

Jason Gross

github.com/JasonGross
people.csail.mit.edu/jgross

CONTACT
jgross@mit.edu
(631) 790-8962

RESEARCH INTERESTS

Programming Languages, Formal Verification, Cryptography, Performance of Automation in Interactive Proof Assistants, Homotopy Type Theory, Category Theory, Program Synthesis

EDUCATION

Massachusetts Institute of Technology 2013–2021
PhD in Computer Science Cambridge, MA
Advisor: Adam Chlipala
Thesis: Performance Engineering of Proof-Based Software Systems at Scale
SM Thesis: An Extensible Framework for Synthesizing Efficient, Verified Parsers

Massachusetts Institute of Technology 2009–2013
BS in Mathematics and Physics Cambridge, MA
GPA: 4.6/5

EXPERIENCE

Coq Development Team, INRIA June 2021–Present
Core Team Member Nantes, France (remote)

- Stress Testing, Bug Reporting, Bug Minimizer, Compatibility Assurance
- Engineering and maintaining a bug minimizer for automatically producing minimized stand-alone test-cases from buggy code
- Researching performance issues that impact scalability of automated verification
- Have reported the plurality of all-time bugs in Coq (since 2012)

Machine Intelligence Research Institute February 2021–Present
Research Staff Berkeley, CA (remote)

- Performing self-directed research into topics in fundamental programming language theory and mathematics

MIT CSAIL September 2013–February 2021
PhD Researcher Cambridge, MA

- Main Research Project: Fiat Cryptography (github.com/mit-plv/fiat-crypto)
- Collaboratively implemented proven-correct cryptographic code now used by Google Chrome, and in the majority of secure connects from web browsers
- Led development of one of the world's first algorithm-level-optimizing compilers
- Wrote backends to C, Go, Java, and JSON; managed development of backends to Rust and Zig

INTERNSHIPS

Machine Intelligence Research Institute June 2019–August 2019
Type Theory Intern Berkeley, CA

- Worked on formalizing type theories and on proving things within proof assistants

Google June 2018–August 2018
Software Engineering Intern Cambridge, MA

- Worked with BoringSSL on integration of proven-correct low-level ECC primitives into Chrome

Google June 2016–September 2016
Software Engineering Intern Mountain View, CA

- Formalized low-level ECC primitives with proofs of correctness

MIT Fall 2009–Present
Teacher Cambridge, MA

- Taught classes on L^AT_EX, philosophy, linear algebra, and quantum mechanics for MIT Educational Studies Program’s Splash, Spark, and Summer HSSP (High School Studies Program)
- Teaching Assistant for 8.012 (Physics I) and 8.022 (Physics II) in Experimental Study Group

Microsoft Research June 2014–August 2014
Intern Cambridge, United Kingdom

- Collaboratively created a language for specifying input/output behavior of x86 assembly programs; Verified the I/O behavior of a number of simple programs
- Improved automation of the x86proved library

MIT CSAIL April 2012–June 2014
Researcher Cambridge, MA

- Entered a significant amount of category theory into the automated proof assistant Coq (<https://github.com/HoTT/HoTT/tree/master/theories/Categories>)
- Made progress towards an interface for databases and database migration on top of category theory in Coq

MIT CSAIL November 2009–September 2011
Researcher Cambridge, MA

- Designed from scratch a data collection webpage, collected data for, and helped with research on categorical and transfer learning

Commack High School Fall 2006–Summer 2009
Independent Researcher Commack, NY

- Independently researched circuits over sets of natural numbers for three years.
- Won fourth place award in mathematics in ISEF (Intel International Science and Engineering Fair) in 2009, third place award in ISEF 2008.

