# Denis Mazzucato

*Researcher in Formal Verification & Security*

✉ *denismazzucato@outlook.com*
🌐 *denismazzucato.github.io*
in *denis-mazzucato*

## Education

March 2025
October 2024

**Postdoc**, *Carnegie Mellon University*, Pittsburgh (US), supervised by Corina Pasareanu
*"Proving the Absence of Timing Side Channels in Cryptographic Applications."*

- Verification of the absence of timing side channels in the *s2n-bignum* library via HOL Light theorem prover.
- Developed a static analysis tool to detect Hertzbleed side-channel attacks (timing vulnerabilities through frequency scaling) on post-quantum cryptographic algorithms.

December 2024
October 2020

**Ph.D.**, *École Normale Supérieure | PSL & INRIA*, Paris (FR), supervised by Caterina Urban
*"Static Analysis by Abstract Interpretation of Quantitative Program Properties."*

- Research in program verification by abstract interpretation for quantitative properties.
- Developed the TimeSec tool for certifying cryptographic applications against timing side-channel attacks.

September 2020
October 2015

**Master and Bachelor**, *University of Padua*, Padua (IT), magna cum laude 110/110
Computer Science, Dipartimento di Matematica, Università degli Studi di Padova.

## Professional Experience

2022
6 months

**Applied Scientist Intern–Automated Reasoning Team**, Amazon Prime Video, London (UK)

- Developed a static analysis tool for backwards reasoning on TypeScript code within promise chains, leveraging TaJS, Z3, and Datalog to enable local reasoning around code assertions.
- Collaborated in a customer-driven environment to ensure production needs and security best practices; under the supervision of Franco Raimondi and Bor-Yuh Evan Chang.

2018
6 months

**Quality Assurance Developer**, *THRON*, Padua (IT)

- Developed automated testing frameworks for the THRON document management system.
- Engineered a serverless architecture for real-time probe monitoring, deploying the solution on AWS Lambda.

## Core Competencies

Verification — Expertise in abstract interpretation, SMT solvers, and theorem provers (such as Lean).

Languages — Experienced in Python and Haskell; familiar with Go, OCaml, C, C++, JavaScript, Scala, and Solidity.

Tooling — Proficient with Git, GitHub, CI/CD, and knowledge of AWS cloud computing platforms and web3.

Research — Award-winning research and top conference publications in formal methods and security.

## Awards & Recognitions

October 2024

**Radhia Cousot Award**, for *Young Researcher*, SAS 2024, Pasadena (USA), 3 000€ prize from the ENS foundation for my publication: "Quantitative Static Timing Analysis."

Spring 2024

**Automated Reasoning Amazon Research Award (ARA)**, *Funding Award*, Amazon, 70 000€ prize
"Proving the Absence of Timing Side Channels in Cryptographic Applications" with Corina Pasareanu.

## Additional Experience, Projects, & Selected Publications

CAV 2025
First-authored publication
ICORE: A*

**Relational Hoare Logic for Realistically Modelled Machine Code**, in collaboration with *Carnegie Mellon University, NASA Ames Research Center, Stanford University, AWS Amazon*
Exploring relational Hoare logic for verifying security properties, such as the absence of timing side channels, in the s2n-bignum library of AWS within cryptographic TLS/SSL implementations.

SAS 2024
First-authored publication

**Quantitative Static Timing Analysis**, *with Marco Campion and Caterina Urban*, ENS & INRIA
A sound static analysis framework based on abstract interpretation for quantifying timing side-channel vulnerabilities in cryptographic applications.

2023
2 weeks

**Summer School on Formal Methods**, Marktoberdorf (DE)
Deepened expertise in the scientific foundations and technologies for improving software quality and security.

2020
6 months

**Exchange Program**, *Vrije Universiteit*, Amsterdam (NL)
Advanced training in Lean and formal methods under the supervision of Jasmin Blanchette.

2019
1 year

**Marvin–University Managment System**, *University of Padua (IT)*
Developed the architecture of a web application in Solidity on the Ethereum blockchain, and the web3 interface from the React-Redux front-end.