Riad S. Wahby

riad@cmu.edu
https://wahby.net

Summary

Assistant Professor in ECE at CMU, focusing on systems, security, and applied cryptography. I build secure computer systems with untrusted components, asking questions like "how can we build trustworthy chips at untrusted fabs?" and "how do we secure operating systems against malicious peripherals?" My recent focus has been on probabilistic proof systems and cryptography. Expert circuit designer: analog, digital, mixed-signal; control systems; MEMS. Proficient programmer; open-source software contributor; former competitive violinist; American citizen.

Education

Stanford University **Stanford, CA**
Ph.D. in Computer Science, September 2021.
Dissertation: "Concretely efficient interactive proofs and their applications."
Advisors: Dan Boneh and Keith Winstein.

Massachusetts Institute of Technology **Cambridge, MA**
SB/M.Eng in Electrical Engineering and Computer Science, June 2004.
Thesis: "Radio-Frequency Rectifiers for DC-DC Power Conversion."
Advisor: David Perreault.

Saint Edmond High School **Fort Dodge, IA**
Valedictorian, June 1998.

Experience

Carnegie Mellon University **Pittsburgh, PA**
September 2022–present
Assistant Professor, Electrical and Computer Engineering

Cubist **Pittsburgh, PA**
May 2022–present
Co-founder and CEO

Algorand **Boston, MA**
May 2019–March 2022
Consultant, Postdoctoral Researcher.

Courant Institute of Mathematical Sciences, NYU **New York, NY**
January 2014–September 2015
Junior Research Scientist.

Department of Computer Science, University of Texas **Austin, TX**
September 2013–December 2013
Visiting Researcher.

Silicon Laboratories, Inc. **Austin, TX**
June 2004–December 2013
Staff Design Engineer. High performance analog and mixed-signal integrated circuit design. Technical leader on ProSLIC™ and Digital Isolator product teams.

Publications (including under submission)

P.-L. Wang, R.S. Wahby, and F. Brown, "Bending microarchitectural weird machines towards practicality," *In submission*, February 2024.

F. Wang, S. Cohney, R.S. Wahby, J. Bonneau, "NOTRY: Deniable messaging with retroactive avowal," *Privacy Enhancing Technology Symposium (PETS24)*, July 2024. Open access: Cryptology ePrint 2023/1926.

S. Setty, J. Thaler, and R.S. Wahby, “Unlocking the lookup singularity with Lasso,” *IACR International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT24)*, May 2024. Open access: Cryptology ePrint 2023/1216.

N. Tyagi, A. Arun, C. Freitag, R.S. Wahby, J. Bonneau, and D. Mazières, “Riggs: Decentralized sealed-bid auctions,” *ACM SIGSAC Conference on Computer and Communications Security (CCS23)*, November 2023. Open access: Cryptology ePrint 2023/1336.

A. Kwong, W. Wang, J. Kim, J. Berger, D. Genkin, E. Ronen, H. Shacham, R.S. Wahby, and Y. Yarom, “Checking passwords on leaky computers: a side-channel analysis of Chrome’s password leak detection protocol,” *USENIX Security Symposium (Security23)*, August 2023.

A. Golovnev, J. Lee, S. Setty, J. Thaler, and R.S. Wahby, “Brakedown: Linear-time and field-agnostic SNARKs for R1CS,” *IACR International Cryptology Conference (CRYPTO23)*, August 2023. Open access: Cryptology ePrint 2021/1043.

A. Ozdemir, R.S. Wahby, F. Brown, and C. Barrett, “Bounded verification for finite-field-blasting (in a compiler for zero knowledge proofs),” *International Conference on Computer Aided Verification (CAV23)*, July 2023. Open access: Cryptology ePrint 2023/778.

P.-L. Wang, F. Brown, and R.S. Wahby, “The ghost *is* the machine: weird machines in transient execution,” *IEEE Workshop on Offensive Technologies (WOOT23)*, May 2023.

