# David Heath

1317 Grandview Drive
Champaign, Illinois, 61820

Phone: 770-361-6450
Email: daheath@illinois.edu
Web: https://daheath.web.illinois.edu

Office: Siebel Center for Computer Science, Room 4322

## Expertise

Cryptography; Secure Multiparty Computation; Zero Knowledge Proofs

## Employment

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

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

## Earned Degrees

**PhD in Computer Science** 2016 - 2022
Georgia Institute of Technology, Atlanta, Georgia
Advisor: Vladimir Kolesnikov
Thesis: "New Directions in Garbled Circuits"

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

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

## Funding

**USDA APHIS Funding Opportunity** *2023 - 2024*
"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*

**NSF Secure and Trustworthy Cyberspace Medium Award** *2023 - 2026*
"New Constructions for Garbled Computation"
Principal Investigator: David Heath
*Award: USD 1,200,000*
*UIUC subward: USD 400,000*

## Awards

**CCS Distinguished Paper Award** *2023*
"Batchman and Robin: Batched and Non-batched Branching for Interactive ZK"
Yibin Yang, David Heath, Carmit Hazay, Vladimir Kolesnikov, and Muthuramakrishnan Venkitasubramaniam

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

**IACR Eurocrypt Best Paper Award** *2022*
"EpiGRAM: Practical Garbled RAM"
David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky

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

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

## Teaching

### Instructor:

**CS 598 DH** Special Topics in Secure Computation *Spring 2024*
**CS407/ECE407** Cryptography *Fall 2023*
**CS 598 DH** Special Topics in Secure Computation *Spring 2023*
**CS 598 DH** Special Topics in Secure Computation *Fall 2022*

### Graduate Teaching Assistant:

**Special Topics: Blockchain** *Spring 2019*
Instructor: Vladimir Kolesnikov

**Compilers and Interpreters** *Spring 2018*
Instructor: Vivek Sarkar

## Students Advised

### PhD

Cruz Barnum *Fall 2022 - Present*
Ananya Appan *Fall 2023 - Present*
Anwesh Bhattacharya *Fall 2023 - Present*
Ziling Yang *Fall 2023 - Present*

### MS

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

Overhead"

## Conference Publications

### 2024

- David Heath. Efficient arithmetic in garbled circuits. In *IACR Eurocrypt*, 2024.
- David Heath, Vladimir Kolesnikov, and Lucien Ng. Garbled circuit lookup tables with logarithmic number of ciphertexts. In *IACR Eurocrypt*, 2024.
- David Heath and Yibin Yang. Two shuffles make a RAM: Improved constant overhead ZK RAM. In *USENIX*, 2024.

### 2023

- Yibin Yang, David Heath, Carmit Hazay, Vladimir Kolesnikov, and Muthu Venkitasubramaniam. Batchman and Robin: Batched and non-batched branching for interactive ZK. In *CCS*, 2023. **Distinguished paper award.**
- 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 Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part IV*, volume 14084 of *LNCS*, pages 128–160. Springer, Heidelberg, August 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. **Best paper award.**
- 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 *EuroS&P 2022*, June 2022.

### 2021

- David Heath and Vladimir Kolesnikov. One hot garbling. In Giovanni Vigna and Elaine Shi, editors, *ACM CCS 2021*, pages 574–593. ACM Press, November 2021.
- David Heath and Vladimir Kolesnikov. PrORAM - fast $P(\log n)$ authenticated shares ZK ORAM. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part IV*, volume 13093 of *LNCS*, pages 495–525. Springer, Heidelberg, December 2021.
- David Heath, Vladimir Kolesnikov, and Stanislav Peceny. Garbling, stacked and staggered - faster k-out-of-n garbled function evaluation. In Mehdi Tibouchi and Huaxiong Wang,

editors, *ASIACRYPT 2021, Part II*, volume 13091 of *LNCS*, pages 245–274. Springer, Heidelberg, 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 *Cyber Security Cryptography and Machine Learning*, 2021.

### 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, Vladimir Kolesnikov, Varun Narayanan, Rafail Ostrovsky, and Akash Shah. Multiparty garbled RAM with linear scaling. 2024.

- Ananya Appan, David Heath, and Ling Ren. Oblivious single access machines: A new model for oblivious computation. 2024.
- Cruz Barnum, David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky. Adaptive garbled circuits and garbled RAM from non-programmable random oracles. 2024.
- Yibin Yang, David Heath, Carmit Hazay, Vladimir Kolesnikov, and Muthuramakrishnan Venkitasubramaniam. Tight ZK CPU: Batched ZK branching with cost proportional to evaluated instruction. 2024.
- David Heath. Parallel RAM from cyclic circuits. 2023.

## Invited Lectures

### 2024

- David Heath. Garbled RAM from tri-state circuits. In *MongoDB Inc. Cryptography Research Group Seminars*, February 2024.
- David Heath. Garbled RAM from tri-state circuits. In *AlgoCRYPT Seminars*, January 2024.

### 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

- Eurocrypt 2024
- CANS 2023
- Crypto 2023
- PKC 2023
- Asiacrypt 2022
- CSCML 2022
- CCS 2021
- CSCML 2021
- CSCML 2020

### UIUC Computer Science

| | |
|---|---|
| Graduate Admissions Committee | *2023-2024* |
| Undergraduate Studies Committee | *2022-2023* |

## 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.