

# Katherine Ye

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

- EDUCATION**
- Ph.D. in Computer Science, Carnegie Mellon University**  
Advised by Keenan Crane and Jonathan Aldrich.
- A.B. in Computer Science, Princeton University (2012–2016)**  
Worked with Andrew W. Appel, Adam Chlipala, David Walker, and Matthew Green.
- HONORS**
- ARCS Foundation Fellowship 2016  
Google Anita Borg Scholarship (1 of 30 in North America) 2016  
Computing Research Association (CRA) Outstanding Undergraduate Researcher Award 2016  
Honorable mention, NSF Graduate Research Fellowship 2016
- PUBLICATIONS**
- Verified correctness and security of mbedTLS HMAC-DRBG**  
**Katherine Ye**, Matthew Green, Naphat Sanguansin, Lennart Beringer, Adam Petcher, and Andrew W. Appel.  
To appear in *ACM CCS '17* (18% acceptance rate).
- 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 W. Appel.  
In *USENIX Security '15* (16% acceptance rate).
- OTHER REFEREED PUBLICATIONS**
- Substance and Style: domain-specific languages for mathematical diagrams**  
Wode Ni\*, **Katherine Ye\***, Joshua Sunshine, Jonathan Aldrich, and Keenan Crane.  
To appear in *DSLDI (Domain-Specific Language Design and Implementation) '17*.
- Designing extensible, domain-specific languages for mathematical diagrams**  
**Katherine Ye**, Keenan Crane, Jonathan Aldrich, and Joshua Sunshine.  
In *OBT (Off the Beaten Track) '17*.
- EXPERIENCE**
- Software Engineering Intern** Summer 2017  
*Google Brain, Distill team*
- ◊ Distill is a journal of machine learning that is dedicated to presenting clear explanations of research in a modern medium. <https://distill.pub/about/>
  - ◊ I designed and built novel interactive visualizations of mathematical ideas for an upcoming Distill article. This article was written in collaboration with a professor at the University at Toronto and three research scientists at Google Brain.
- Software Engineering Intern** Summer 2014  
*Facebook, Search team*
- ◊ Visualized pairwise correlations between features in Facebook’s machine learning models.
- Resident** Summer 2013  
*The Recurse Center (A three-month, full-time “writers’ retreat for programmers”)*
- TALKS**
- PROCESS: finding desire paths in creative interfaces** 2017  
Experimental talk given at Y Conf, a conference hosted by Y Combinator Research.
- Proof assistants as a tool for thought** 2016  
Talk given at the Tools for Thought workshop, hosted by the Recurse Center.

**Strange loops: powerful knot notations** 2015  
Talk given at Strange Loop, an industry conference, on insights in Conway's knot notation.

**Proofs about programs, proofs as programs, programs as proofs!** 2015  
Lightning talk given at !!con on proving code "equal" in Coq.

**SERVICE** CMU REU Program in Software Engineering, Admissions Committee 2017  
SCS Dean's PhD Student Advisory Council 2017  
Founder and co-president, Open Source at Princeton 2013–2015

**ADVISING** Advising Nimo Ni, an undergraduate research intern, as part of a CMU REU program.

**PRESS** **Schneier on Security**, *Proof that HMAC-DRBG has no back doors* (2017)  
**Princeton.edu**, *Ambitious vision for computer science drives Princeton senior Ye's research success* (2016)