Biographical Sketch: Riad S. Wahby

Professional preparation

Institution	Major	Degree/Position	Date(s)
Massachusetts Institute of Technology	Elec. Eng. and Comp. Sci.	S.B.	6/2002
Massachusetts Institute of Technology	Elec. Eng. and Comp. Sci.	M.Eng.	6/2004
Stanford University	Computer Science	Ph.D.	(ongoing)

Appointments

Organization	Position	Dates
Stanford University	Graduate Research Assistant	9/2015–
New York University	Junior Research Scientist	1/2014–8/2015
The University of Texas at Austin	Visiting Researcher	9/2013–12/2013
Silicon Laboratories, Inc.	Staff Design Engineer, Mixed-Signal	6/2004–12/2013
Massachusetts Institute of Technology	Graduate Research Assistant	9/2002–5/2004

Awards: USENIX Annual Technical Conference best paper award (2018), IEEE Security and Privacy distinguished student paper award (2016)

Publications / products

Five publications most related to proposal

[1] Riad S. Wahby, Ioanna Tzialla, abhi shelat, Justin Thaler, and Michael Walfish. Doubly-efficient zkSNARKs without trusted setup. In *IEEE S&P*, May 2018.

[2] Riad S. Wahby, Ye Ji, Andrew J. Blumberg, abhi shelat, Justin Thaler, Michael Walfish, and Thomas Wies. Full accounting for verifiable outsourcing. In *ACM CCS*, October 2017.

[3] Riad S. Wahby, Max Howald, Siddharth Garg, abhi shelat, and Michael Walfish. Verifiable ASICs. In *IEEE S&P*, May 2016.

[4] Riad S. Wahby, Srinath Setty, Zuocheng Ren, Andrew J. Blumberg, , and Michael Walfish. Efficient RAM and control flow in verifiable outsourced computation. In *NDSS*, February 2015.

[5] Riad S. Wahby and Dan Boneh. Fast and simple constant-time hashing to the BLS12-381 elliptic curve. *IACR TCHES (to appear)*, 2019(4), August 2019. Preprint: `https://ia.cr/2019/403`.

Selected other publications

[6] Sunjay Cauligi, Gary Soeller, Brian Johannesmeyer, Fraser Brown, Riad S. Wahby, John Renner, Benjamin Grégoire, Gilles Barthe, Ranjit Jhala, and Deian Stefan. FaCT: a DSL for timing-sensitive computation. In *PLDI*, June 2019.

[7] Sadjad Fouladi, Riad S. Wahby, Brennan Shacklett, Karthikeyan Vasuki Balasubramaniam, William Zheng, Rahul Bhalerao, Anirudh Sivaraman, George Porter, and Keith Winstein. Encoding, fast and slow: Low-latency video processing using thousands of tiny threads. In *NSDI*, March 2017.

[8] Judson Wilson, Riad S. Wahby, Henry Corrigan-Gibbs, Dan Boneh, Philip Levis, and Keith Winstein. Trust but verify: auditing secure Internet of Things devices. In *MobiSys*, June 2017.

[9] Sebastian Angel, Riad S. Wahby, Max Howald, Joshua B. Leners, Michael Spilo, Zhen Sun, Andrew J. Blumberg, and Michael Walfish. Defending against malicious peripherals with Cinch. In *USENIX Security*, August 2016.

[10] Riad S. Wahby. Pseudo-constant frequency control for voltage converter. US Patent #9531284.

■ Synergistic activities

- IETF/IRTF CFRG and related working groups. Author of draft standard for hashing to elliptic curves.
- Redesigning undergraduate networking course at Stanford: "Introduction to Computer Networking" (CS144, first offering TBD).
- Previously involved in mentorship and organizing activities for FIRST Robotics competitions, which encourage STEM engagement for middle- and high-schoolers.

■ Selected collaborators & other affiliations

Collaborators: Sebastian Angel (UPenn), Russell Apfel (Audiotoniq), Gilles Barthe (MPI-SWS), Andrew Blumberg (UT Austin), Henry Corrigan-Gibbs (Stanford), Dan Boneh (Stanford), Timothy Dupuis (Silicon Labs), Dawson Engler (Stanford), Douglas Frey (Lehigh), Siddharth Garg (NYU), Marius Goldenberg (Uhnder), Ranjit Jhala (UC San Diego), Philip Levis (Stanford), Michael Mills (Texas Instruments), George Porter (UC San Diego), Srinath Setty (Microsoft Research), abhi shelat (Northeastern), Jeffrey Sonntag (Silicon Labs), Deian Stefan (UC San Diego), Ion Tesu (Silicon Labs), Justin Thaler (Georgetown), Michael Walfish (NYU), Jeffrey Whaley (Silicon Labs), Thomas Wies (NYU), Keith Winstein (Stanford), Yan Zhou (Silicon Labs)

Ph.D. advisors: Dan Boneh, David Mazières, Keith Winstein (Stanford).