COMPUTER SKILLS

- Proficient: Coq, Mathematica, git, Python, JavaScript, BASIC
- Working knowledge: C, C++, Agda, OCaml, Haskell, Scheme, HTML, CSS, Perl, Java
- Basic knowledge: Matlab, Lean, Idris, Ruby, Go, Ur/Web, x86 Assembly

TEACHING

- Instructor at Monsoon Math Camp: category theory, linear logic, Löb’s theorem
- TA for 6.172 (Performance Engineering): Led recitations, analyzed and explained assembly output of `gcc -O3` to teach vectorization
- TA for 8.012 (Physics I) and 8.022 (Physics II) in Experimental Study Group
- Teacher at MIT ESP Programs: L^AT_EX, philosophy, linear algebra, quantum mechanics

OTHER ACTIVITIES

- Co-maintainer of the Fiat Cryptography project (`mit-plv/fiat-crypto` on GitHub)

- Co-maintainer of the homotopy type theory Coq repository (HoTT/HoTT on GitHub)
- Program Committee Member of ITP 2023 and CoqPL 2022
- Committer to the SIPB BarnOwl project (<https://barnowl.mit.edu>)
- SIPB (Student Information and Processing Board) Member
- President of Tech Squares, MIT's Square Dancing Club (May 2013–October 2014)
- Canada/USA Mathcamp (Summers 2006–2009)

SELECTED PRESENTATIONS AND PUBLICATIONS

- [Gro+23] Jason Gross, Andres Erbsen, Jade Philipoom, Rajashree Agrawal, and Adam Chlipala. *Towards a Scalable Proof Engine: A Performant Prototype Rewriting Primitive for Coq*. 2023. arXiv: 2305.02521 [cs.PL].
- [Kue+23] Joel Kuepper, Andres Erbsen, Jason Gross, Owen Conoly, Chuyue Sun, Samuel Tian, David Wu, Adam Chlipala, Chitchanok Chuengsatiansup, Daniel Genkin, Markus Wagner, and Yuval Yarom. “CryptOpt: Verified Compilation with Random Program Search for Cryptographic Primitives”. In: *PLDI’23: Proceedings of the 44th ACM SIGPLAN Conference on Programming Language Design and Implementation*. Distinguished Paper Award. Orlando, FL, USA, June 2023. URL: <http://adam.chlipala.net/papers/CryptoptPLDI23/>.
- [GE22] Jason Gross and Andres Erbsen. *10 Years of Superlinear Slowness in Coq*. Presented at The Coq Workshop 2022. Aug. 2022. URL: <https://jasongross.github.io/papers/2022-superlinear-slowness-coq-workshop.pdf>.
- [Gro+22a] Jason Gross, Andres Erbsen, Jade Philipoom, Miraya Poddar-Agrawal, and Adam Chlipala. “Accelerating Verified-Compiler Development with a Verified Rewriting Engine”. In: *Proceedings of the 13th International Conference on Interactive Theorem Proving (ITP 2022)*. Ed. by June Andronick and Leonardo de Moura. Vol. 237. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Aug. 2022, 17:1–17:18. ISBN: 978-3-95977-252-5. DOI: 10.4230/LIPIcs.ITP.2022.17. eprint: 2205.00862. URL: <https://jasongross.github.io/papers/2022-rewriting-ity.pdf>.
- [Gro+22b] Jason Gross, Théo Zimmermann, Miraya Poddar-Agrawal, and Adam Chlipala. “Automatic Test-Case Reduction in Proof Assistants: A Case Study in Coq”. In: *Proceedings of the 13th International Conference on Interactive Theorem Proving (ITP 2022)*. Ed. by June Andronick and Leonardo de Moura. Vol. 237. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Aug. 2022, 18:1–18:18. ISBN: 978-3-95977-252-5. DOI: 10.4230/LIPIcs.ITP.2022.18. URL: <https://jasongross.github.io/papers/2022-coq-bug-minimizer-ity.pdf>.
- [Gro21a] Jason S. Gross. “Performance Engineering of Proof-Based Software Systems at Scale”. PhD Thesis. Massachusetts Institute of Technology, Feb. 2021. URL: <https://jasongross.github.io/papers/2021-JGross-PhD-EECS-Feb2021.pdf>.
- [Gro21b] Jason Gross. *A Limited Case for Reification by Type Inference*. Presented at The Seventh International Workshop on Coq for Programming Languages (CoqPL’21). Jan. 2021. URL: <https://jasongross.github.io/papers/2021-reification-by-type-inference-coqpl.pdf>.
- [Pit+20] Clément Pit–Claudel, Peng Wang, Benjamin Delaware, Jason Gross, and Adam Chlipala. “Extensible Extraction of Efficient Imperative Programs with Foreign Functions, Manually Managed Memory, and Proofs”. In: *Proceedings of the 9th International Joint Conference on Automated Reasoning (IJCAR’20)*. Ed. by Nicolas Peltier and Viorica Sofronie-Stokkermans. Paris, France: Springer International Publishing, June 2020, pp. 119–137. ISBN: 978-3-030-51054-1. DOI: 10.1007/978-3-030-51054-1_7.