E. Chen, J. Zhu, A. Ozdemir, R.S. Wahby, F. Brown, and W. Zheng, “Silph: A framework for scalable and accurate generation of hybrid MPC protocols,” *IEEE Symposium on Security and Privacy (Oakland23)*, May 2023. Open access: Cryptology ePrint 2023/060.

S. Setty, J. Thaler, and R.S. Wahby, “Customizable constraint systems for succinct arguments,” *Under submission*, 2023. Preprint: Cryptology ePrint 2023/552.

T.B. Youssef, and R.S. Wahby, “Specialized Proof of Confidential Knowledge (SPoCK),” *Technical report*, 2023. Cryptology ePrint 2023/082.

A. Ozdemir, F. Brown, and R.S. Wahby, “CirC: Compiler infrastructure for proof systems, software verification, and more,” *IEEE Symposium on Security and Privacy (Oakland22)*, May 2022. Open access: Cryptology ePrint 2020/1586.

S. Micali, L. Reyzin, G. Vlachos, R.S. Wahby, and N. Zeldovich, “Compact certificates of collective knowledge,” *IEEE Symposium on Security and Privacy (Oakland21)*, May 2021. Open access: Cryptology ePrint 2020/1568.

F. Brown, A. Ozdemir, J. Renner, M. Smith, R.S. Wahby, D. Engler, S. Lerner, H. Shacham, and D. Stefan, “Just-in-time checking for just-in-time compilers,” *Under submission*, 2020.

J. Cogan, F. Brown, A. Ozdemir, and R.S. Wahby, “High-level high-speed high-assurance crypto,” *Principles of Secure Compilation (PriSC21)*, January 2021.

A. Ozdemir, R.S. Wahby, and D. Boneh, “Scaling verifiable computation using efficient set accumulators,” *USENIX Security Symposium (Security20)*, August 2020. Open access: Cryptology ePrint 2019/1494.

R.S. Wahby, D. Boneh, C. Jeffrey, and J. Poon, “An airdrop that preserves recipient privacy,” *Financial Cryptography and Data Security (FC20)*, February 2020. Open access: Cryptology ePrint 2020/676.

M. Patrignani, R.S. Wahby, and R. Künnemann, “Universal Composability is Secure Compilation,” *Principles of Secure Compilation (PriSC20)*, January 2020. Open access: arXiv:1910.08634.

R.S. Wahby and D. Boneh, “Fast and simple constant-time hashing to the BLS12-381 elliptic curve,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(4), August, 2019. Open access: Cryptology ePrint 2019/403.

S. Cauligi, G. Soeller, B. Johannesmeyer, F. Brown, R.S. Wahby, J. Renner, B. Grégoire, G. Barthe, R. Jhala, and D. Stefan, "FaCT: a DSL for timing-sensitive computation," *ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI19)*, June 2019.

F.Y. Yan, J. Ma, G. Hill, D. Raghavan, R.S. Wahby, P. Levis, and K. Winstein, "Pantheon: the training ground for Internet congestion-control research," *USENIX Annual Technical Conference (ATC18)*, July 2018. *Best paper award.*

R.S. Wahby, I. Tzialla, a. shelat, J. Thaler, and M. Walfish, "Doubly-efficient zkSNARKs without trusted setup," *IEEE Symposium on Security and Privacy (Oakland18)*, May 2018. Open access: Cryptology ePrint 2017/1132.

S. Fouladi, J. Emmons, E. Orbay, C. Wu, R.S. Wahby, and K. Winstein, "Salsify: Low-latency network video through tighter integration between a video codec and a transport protocol," *USENIX Symposium on Networked Systems Design and Implementation (NSDI18)*, April 2018.

R.S. Wahby, Y. Ji, A. Blumberg, a. shelat, J. Thaler, M. Walfish, and T. Wies, "Full accounting for verifiable outsourcing," *ACM SIGSAC Conference on Computer and Communications Security (CCS17)*, October 2017. Open access: Cryptology ePrint 2017/242.

