

National and Kapodistrian University of Athens — *2019 - 2021*

- M.Sc. Thesis: *"A Study of Typing-Related Bugs in JVM Compilers"*
- Academic Advisors: Alex Delix, Dimitris Mitropoulos

**B.S. in Management Science and Technology – Major: Software Engineering and Data Science (GPA 7.8/10)** — *Athens, Greece*

Athens University of Economics and Business (AUEB) — *2014 - 2019*

- B.S. Thesis: "Mix network implementations in e-voting system"
- Thesis Advisor: Panagiotis Louridas

## Professional Appointments

**zkSecurity** — *Remote*

Security Researcher — *April 2024 - Today*

As a Security Researcher at zkSecurity, I am responsible for conducting in-depth security audits on advanced protocols leveraging Zero-Knowledge Proofs (ZKPs), Multi-Party Computation (MPC), and Fully Homomorphic Encryption (FHE). My role includes leading a focused research team to develop innovative techniques for protocol security and vulnerability detection. My research focuses on bug finding, software testing, formal verification, and mechanism design for ZKPs.

**Matter Labs** — *Remote*

Research Scientist — *August 2023 - November 2023*

As a Research Scientist working in Blockchain Migration, I conducted in–depth research to understand the complexities involved in the migration from Ethereum (EVM-Based) blockchains to the zkSync Era blockchain. My role included developing specialized tooling to ensure the seamless functionality of top Decentralized Applications within the zkSync Era ecosystem, as well as analyzing and documenting the benefits of EVM–compatibility and EVM-equivalence, thereby contributing to an enhanced understanding of their implications in blockchain technology and migration strategies.

**Veridise** — *Remote (Part time)*

R&D Engineer — *January 2023 - August 2023*

Working on developping a fuzzer for ZK circuits combyining dynamic analysis with SMT solvers and static analysis.

**Veridise** — *Remote*

R&D Engineer — *September 2022 - December 2022*

Doing research/developping tools to secure ZK applications and Scroll's zkEVM.

**Athens University of Economics and Business (AUEB) – BALAB** *Athens, Greece*

RESEARCHER *March 2019 - October 2021*

Research scientist for the FASTEN European Research Project. I have been working on generating C call graphs for the whole Debian ecosystem using static analysis techniques and providing a framework to enable various analyses to tackle security and risk evaluation problems, license compliance, and change impact analysis. I have also taken part in other research projects in web security, programming languages, and software testing.

**GRNET** *Athens, Greece*

SOFTWARE ENGINEER *February 2018 - February 2019*

Software engineer for the PANORAMIX European Research Project. During my time at GRNET, I worked on making an e-voting platform, namely Zeus, modular regarding its cryptosystem. Specifically, I refactored the code base of the platform to support multiple cryptosystems. I also integrated two different mix nets into the platform.

## Service

### PROGRAM COMMITTEE

**CCS** ACM Conference on Computer and Communications Security: 2025
**FC** Financial Cryptography: 2024, 2025
**ISSTA/ECOOP (Tool Demos)** ISSTA/ECOOP (Tool Demos): 2024
**ACM DeFi** ACM CCS Workshop on Decentralized Finance and Security : 2023, 2024
**USENIX Security Artifacts** USENIX Security – Artifacts: 2023
**ECOOP Extended Review Committee** European Conference on Object-Oriented Programming – Extended Review Committee: 2023
**POPL Artifacts** Principles of Programming Languages – Artifacts: 2023
**OOPSLA Artifacts** Object-oriented Programming, Systems, Languages, and Applications – Artifacts: 2021
**PLDI Artifacts** Programming Language Design and Implementation – Artifacts: 2022, 2023
**OSDI Artifacts** USENIX Symposium on Operating Systems Design and Implementation – Artifacts: 2022
**ATC Artifacts** USENIX Annual Technical Conference – Artifacts: 2022

### EXTERNAL REVIEWER

CCS, NDSS, S&P, Usenix Security, FC, SBC, CESC

## Teaching

**Teaching Assistant** *London, UK*

IMPERIAL COLLEGE LONDON *Spring 2022 - Spring 2024*

- Spring 2024: Teaching Assistant (TA) for Advanced Computer Security (Graduate level. Instr. Ben Livshits)
- Spring 2023: Teaching Assistant (TA) for Advanced Computer Security (Graduate level. Instr. Ben Livshits)
- Spring 2022: Teaching Assistant (TA) for Principles of Distributed Ledgers (Graduate level. Instr. Arthur Gervais)
- Spring 2022: Teaching Assistant (TA) for Decentralised Finance (Graduate level. Instr. Arthur Gervais)

**Teaching Assistant** *Athens, Greece*

NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS *Spring 2018 and Spring 2021*

- Spring 2018: Lead Teaching Assistant (TA) for Computer Security (Undergraduate and Graduate level. Instr. Dimitris Mitropoulos. Students: 90)
- Spring 2021: Teaching Assistant (TA) for Systems Programming (Undergraduate level. Instr. Mema Roussopoulos. Students: 240)

**Teaching Assistant** *Athens, Greece*

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS *Fall 2017 - Spring 2020*

- Fall 2017-2018-2019: Lead Teaching Assistant (TA) for Introduction to Computer Science (Undergraduate level. Instr. Dimitris Mitropoulos. Students: 180)
- Spring 2018-2019-2020: Lead Teaching Assistant (TA) for Computer Security (Undergraduate level. Instr. Dimitris Mitropoulos. Students: 20)

