David Heath

1101 Juniper Street NE
Unit 211
Atlanta, Georgia, 30309

Phone: 770-361-6450
Email: heath.davidanthony@gatech.edu

Area of Study

Cryptography; Secure Multiparty Computation

Education

2016-Present   **PhD in Computer Science**, Georgia Institute of Technology, Atlanta, Georgia
Advisor: Vladimir Kolesnikov
GPA: 4.0

2010-2014   **BS in Computer Science**
BS in Mechanical Engineering, Georgia Institute of Technology, Atlanta, Georgia
Honors: Summa Cum Laude

Experience

2014-2016   **Research Engineer I**, Georgia Tech Research Institute, Atlanta, Georgia
As part of GTRI's Electronic Systems Laboratory, I worked with safety-critical software systems and helped to verify the Future Airborne Capability Environment (FACE™) Technical Standard.

Awards

2016-2020   **Georgia Tech President's Fellowship**
Georgia Tech offers a fellowship to the top 10 percent of PhD applicants.

2016-2020   **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.

Conference Publications

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 (SP)*, pages 1538–1556, Los Alamitos, CA, USA, 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, Vladimir Kolesnikov, and Rafail Ostrovskey. Practical garbled RAM

Yibin Yang, David Heath, Vladimir Kolesnikov, and David Devecsery. EZEE: Epoch parallel zero knowledge for ANSI C

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

Abida Haque, David Heath, Vladimir Kolesnikov, Steve Lu, Rafail Ostrovsky, and Akash Shah. GCWise: Garbled circuits with sublinear evaluator

Talks

2021   David Heath. Logstack: Stacked garbling with $O(b \log b)$ computation. In *Stanford Security Seminar*, May 2021

David Heath. Zero-knowledge for everything and everyone. In *Georgia Tech Cybersecurity Lecture Series*, February 2021

2020   David Heath. Stacked garbling: Garbled circuit proportional to longest execution path. In *Stanford Security Seminar*, September 2020

2019   David Heath. Efficiently computing with private data. In *Georgia Tech Cybersecurity Lecture Series*, September 2019