

Aaron M. Johnson

CONTACT INFORMATION

Email: ajohnson@cs.utexas.edu

Phone: (651) 398-3103

WWW: <http://www.cs.utexas.edu/~ajohnson>

Mailing Address:

Center for Information Security

Department of Computer Science

The University of Texas at Austin

1 University Station C0500

Austin, Texas 78712

EDUCATION

Yale University, New Haven, CT U.S.A.

- Ph.D., Computer Science, December 2009

Thesis adviser: Prof. Joan Feigenbaum

Dissertation: Design and Analysis of Efficient Anonymous-Communication Protocols

- M.S., Computer Science, May 2005

Northwestern University, Evanston, IL U.S.A.

- B.S. *cum laude* with honors, Computer Science, June 2004

Honors thesis adviser: Prof. Ming-Yang Kao

Honors thesis: Routing Network Flow Among Selfish Agents

PROFESSIONAL EXPERIENCE

Postdoctoral Fellow, The University of Texas at Austin (September 2009 – present)

Adviser: Prof. Vitaly Shmatikov

Department of Computer Science

Conducted research on private data publishing. Developed algorithms for publishing genetic data that are *provably private* and have high accuracy on real data.

Visiting Researcher, Naval Research Laboratory (June 2008 – August 2008)

Host: Dr. Paul Syverson

Conducted research on improved anonymous communication protocols through trust. Designed a model of trust and developed algorithms to improve anonymity in onion routing.

Teaching Fellow, Yale University

ECON 424/563 // CPSC 455/555: Economics and Computation (Fall 2008)

CPSC 365: Design and Analysis of Algorithms (Spring 2007)

CPSC 455/555: Economics and Computation (Spring 2006)

CPSC 150: Computer Science and the Modern Intellectual Agenda (Fall 2006)

RESEARCH INTERESTS

Anonymous communication: Design and analyze anonymous-communication protocols, with an emphasis on provable guarantees for useful systems.

Digital privacy: Design and analyze algorithms for privacy-preserving data publishing and web privacy.

Mathematical foundations of privacy: Develop mathematical models and techniques for problems in digital privacy.

Economics and computation: Understand markets from a computational perspective, and incorporate the rational behavior of agents into the design of computer systems.

PUBLICATIONS

1. **Preventing Active Timing Attacks in Low-Latency Anonymous Communication**
With Joan Feigenbaum and Paul Syverson. In *Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS 2010)*, pp. 166–183, Springer Berlin / Heidelberg, LNCS, 2010.
2. **More Anonymous Onion Routing Through Trust**
With Paul Syverson. In *Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF 2009)*, pp. 3–12, IEEE Computer Society, 2009.
3. **Online and Offline Selling in Limit Order Markets**
With Kevin L. Chang. In *Proceedings of the 4th International Workshop on Internet and Network Economics (WINE 2008)*, pp. 41–52, Springer Berlin / Heidelberg, LNCS, 2008.
4. **Probabilistic Analysis of Onion Routing in a Black-box Model**
With Joan Feigenbaum and Paul Syverson. In *Proceedings of the 2007 ACM Workshop on Privacy in the Electronic Society (WPES 2007)*, pages 1–10. ACM, 2007.
5. **Private Web Search**
With Felipe Saint-Jean, Dan Boneh, and Joan Feigenbaum. In *Proceedings of the 2007 ACM Workshop on Privacy in the Electronic Society (WPES 2007)*, pages 84–90, ACM, 2007.
6. **A Model of Onion Routing with Provable Anonymity**
With Joan Feigenbaum and Paul Syverson. In *Proceedings of the 11th Financial Cryptography and Data Security Conference (FC 2007)*, pages 57–71, Springer Berlin / Heidelberg, LNCS, 2007.

PROGRAM-COMMITTEE MEMBER

- 7th International Workshop on Security and Trust Management (STM'11)**. June 27 – June 28, 2011. Copenhagen, Denmark.
- 11th Privacy Enhancing Technologies Symposium (PETS 2011)**. July 27 – July 29, 2011. Waterloo, Canada.
- 10th Privacy Enhancing Technologies Symposium (PETS 2010)**. July 21 – July 23, 2010. Berlin, Germany.
- 15th ACM Conference on Computer and Communications Security (CCS 08)**. Oct. 27 – Oct 31, 2008. Alexandria, VA, USA.
- 6th ACM Workshop on Formal Methods in Security Engineering (FMSE 08)**. Oct. 27, 2008. Alexandria, VA, USA.
- I have also been an external reviewer for ICALP 2010, IFIP SEC 2010, IEEE S&P 2010, ESORICS 2009, PODC 2009, WWW 2009, PETS 2008, ACM TISSEC, and IEEE TDSC.

TALKS

1. **Preventing Active Timing Attacks in Low-Latency Anonymous Communication**. 10th Privacy Enhancing Technologies Symposium (PETS 2010). July 22, 2010. Berlin, Germany.
2. **More Anonymous Onion Routing Through Trust**. 22nd IEEE Computer Security Foundations Symposium (CSF 2009). July 8, 2009. Port Jefferson, New York.
3. **Online and Offline Selling in Limit Order Markets**. 4th International Workshop on Internet and Network Economics (WINE 2008). December 17, 2008. Shanghai, China.
4. **Towards a Theory of Onion Routing**. Invited talk, Department of Electrical and Computer Engineering, Iowa State University. May 27, 2008. Ames, Iowa.
5. **A Probabilistic Analysis of Onion Routing in a Black-box Model**. 2007 ACM Workshop on Privacy in the Electronic Society (WPES 2007). October 29, 2007. Alexandria, VA.

6. **A Formal Analysis of Onion Routing.** Protocol Exchange Seminar. October 26, 2007. Baltimore, MD.
7. **A Model of Onion Routing with Provable Anonymity.** 11th Financial Cryptography and Data Security Conference (FC 2007). February 12, 2007. Lowlands, Scarborough, Trinidad/Tobago.

OTHER

Technical skills: Python, MATLAB, Mathematica, Java, Haskell, PHP, C++

Citizenship: USA

REFERENCES

Joan Feigenbaum, Ph.D.

Grace Murray Hopper Professor of Computer Science
Department of Computer Science
Yale University
P.O. Box 208285
New Haven, CT 06520
Phone: (203) 436-1267
Email: Joan.Feigenbaum@yale.edu
WWW: <http://www.cs.yale.edu/~jf>

Paul Syverson, Ph.D.

Mathematician
Center for High Assurance Computer Systems
Naval Research Laboratory
P.O. Box 3735
Silver Spring, MD 20918
Phone: (202) 404-7931
Email: syverson@itd.nrl.navy.mil
WWW: <http://www.syverson.org/>

Vitaly Shmatikov, Ph.D.

Associate Professor of Computer Science
Department of Computer Science
The University of Texas at Austin
1616 Guadalupe, Suite 2.408
Austin, TX 78701
Phone: (512) 220 1650
Email: shmat@cs.utexas.edu
WWW: <http://www.cs.utexas.edu/~shmat/>