David Heath

1317 Grandview Drive
Champaign, Illinois, 61820

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

Expertise

Cryptography; Secure Multiparty Computation

Employment

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**, Georgia Institute of Technology, Atlanta, Georgia

BS in Mechanical Engineering, Georgia Institute of Technology, Atlanta, Georgia

Funding

2023 **USDA APHIS Funding Opportunity**
"Research data and privacy: Building a Framework for Large Scale AMS Data Collection and Utilization in Domesticated Animals"
Principal Investigator: Becky Smith. *UIUC award: USD 212,955*

National Science Foundation Secure and Trustworthy Cyberspace Medium Award
"New Constructions for Garbled Computation"
Principal Investigator: David Heath. *Award: USD 1,200,000. UIUC subward: USD 400,000*

Awards

2023 **Outstanding Doctoral Dissertation Award**
Georgia Tech College of Computing

2022 **Best Paper Award**
IACR Eurocrypt. "EpiGRAM: Practical Garbled RAM".

2020-2021 **Georgia Tech Institute for Information Security and Privacy Cybersecurity Seed Funding**
Principal Investigator: Vladimir Kolesnikov. *USD 50,000*

2016-2020 **Georgia Tech President's Fellowship**
Awarded to top 10 percent of Ph.D. applicants

2017 **Rising Star Doctoral Student Research Award**
Georgia Tech College of Computing

Teaching

Fall 2023 **Instructor**, CS407/ECE407: Cryptography

Spring 2023 **Instructor**, CS598 DH: Special Topics in Secure Computation

Fall 2022 **Instructor**, CS598 DH: Special Topics in Secure Computation

Fall 2019 **Guest Lecturer**, Special Topics: Secure Multiparty Computation

Spring 2019 **Graduate Teaching Assistant**, Special Topics: Blockchain

Spring 2018 **Graduate Teaching Assistant**, Compilers and Interpreters

Students Advised

PhD

2023-... **Ananya Appan**

Anwesh Bhattacharya

Ziling Yang

2022-... **Cruz Barnum**

MS

2023 **Zexiang Chen**. Thesis: "3PC Honest-Majority PRAM Computation with Perfect Security and Low Overhead"

Conference Publications

2023 David Heath and Yibin Yang. Two shuffles make a RAM: Improved constant overhead ZK RAM. In *USENIX*, 2023

Yibin Yang, David Heath, Carmit Hazay, Vladimir Kolnesikov, and Muthu Venkitasubramaniam. Batchman and Robin: Batched and non-batched branching for interactive ZK. In *CCS*, 2023

David Heath, Vladimir Kolesnikov, Stanislav Peceny, and Yibin Yang. Towards generic MPC compilers via variable instruction set architectures (VISAs). In *CCS*, 2023

David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky. Tri-state circuits: A circuit model that captures RAM. In *IACR Crypto*, 2023

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

Unpublished Manuscripts

David Heath. Arithmetic garbled circuits from free XOR. 2023

David Heath. Parallel RAM from cyclic circuits. 2023

David Heath, Vladimir Kolesnikov, and Lucien Ng. Garbled circuit lookup tables with logarithmic number of ciphertexts. 2023

Ph.D. Dissertation

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

Invited Lectures

2023 David Heath. Garbled RAM from tri-state circuits. In *Midwest Crypto Day*, April 2023

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

Service

Conference Program Committee Member

2024 Eurocrypt

2023 CANS

Crypto

PKC

2022 ASIACRYPT

CSCML

2021 CCS

CSCML

2020 CSCML

UICU Computer Science

2023-2024 Member, Graduate Admissions Committee

2022-2023 Member, Undergraduate Studies Committee

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