J. Wilson, R.S. Wahby, H. Corrigan-Gibbs, D. Boneh, P. Levis, and K. Winstein, "Trust but verify: auditing secure Internet of Things devices," *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys17)*, June 2017.

F. Brown, S. Narayan, R.S. Wahby, D. Engler, R. Jhala, and D. Stefan, "Finding and preventing bugs in JavaScript bindings," *IEEE Symposium on Security and Privacy (Oakland17)*, May 2017.

S. Fouladi, R.S. Wahby, B. Shacklett, K.V. Balasubramaniam, W. Zheng, R. Bhalerao, A. Sivaraman, G. Porter, and K. Winstein, "Encoding, fast and slow: Low-latency video processing using thousands of tiny threads," *USENIX Symposium on Networked Systems Design and Implementation (NSDI17)*, March 2017.

B. Lampert, R.S. Wahby, S. Leonard, and P. Levis, "Robust, low-cost, auditable random number generation for embedded system security," *ACM Conference on Embedded Networked Sensor Systems (SenSys16)*, November 2016.

S. Angel, R.S. Wahby, M. Howald, J.B. Leners, M. Spilo, Z. Sun, A.J. Blumberg, and M. Walfish, "Defending against malicious peripherals," *USENIX Security Symposium (Security16)*, August 2016. Open access: arXiv:1506.01449.

R.S. Wahby, M. Howald, S. Garg, a. shelat, and M. Walfish, "Verifiable ASICs," *IEEE Symposium on Security and Privacy (Oakland16)*, May 2016. *Distinguished student paper award.* Open access: Cryptology ePrint 2015/1243.

R.S. Wahby, S. Setty, Z. Ren, A.J. Blumberg, and M. Walfish, "Efficient RAM and control flow in verifiable outsourced computation," *Network and Distributed System Security Symposium (NDSS15)*, February 2015. Open access: Cryptology ePrint 2014/674.

J.M. Rivas, R.S. Wahby, J.S. Shafran, and D.J. Perreault, "New architectures for radio-frequency dc-dc power conversion," *IEEE Transactions on Power Electronics*, vol. 21, no. 2, pp. 380–393, June 2006. Conference version: *PESC04*.

Invited presentations (excluding conference presentations)

"Fast and simple constant-time hashing to the BLS12-381 elliptic curve (and other curves, too!)."
ECC19: 23rd Workshop on Elliptic Curve Cryptography, December 2–4, 2019.

"BLS signatures, hashing to curves, and more: dispatches from the IETF."
ACS19: 1st Workshop on Advanced Cryptography Standardization, August 18, 2019.

"Practical proof systems: Implementations, applications, and next steps."
Simons Institute Workshop on Probabilistically Checkable and Interactive Proof Systems, September 23–27, 2019.

"Full accounting for verifiable outsourcing."
DIMACS Workshop on Outsourcing Computation Securely, July 7, 2017.

"Verifiable ASICs: trustworthy hardware with untrusted components."
DIMACS/MACS Workshop on Crypto for the RAM Model of Computation, June 10, 2016.

"Accelerating Cryptographic Protocols with Reconfigurable Hardware."
NSF Secure and Trustworthy Computing / SRC STARSS Kickoff Meeting, January 7, 2015.

"Design of Inertial Sensors in CMEMS."
Silicon Labs Technical Symposium, October 7, 2011.

"A Novel Quasi-Ćuk DC-DC Converter Architecture and Implementation."
Silicon Labs Technical Symposium, January 21, 2008.

