Zacharie Moughanim

zacharie[dot]moughanim[at]ens-rennes.fr | github.com/zacharie-moughanim | perso.eleves.ens-rennes.fr/people/zacharie.moughanim

Education

Université Paris-Cité 2026 — 2027 (expected)
Master Parisien de Recherche en Informatique *(Parisian Master of Computer Science Research), courses: Functional programming, Proofs of security protocols, Algorithmic aspects of well quasi-orders, Proof assistants, Linear logic, Foundations of proof systems, Models of programming languages (more to come in second semester)* *Paris, France*

École Normale Supérieure de Rennes - Université de Rennes 2025 — 2026
Master in Computer Science's Teaching, highest honour - Prepared the Agrégation d'Informatique*, a recruitment exam for computer science teachers, ranked 1st.* *Rennes, France*

École Normale Supérieure de Rennes - Université de Rennes 2023 — 2024
License, dual curriculum Computer Science/Mathematics, highest honour. *Rennes, France*

Lycée Louis-le-Grand 2021 — 2023
CPGE (Classes Préparatoires aux Grandes Écoles) *MP2I/MPI*.* *Paris, France*

Lycée Jean Lurçat 2021
Baccalauréat général, Mathematics and Computer science, highest honour. *Martigues, France*

Work Experience

Research Internship supervised by David Baelde and Stéphanie Delaune, SPICY team Summer 2026
Searched several algorithms and undecidability results for bideduction – a notion useful in cryptography, in particular to encode game reductions – in the symbolic cryptographic model. *Rennes, France*

Research Internship supervised by Lars Birkedal and Philipp G. Haselwarter, Århus University Summer 2025
Cryptographic proofs in Approxis. Wrote cryptographic proofs in Rocq, within the relational separation logic Approxis, allowing to prove approximate equivalences between probabilistic programs. Implemented new cryptographic games, and proved cryptographic systems. *Århus, Denmark*

Research Project supervised by Stéphanie Delaune, Joseph Lallemand and Clément Hérouard, SPICY team2024 – 2025
Type system for automated proof of cryptographic protocols. Extended the existing type system to signature primitives. Generalized the type system to take into account more cryptographic systems, which is a stepping stone toward adding refinement types. *Rennes, France*

Research Internship supervised by Lionel Vaux Auclair, *Logique de la Programmation* team Summer 2024
Studied a new variant of the algebraic λ-calculus and proved properties on this new formalism: confluence, normalizability via intersection type systems, conservativity of the Taylor expansion (JFLA 2025 paper). *Marseille, France*

Popularization in elementary school Rennes, France January 2024 – May 2024
Unplugged computer science activities as part of the *Pédagogie* course. Designed a new activity introducing graph coloring to pupils. *Rennes, France*

Mathematics Popularization 2019 & 2020
Stand at the *Forum des Mathématiques de Marseille*, about mathematics behind Blender: Bézier curve for interpolation of translations, projection of templates on 3D objects. *Marseille, France*

Projects

VSquirrel (https://https://github.com/zacharie-moughanim/vsquirrel) 2026 –
A Vscode/ium extension for the Squirrel Proof assistant, a proof assistant for cryptographic protocols.

VSUnicodex (https://https://github.com/zacharie-moughanim/vsunicodexinput) 2026 –
A Vscode/ium extension to input unicode symbols using Typst's extensive symbol name list

TresML (https://github.com/Ilianmgh/tresfreroserver) 2025 –
A functional language for server-side dynamic webpages.

λMLC2 (https://github.com/zacharie-moughanim/LMLC2) 2024 –
A project of verified transpiler (in Coq/Rocq) from a subset of OCaml to the untyped λ-calculus.

TIPE (https://perso.eleves.ens-rennes.fr/people/zacharie.moughanim/TIPE_ENS.pdf) 2021 – 2023
Personal projects as part of the CPGE curriculum, lead to the publication of a sequence to the OEIS.

Extracurricular Activities

Cinema Jan 2021 — Present

- Film analysis courses during the academic year 2024-2025 at the *Université de Rennes 2*.
- Video editing and 3D animation on Blender as a hobby.

Skills

Natural languages

French, Native
English certificate, C1, TOEIC 2025

Programming

OCaml, Python, Rust, Java/TypeScript, C, C++, Java, Typst, Latex