Riad S. Wahby

(512) 538–8454
353 Serra Mall, Gates 286
Stanford, CA 94305

rsw@cs.stanford.edu
https://wahby.net

Objective

Research at the intersection of computer systems and integrated circuit design, with emphasis on secure, reliable, and verifiable systems.

Summary

Expert circuit designer: analog, digital, and mixed-signal circuits; control systems; MEMS. Proficient programmer; open-source software contributor; excellent oral and written communication; accomplished violinist; American citizen.

Education

Stanford University **Stanford, CA**
Ph.D. candidate (ongoing; began September 2015).
Advisors: Keith Winstein and David Mazières

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

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. Technical leader on ProSLIC™ and Digital Isolator product teams.

Publications

R.S. Wahby, I. Tzialla, a. shelat, J. Thaler, and M. Walfish, "Doubly-efficient zkSNARKs without trusted setup," *39th IEEE Symposium on Security and Privacy (Oakland18)*, May 2018. Technical report: 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," *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI18)*, April 2017.

R.S. Wahby, Y. Ji, A. Blumberg, a. shelat, J. Thaler, M. Walfish, and T. Wies, "Full accounting for verifiable outsourcing," *2017 ACM SIGSAC Conference on Computer and Communications Security (CCS17)*, October 2017. Technical report: 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," *15th 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," *38th 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," *14th 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," *14th 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," *25th USENIX Security Symposium (Security16)*, August 2016. Technical report: arXiv:1506.01449.

R.S. Wahby, M. Howald, S. Garg, a. shelat, and M. Walfish, "Verifiable ASICs," *37th IEEE Symposium on Security and Privacy (Oakland16)*, May 2016. *Distinguished student paper award.* Technical report: 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," *22nd Network and Distributed System Security Symposium (NDSS15)*, February 2015. Technical report: 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

"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

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)

Patents (and 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.

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.

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.

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,” US20150171901.

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