Katherine Ye

katherineye.com ◇ kqy@cs.cmu.edu ◇ Smith 232 ◇ (732) 599-4732

EDUCATION

Ph.D. in Computer Science, Carnegie Mellon University (2016–?)
A.B. Computer Science, Princeton University (2012–2016)

HONORS

Computing Research Association (CRA) Outstanding Undergraduate Researcher Award	2016
Google Anita Borg Scholarship (1 of 30 in North America)	2016
ARCS Fellowship (1 of 2 first-years in the CS department)	2016
Honorable mention, NSF Graduate Research Fellowship	2016
Invited to attend High Assurance Crypto Software Workshop (at Real World Crypto)	2015
Outstanding Work Award, Princeton Creative Writing Program	2014

PAPERS

The end of history? Using a proof assistant to replace language design with library design
Adam Chlipala, Benjamin Delaware, Samuel Duchovni, Jason Gross, Clément Pit-Claudel, Sorawit Suriyakarn, Peng Wang and Katherine Ye (alphabetical).
In *SNAPL (The Summit on Advances in Programming Languages) '17.*

Verified correctness and security of OpenSSL HMAC
Lennart Beringer, Adam Petcher, Katherine Ye, and Andrew Appel.
In *USENIX Security '15.*

OTHER PUBLICATIONS

Designing extensible, domain-specific languages for mathematical diagrams
Katherine Ye, Keenan Crane, Jonathan Aldrich, and Joshua Sunshine.
Proposal for current work appearing in *Off the Beaten Track '17.*

The Notorious PRG: Formal verification of the HMAC-DRBG pseudorandom number generator
Katherine Ye, advised by Andrew Appel and Matt Green.
Senior thesis; paper in progress.

TALKS

Proof assistants as a tool for thought
Talk at the Tools for Thought workshop, hosted by the Recurse Center. 2016

Strange loops: powerful knot notations See website
Industry conference talk on insights encoded in Conway's knot notation.
Reviewed by Prof. Philip Wadler: "In my series of favourites from Strange Loop 2015... Great fun for anyone interested in how to describe complex situations, and which programming language aficionado can resist that?"

One weird type (inductive types in Coq) See website
Industry conference talk on good representations as a tool for thought. Lambda Jam, 2014

Proofs about programs, proofs as programs, programs as proofs! See website
Lightning talk on proving code "equal" in Coq. !!con, 2014

RESEARCH

Formally proving security of pseudorandom number generators Senior thesis
Advisors: Prof. Andrew Appel (Princeton) and Prof. Matt Green (Johns Hopkins)
Writing computer-checked proofs of security properties of AES-DRBG, a widely-used but unformalized PRNG, in the Foundational Cryptography Framework, embedded in the Coq proof assistant.

Automated synthesis of secure DNS servers in Fiat Summer 2015
Advisor: Prof. Adam Chlipala (MIT)

Wrote Coq tactic to do proof search that turned a manual, 200-line proof into a one-line automated proof, successfully synthesizing an authoritative DNS server. Wrote a formal specification for a recursive caching server, which helped discover new opportunities for synthesis.

Testing typed functional programs and re-synthesizing them Spring 2015
Advisor: Prof. David Walker (Princeton)
Developed novel algorithm for symbolic execution of typed functional programs and extended it to re-synthesize programs in a synthesis system.

Formally proving equivalence between HMAC specifications Fall 2014
Advisor: Prof. Andrew W. Appel (Princeton)
Linked an abstract and a concrete spec, allowing security properties to hold on an implementation. Proofs were added to the Verified Software Toolchain codebase and helped complete a paper that was accepted to *USENIX Security* '15 (see below).

EXPERIENCE

Software Engineering Intern Summer 2014
Facebook, Search Team
- ◇ Visualized pairwise correlations between features in Facebook's machine learning models
- ◇ Derived algorithm to calculate the matrix incrementally in backend; implemented querying interface in frontend
- ◇ Found unexpected correlations between features in important Facebook search verticals

Recurser Summer 2013
The Recurse Center
- ◇ A three-month, full-time "writers' retreat for programmers"
- ◇ Learned Haskell; wrote a tic-tac-toe client, a tic-tac-toe AI, and a graphical game in Haskell

SERVICE

CMU REU Program in Software Engineering, Admissions Committee 2017
SCS Dean's PhD Student Advisory Council 2017

Founder and Co-President Oct. 2013–May 2015
Open Source at Princeton
- ◇ Founded an organization to increase the visibility of free and open source software on campus, as well as the diversity of open source contributors
- ◇ Led a mentorship program to help student developers contribute to OpenMRS, an open source electronic medical record platform, and Ubuntu
- ◇ Students' pull requests have been merged in projects such as Drupal, OpenMRS, & Ubuntu

PRESS

Princeton.edu, *Ambitious vision for computer science drives Princeton senior Ye's research success* (2016)