Teaching experience

18-330: Computer Security Lecturer, CMU, Spring 2024

CS355: Topics in Cryptography Lecturer, Stanford, Spring 2021

CS144: Introduction to Computer Networking (Course Assistant, Stanford, Winter 2019)

CS140: Operating Systems (Course Assistant, Stanford, Winter 2017)

CS240h: Functional Systems in Haskell (Course Assistant, Stanford, Winter 2016)

6.302: Feedback Systems (Teaching Assistant, MIT, Fall 2002)

Professional service

Program committee member:
IEEE Security and Privacy 2022, 2023; Financial Cryptography and Data Security 2022, 2021; ZKProof Standards Workshop 2020

External reviewer:
FOCS 2022; Crypto 2022, 2021, 2019; Eurocrypt 2021; Asiacrypt 2021; PriSC 2021; ITCS 2020; ACM CCS 2020; IEEE S&P 2018

Journal reviewer:
IEEE Transactions on Networking; Advances in Mathematical Communication; Elsevier Information Sciences; Elsevier Theoretical Computer Science; Designs, Codes and Cryptography; SIAM Journal of Applied Algebraic Geometry

Standards documents (including drafts)

A. Faz-Hernández, S. Scott, N. Sullivan, R.S. Wahby, and C. Wood, "Hashing to Elliptic Curves," IETF RFC 9380, 2023.

D. Boneh, S. Gorbunov, R.S. Wahby, H. Wee, and Zhenfei Zhang, "BLS Signatures," IETF CFRG Internet-Draft, 2020.

Y. Sakemi, T. Kobayashi, T. Saito, and R.S. Wahby, "Pairing-Friendly Curves," IETF CFRG Internet-Draft, 2020.

Patents (including applications)

D.J. Perreault, J.M. Rivas, R.S. Wahby, and J.S. Shafran, “Method and Apparatus for Switched-Mode Power Conversion at Radio Frequencies,” US20050286278 (abandoned application).

G.B. Thompson, S. Sundar, D.R. Frey, R.J. Apfel, M. Goldenberg, I.C. Tesu, R.S. Wahby, and M.J. Mills, “Power Supply with Digital Control Loop,” US7688119.

R.S. Wahby, M.J. Mills, J.A. Whaley, M. Goldenberg, and I.C. Tesu, “Power Supply with Digital Control Loop,” US8462937.

M.J. Mills, R.S. Wahby, G.B. Thompson, D.R. Frey, Z. Li, S. Sundar, and I.C. Tesu, “Power Supply with Digital Control Loop,” US20090243572 (abandoned application).

R.S. Wahby, D.R. Frey, Z. Li, X. Yang, M. Goldenberg, I.C. Tesu, and J.A. Whaley, “Power Supply with Digital Control Loop,” US20090243578 (abandoned application).

I.C. Tesu and R.S. Wahby, “Wide-swing Cascode Current Mirror,” US8450992.

E.B. Smith, R.S. Wahby, and Y. Zhou, “Resonant MEMS Lorentz-Force Magnetometer Using Force-Feedback and Frequency-Locked Coil Excitation,” US9588190.

M.J. Mills, J. Li, and R.S. Wahby, “Isolation Receiver,” US8975914.

S. Sundar, M.J. Mills, H. Zhu, R.S. Wahby, J.L. Sonntag, Y. Huang, and A.N. Nemmani, “Isolated Serializer-Deserializer,” US9118392.

R.S. Wahby, J.L. Sonntag, T.C. Karalar, M.J. Mills, E.B. Smith, I.C. Tesu, and D.E. Alfano, “Soft-Start for Isolated Power Converter,” US9531253.

R.S. Wahby, “Pseudo-Constant Frequency Control for Voltage Converter,” US9531284.

T.J. Dupuis, J.L. Sonntag, M.J. Mills, R.S. Wahby, “Techniques for Reduced Jitter in Digital Isolators,” US9923643.

M.J. Mills, T.J. Dupuis, R.S. Wahby, S. Sundar, J.L. Sonntag, “Suppression of Transients in Communications Across an Isolation Barrier,” US9257836.

M.I. Howald, R.S. Wahby, M. Walfish, A.J. Blumberg, “System and method for authentication with out-of-band user interaction,” US11410175.