# Denis Mazzucato Ph.D.

*Compiler Engineer @ AdaCore*

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

## Current Position

MAY 2025 — **Compiler Engineer**, AdaCore, Paris (FR)
Working on the GNAT Ada compiler integrated into the GCC compiler system (more than 11 million loc).

## Education

APRIL 2025 – OCTOBER 2024 — **Postdoc**, *Carnegie Mellon University & NASA*, 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 Assembly *s2n-bignum* library with HOL Light.
- Developed a program 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
*"Program Analysis by Abstract Interpretation of Quantitative Program Properties."*

- Research in program verification by abstract interpretation for quantitative properties.
- Customized the `interproc` OCaml static analyzer to support a quantitative analysis of C programs.
- Developed the TimeSec tool for certifying cryptographic applications against timing side-channel attacks, combining a syntactical dependency analysis with a semantics-based abstraction.

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 program 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.

2018, 6 MONTHS — **Quality Assurance Intern**, *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

| | |
|---|---|
| PASSION | Strong curiosity for new programming languages, and the compilation trade. |
| LANGUAGES | Fluent in Ada, Python and Haskell; familiar with C, C++, Go, Rust, OCaml, JavaScript, and Scala. |
| TOOLING | Proficient with Git, GitHub, CI/CD pipelines, GDB debugger, and AWS infrastructure. |
| 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.

## Selected Projects & 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 in HOL Light (based in OCaml) for verifying security properties, such as the absence of timing side channels, in the Assembly *s2n-bignum* library within AWS TLS/SSL implementations.

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 Prof. Jasmin Blanchette.