- [Erb+19] Andres Erbsen, Jade Philipoom, Jason Gross, Robert Sloan, and Adam Chlipala. “Simple High-Level Code For Cryptographic Arithmetic – With Proofs, Without Compromises”. In: *Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P’19)*. May 2019. DOI: 10.1145/3421473.3421477. URL: <https://jasongross.github.io/papers/2019-fiat-crypto-ieee-sp.pdf>.
- [Gro18] Jason Gross. *Presentation Proposal for Teaching Your Rooster to Crow in C*. Presented at The Coq Workshop 2018. July 2018. URL: <https://jasongross.github.io/presentations/coq-workshop-2018/coq-workshop-proposal-notations.pdf>.
- [GEC18] Jason Gross, Andres Erbsen, and Adam Chlipala. “Reification by Parametricity: Fast Setup for Proof by Reflection, in Two Lines of Ltac”. In: *Proceedings of the 9th International Conference on Interactive Theorem Proving (ITP’18)*. Ed. by Jeremy Avigad and Assia Mahboubi. Cham: Springer International Publishing, July 2018, pp. 289–305. ISBN: 978-3-319-94821-8. DOI: 10.1007/978-3-319-94821-8_17. URL: <https://jasongross.github.io/papers/2018-reification-by-parametricity-ityp-camera-ready.pdf>.
- [Chl+17] Adam Chlipala, Benjamin Delaware, Samuel Duchovni, Jason Gross, Clément Pit-Claudel, Sorawit Suriyakarn, Peng Wang, and Katherine Ye. “The End of History? Using a Proof Assistant to Replace Language Design with Library Design”. In: *Proceedings of the The 2nd Summit on Advances in Programming Languages (SNAPL’17)*. Ed. by Benjamin S. Lerner, Rastislav Bodík, and Shriram Krishnamurthi. Vol. 71. Leibniz International Proceedings in Informatics (LIPIcs). Asilomar, CA, USA: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, May 2017, 3:1–3:15. ISBN: 978-3-95977-032-3. DOI: 10.4230/LIPIcs.SNAPL.2017.3. URL: <https://jasongross.github.io/papers/FiatSNAPL17.pdf>.
- [Bau+17] Andrej Bauer, Jason Gross, Peter LeFanu Lumsdaine, Michael Shulman, Matthieu Sozeau, and Bas Spitters. “The HoTT Library: A Formalization of Homotopy Type Theory in Coq”. In: *Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs. CPP 2017*. Paris, France: ACM, Jan. 2017, pp. 164–172. ISBN: 978-1-4503-4705-1. DOI: 10.1145/3018610.3018615. eprint: 1610.04591. URL: <https://jasongross.github.io/papers/2017-HoTT-formalization.pdf>.
- [Gro16] Jason Gross. *The HoTT/HoTT Library in Coq: Designing for Speed*. Presented at The 5th International Congress on Mathematical Software (ICMS 2016). July 2016. URL: <https://jasongross.github.io/presentations/icms-2016/hott-hott-and-category-coq-experience.pdf>.
- [Gro15a] Jason Gross. “An Extensible Framework for Synthesizing Efficient, Verified Parsers”. MA thesis. Massachusetts Institute of Technology, Sept. 2015. URL: <https://jasongross.github.io/papers/2015-jgross-thesis.pdf>.
- [Del+15] Ben Delaware, Clément Pit-Claudel, Jason Gross, and Adam Chlipala. “Fiat: Deductive Synthesis of Abstract Data Types in a Proof Assistant”. In: *Proceedings of the 42nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL’15)*. Jan. 2015. DOI: 10.1145/2775051.2677006. URL: <https://jasongross.github.io/papers/2015-adt-synthesis.pdf>.
- [Gro15b] Jason Gross. *Coq Bug Minimizer*. Presented at The First International Workshop on Coq for PL (CoqPL’15). Jan. 2015. URL: <https://jasongross.github.io/papers/2015-coq-bug-minimizer.pdf>.
- [TG15] Tobias Tebbi and Jason Gross. *A Profiler for Ltac*. Presented at The First International Workshop on Coq for PL (CoqPL’15). Jan. 2015. URL: <https://jasongross.github.io/papers/2015-ltac-profiler.pdf>.

