David Heath

1101 Juniper Street NE
Unit 211
Atlanta, Georgia, 30309

Phone: 770-361-6450
Email: daheath@illinois.edu

Area of Expertise

Cryptography; Secure Multiparty Computation

Employment

August 2022 - **Assistant Professor**, University of Illinois Urbana-Champaign

2014-2016 **Research Engineer I**, Georgia Tech Research Institute, Atlanta, Georgia

Earned Degrees

2016-2022 **PhD in Computer Science**, Georgia Institute of Technology, Atlanta, Georgia
Advisor: Vladimir Kolesnikov

2010-2014 **BS in Computer Science**
BS in Mechanical Engineering, Georgia Institute of Technology, Atlanta, Georgia

Research Experience

2018-2022 **Graduate Research Assistant**, Georgia Institute of Technology, Atlanta, Georgia
Advisor: Vladimir Kolesnikov

- I co-discovered "stacked garbling", a fundamental improvement to the Garbled Circuit cryptographic primitive. Stacked garbling greatly accelerates the secure handling of programs with conditional branching. Subsequently, I found similar improvements to other secure computation protocols.
- I co-discovered "one-hot garbling", a fundamental improvement to the Garbled Circuit cryptographic primitive. One-hot garbling greatly accelerates the secure handling of vector operations.
- I improved the efficiency of "garbled RAM" by multiple orders of magnitude. Garbled RAM allows the secure handling of random access arrays.
- I developed crypto-technical improvements to interactive Zero Knowledge. These improvements culminated in a system that handles proofs expressed as off-the-shelf C programs and runs them in the 10KHz range.

2016-2018 **Graduate Research Assistant**, Georgia Institute of Technology, Atlanta, Georgia
Advisor: William Harris

- I co-developed "Shara", a new solver for "Constrained Horn Clause" (CHC) systems. CHC systems can be used to formalize programs; solvers for such systems can prove interesting properties of programs.
- I co-developed "Pequod", a solver that automatically deduces the equivalence of programs.

Awards, Grants, and Experience on Sponsored Projects

2020-2021 **Institute for Information Security and Privacy Cybersecurity Seed Funding**
Principal Investigator: Vladimir Kolesnikov
Georgia Tech's Institute for Information Security offers $50,000 in funding to support promising research in the areas of cybersecurity. I drafted and collaborated on a submission with my advisor Vladimir Kolesnikov. The resulting submission"ZK for Anything and Anyone: Practical Zero Knowledge execution of arbitrary C programs" was funded.

2019-2020 **IARPA HECTOR Project**
IARPA sponsored HECTOR (Homomorphic Encryption Computing Techniques with Overhead Reduction), a multi-million dollar research project aimed at improving the usability of secure computation techniques. As a member of the PANTHEON team, I directly worked on the design and implementation of MPC protocols and language design.

2016-2020 **Georgia Tech President's Fellowship**
I received a fellowship that Georgia Tech offers to the top 10 percent of Ph.D. applicants.

2016 **CS 7001 Research Project Award**
Every Computer Science PhD student at Georgia Tech is required to take CS 7001, an introductory course to academic research. Each student is required to write and present work featuring research tasks conducted during the semester. I was presented an award for best research project as part of the Georgia Tech College of Computing Annual Awards and Honors ceremony.

Teaching Experience

Fall 2019 **Guest Lecturer**, Special Topics: Secure Multiparty Computation
I gave two one-hour lectures in this graduate level special topics course. In the first, I presented our new results on Stacked Garbling, both to share interesting new results and to convey a flavor of the research process. In the second, I presented the EMP Toolkit, a state-of-the-art implementation of many multiparty computation, to share how it solves problems with real-world C++ code.

Spring 2019 **Graduate Teaching Assistant**, Special Topics: Blockchain
I generated course materials, held office hours, and graded homeworks and exams for this crosslisted special topics course on blockchain technologies. This was the first year this course was offered at Georgia Tech, so as a TA I helped develop assignments and exams from scratch.

Spring 2018 **Graduate Teaching Assistant**, Compilers and Interpreters
I generated course materials, held office hours, graded homeworks and exams, and gave one lecture for this undergraduate introduction to compiler technologies.

Conference Publications

2022 David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky. EpiGRAM: Practical garbled RAM. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part I*, volume 13275 of *LNCS*, pages 3–33. Springer, Heidelberg, May / June 2022

Abida Haque, David Heath, Vladimir Kolesnikov, Steve Lu, Rafail Ostrovsky, and Akash Shah. Garbled circuits with sublinear evaluator. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part I*, volume 13275 of *LNCS*, pages 37–64. Springer, Heidelberg, May / June 2022

Yibin Yang, David Heath, Vladimir Kolesnikov, and David Devecsery. Ezee: Epoch parallel zero knowledge for ansi c. In *EuroSP 2022*, June 2022

2021 David Heath and Vladimir Kolesnikov. One hot garbling. In *ACM CCS 2021*, November 2021

David Heath and Vladimir Kolesnikov. PrORAM: Fast $O(\log n)$ private coin ZK ORAM. In *ASIACRYPT 2021*, December 2021

David Heath, Vladimir Kolesnikov, and Stanislav Peceny. Garbling, stacked and staggered. In *ASIACRYPT 2021*, December 2021

David Heath and Vladimir Kolesnikov. LogStack: Stacked garbling with $O(b \log b)$ computation. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part III*, volume 12698 of *LNCS*, pages 3–32. Springer, Heidelberg, October 2021