## Awards

| | | |
|---|---|---|
| 2022 | **PLDI 22 Best Artifact Award**, Finding Typing Compiler Bugs | *San Diego, USA* |
| 2022 | **PLDI 22 Distinguished Paper Award**, Finding Typing Compiler Bugs | *San Diego, USA* |
| 2021 | **ICSE 21 Best Artifact Award**, Replication Package for Article: Data-Oriented Differential Testing of Object-Relational Mapping Systems | *Madrid, Spain* |

## Grants & Scholarships

| | | |
|---|---|---|
| 2024 | **Ethereum Foundation Research Grant**, Reproducible ZK Vulnerabilities to Improve Ecosystem's Security | |
| 2024 | **Ethereum Foundation Research Grant**, Detecting Private Information Leakage in Zero-Knowledge Applications | |
| 2024-2025 | **The Latest in DeFi Research Fellowship**, Identifying ZKP Pricing Factors & Auction Mechanisms | |
| 2023 | **Ethereum Foundation Research Grant**, Understanding and Analyzing the Metering Mechanism of zkEVMs | |
| 2023 | **Ethereum Foundation Research Grant**, zk-Harness: Benchmarking ZKPs | |
| 2021-2025 | **Imperial College London**, Doctoral Scholarship Award | *London, UK* |

## Publications

### Publications

P1 **Stefanos Chaliasos**, Jens Ernstberger, David Theodore, David Wong, Mohammad Jahanara, and Benjamin Livshits *"SoK: What don't we know? Understanding Security Vulnerabilities in SNARKs"*. In USENIX Security, USENIX Security '24. USENIX, August 2024.

P2 **Stefanos Chaliasos**, Itamar Reif, Adria Torralba-Agel, Jens Ernstberger, Assimakis Kattis, and Benjamin Livshits *"Analyzing and Benchmarking ZK-Rollups"*. In 6th Advances in Financial Technologies, AFT 2024.

P3 Jens Ernstberger, **Stefanos Chaliasos**, Liyi Zhou, Philipp Jovanovic, and Arthur Gervais *"Do You Need a Zero Knowledge Proof?"*. CfC St. Moritz Academic Research Track 2024.

P4 Jens Ernstberger, **Stefanos Chaliasos**, George Kadianakis, Sebastian Steinhorst, Philipp Jovanovic, Arthur Gervais, Benjamin Livshits, Michele Orru *"zk-Bench: A Toolset for Comparative Evaluation and Performance Benchmarking of SNARKs"*. In 14th International Conference on Security and Cryptography for Networks, SCN 2024.

P5 Thodoris Sotiropoulos, **Stefanos Chaliasos**, and Zhendong Su *" API-driven Program Synthesis for Testing Static Typing Implementations"*. In 51st ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2024). 2024.

P6 **Stefanos Chaliasos**, Marcos Antonios Charalambous, Liyi Zhou, Rafaila Galanopoulou, Arthur Gervais, Dimitris Mitropoulos, and Ben Livshits *"Smart Contract and DeFi Security: Insights from Tool Evaluations and Practitioner Surveys"*. In 46rd International Conference on Software Engineering, ICSE '24. 2024.

P7 Kaihua Qin, **Stefanos Chaliasos**, Liyi Zhou, Benjamin Livshits, Dawn Song, and Arthur Gervais *"The Blockchain Imitation Game"*. In USENIX Security, USENIX Security '23. USENIX, August 2023.

P8 Liyi Zhou, Xihan Xiong, Jens Ernstberger, **Stefanos Chaliasos**, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. *"SoK: Decentralized Finance (DeFi) Attacks"*. In Symposium on Security and Privacy, S&P '23. IEEE, May 2023.

P9 Zhipeng Wang, **Stefanos Chaliasos**, Kaihua Qin, Liyi Zhou, Lifeng Gao, Pascal Berrang, Ben Livshits, and Arthur Gervais. *"On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy"*. In International World Wide Web Conference, WWW '23. IW3C2, May 2023.

P10 **Stefanos Chaliasos**, Arthur Gervais, and Ben Livshits. *"A Study of Inline Assembly in Solidity Smart Contracts"*. In Proceedings of the ACM on Programming Languages, OOPSLA '22. ACM, December 2022.

P11 **Stefanos Chaliasos**, Thodoris Sotiropoulos, Diomidis Spinellis, Arthur Gervais, Ben Livshits, and Dimitris Mitropoulos. *"Finding Typing Compiler Bugs"*. In Proceedings of the 43rd ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2022).

P12 **Stefanos Chaliasos**, Thodoris Sotiropoulos, Giorgos-Petros Drossos, Charalampos Mitropoulos, Dimitris Mitropoulos, and Diomidis Spinellis. *“Well-Typed Programs Can Go Wrong: A Study of Typing-Related Bugs in JVM Compilers”*. In Proceedings of the ACM on Programming Languages, OOPSLA ’21. ACM, October 2021.

P13 Thodoris Sotiropoulos, **Stefanos Chaliasos**, Vaggelis Atlidakis, Dimitris Mitropoulos, and Diomidis Spinellis. *“Data-oriented differential testing of object-relational mapping systems.”*. In 43rd International Conference on Software Engineering, ICSE ’21. 2021.

P14 Thodoris Sotiropoulos, **Stefanos Chaliasos**, Dimitris Mitropoulos, and Diomidis Spinellis. *“A model for detecting faults in build specifications.”*. In Proceedings of the ACM on Programming Languages, OOPSLA ’20. ACM, November 2020.

P15 **Stefanos Chaliasos**, George Metaxopoulos, George Argyros, and Dimitris Mitropoulos. *“Mime artist: bypassing whitelisting for the web with JavaScript mimicry attacks.”*. In 24th European Symposium on Research in Computer Security, ESORICS ’19, 565–585. September 2019.