- [Gro14a] Jason Gross. *Presentation: Input, Output, and Automation in x86 Proved*. Presented at Microsoft Research, Cambridge, UK. Aug. 2014. URL: <https://jasongross.github.io/presentations/msr-2014-final-talk/input-output-and-automation-in-x86proved.pdf>.
- [GCS14] Jason Gross, Adam Chlipala, and David I. Spivak. “Experience Implementing a Performant Category-Theory Library in Coq”. In: *Proceedings of the 5th International Conference on Interactive Theorem Proving (ITP’14)*. Ed. by Gerwin Klein and Ruben Gamboa. Cham: Springer International Publishing, July 2014, pp. 275–291. ISBN: 978-3-319-08970-6. DOI: 10.1007/978-3-319-08970-6_18. eprint: 1401.7694. URL: <https://jasongross.github.io/papers/category-coq-experience-ityp-submission-final.pdf>.
- [Gro14b] Jason Gross. *Presentation Proposal for Three Neat Tricks in Coq 8.5*. Presented at the 6th Coq Workshop. Apr. 2014. URL: <https://jasongross.github.io/presentations/coq-workshop-2014/coq-workshop-proposal-tactics-in-terms.pdf>.
- [Gro14c] Jason Gross. *Jason Gross’ Wishlist for Coq*. Jan. 2014. URL: <https://jasongross.github.io/presentations/coq-8.6-wishlist/jgross-coq-8-6-wishlist-no-pause.pdf>.
- [Gro14d] Jason Gross. *POPL: Minute Madness: Category Theory in Coq, and Program Synthesis*. Presented at the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL’14). Jan. 2014. URL: <https://jasongross.github.io/presentations/popl-2014-minute-madness/jason-gross-minute-madness.pdf>.
- [Gro13a] Jason Gross. *CSAIL Student Workshop 2013: Computational Higher Inductive Types: Computing with Custom Equalities*. Presented at the 2014 MIT CSAIL Student Workshop. Oct. 2013. URL: <https://jasongross.github.io/presentations/csw-2013/jgross-presentation-no-pause.pdf>.
- [Gro13b] Jason Gross. *Building Database Management on top of Category Theory in Coq*. Presented as a student talk at the 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL’13). Jan. 2013. URL: <https://jasongross.github.io/presentations/popl-2013/jgross-student-talk.pdf>.
- [Gro13c] Jason Gross. *POPL: Minute Madness: Database Management on top of Category Theory in Coq: Category of Relational Schemas = Category of Categories*. Presented at the 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL’13). Jan. 2013. URL: <https://jasongross.github.io/presentations/popl-2013/minute-madness.pdf>.
- [Lak+11] Brenden M. Lake, Ruslan Salakhutdinov, Jason Gross, and Joshua B. Tenenbaum. “One shot learning of simple visual concepts”. In: *Proceedings of the 33rd Annual Conference of the Cognitive Science Society*. 2011. URL: <https://jasongross.github.io/papers/LakeEtAl2011CogSci.pdf>.