David Heath, Yibin Yang, David Devecsery, and Vladimir Kolesnikov. Zero knowledge for everything and everyone: Fast ZK processor with cached ORAM for ANSI C programs. In *2021 IEEE Symposium on Security and Privacy*, pages 1538–1556. IEEE Computer Society Press, May 2021

David Heath, Vladimir Kolesnikov, and Stanislav Peceny. Masked triples - amortizing multiplication triples across conditionals. In Juan Garay, editor, *PKC 2021, Part II*, volume 12711 of *LNCS*, pages 319–348. Springer, Heidelberg, May 2021

David Heath, Vladimir Kolesnikov, and Jiahui Lu. Efficient generic arithmetic for KKW: Practical linear MPC-in-the-head NIZK on commodity hardware without trusted setup. In Shlomi Dolev, Oded Margalit, Benny Pinkas, and Alexander Schwarzmann, editors, *Cyber Security Cryptography and Machine Learning*, pages 414–431, Cham, 2021. Springer International Publishing

2020 David Heath, Vladimir Kolesnikov, and Stanislav Peceny. MOTIF: (almost) free branching in GMW - via vector-scalar multiplication. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 3–30. Springer, Heidelberg, December 2020

David Heath and Vladimir Kolesnikov. A 2.1 KHz zero-knowledge processor with BubbleRAM. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, *ACM CCS 2020*, pages 2055–2074. ACM Press, November 2020

David Heath and Vladimir Kolesnikov. Stacked garbling - garbled circuit proportional to longest execution path. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 763–792. Springer, Heidelberg, August 2020

David Heath and Vladimir Kolesnikov. Stacked garbling for disjunctive zero-knowledge proofs. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 569–598. Springer, Heidelberg, May 2020

2019 Qi Zhou, David Heath, and William Harris. Relational verification via invariant-guided synchronization. *Electronic Proceedings in Theoretical Computer Science*, 296:28–41, 2019

2018 Qi Zhou, David Heath, and William Harris. Solving constrained horn clauses using dependence-disjoint expansions. *Electronic Proceedings in Theoretical Computer Science*, 278:3–18, 2018

Ph.D. Dissertation

2022 David Heath. *New Directions in Garbled Circuits*. PhD thesis, Georgia Institute of Technology, Atlanta, GA, USA, 2022

Unpublished Manuscripts

Yibin Yang, David Heath, Stanislav Peceny, and Vladimir Kolesnikov. Towards generic MPC compilers via variable instruction set architectures (VISAs)

David Darais, David Heath, Ryan Estes, William Harris, and Michael Hicks. λ-Symphony: A concise language model for MPC

Invited Lectures

2022 David Heath. Stacked garbling and mpc with improved conditional branching. In *NY CryptoDay*, October 2022. https://nycryptoday.wordpress.com/2022/09/27/cryptoday-columbia-friday-october-21-2022/

David Heath. New directions in garbled circuits. In *Theory and Practice of Multiparty Computation Workshop*, June 2022. https://www.youtube.com/watch?v=jOiTfpiLUkA

David Heath. Epigram: Practical garbled RAM. In *Charles River Crypto Day*, March 2022

2021 David Heath. Practical garbled RAM. In *Berkeley Crypto Reading Group*, December 2021

David Heath. Practical garbled RAM. In *CMU Crypto Reading Group*, December 2021

David Heath. Practical garbled RAM. In *UMD Crypto Reading Group*, December 2021. https://talks.cs.umd.edu/talks/2965

David Heath. Practical garbled RAM. In *Stanford Security Seminar*, November 2021. https://crypto.stanford.edu/seclab/sem-21-22/heath.html

David Heath. Logstack: Stacked garbling with $O(b \log b)$ computation. In *TCC Special in-person Workshop*, November 2021

David Heath. Logstack: Stacked garbling with $O(b \log b)$ computation, May 2021. https://crypto.stanford.edu/seclab/sem-20-21/heath.html

David Heath. Zero-knowledge for everything and everyone. In *Georgia Tech Cybersecurity Lecture Series*, February 2021. https://scp.cc.gatech.edu/2021/02/05/zero-knowledge-for-everything-and-everyone/

2020 David Heath. Stacked garbling: Garbled circuit proportional to longest execution path. In *Stanford Security Seminar*, September 2020. https://crypto.stanford.edu/seclab/sem-20-21/heath.html

David Heath. Stacked garbling: Garbled circuit proportional to longest execution path. In *Berkeley Crypto Reading Group*, August 2020

2019 David Heath. Efficiently computing with private data. In *Georgia Tech Cybersecurity Lecture Series*, September 2019. https://mediaspace.gatech.edu/media/David+Heath+-+Efficiently+Computing+with+Private+Data/1_8qvvz08r

Professional Contributions

2023 Program Committee Member, Crypto 2023.

Program Committee Member, PKC 2023.

2022 Program Committee Member, ASIACRYPT 2022.

Program Committee Member, CSCML 2022.

2021 Program Committee Member, CCS 2021.

Program Committee Member, CSCML 2021.

2020 Program Committee Member, CSCML 2020.

Open Source Repositories

David Heath. One Hot Garbling Implementation. https://github.com/DAHeath/one-hot-garbling, 2021

David Heath. LogStack Implementation. https://github.com/DAHeath/logstack, 2021

David Heath. PrORAM Implementation. https://github.com/DAHeath/proram, 2021