STEPHEN A. WEIS

32G-694, 32 Vassar Street, Cambridge, MA, 02139
http://crypto.csail.mit.edu/~sweis
(617) 823-0570
sweis@mit.edu

OBJECTIVE

Computer science Ph.D. seeks position in software research and development. Strong background in security, cryptography, and algorithms. Offers extensive practical experience and a solid academic background. Skilled in Java, C, C++, Python, PHP, and most major languages. Highly self-motivated and adaptable with excellent written and verbal communication skills.

PROFESSIONAL EXPERIENCE

Researcher **RSA Laboratories** Bedford, MA, Summer 2004

Conducted research in RFID and low-cost pervasive computing device security. Contributed to the EPC Global RFID standard by discovering flaws in random number generation specifications. Invented a highly-efficient authentication protocol appropriate for low-cost devices.

Developer **Sun Microsystems** Burlington, MA, Summer 2003

Implemented public-key certificate chain validation library in C as part of Sun's Internet Security Research Group. Developed certificate chain discovery algorithms. Wrote programming and implementation guideline documentation.

Researcher **OceanStore Project** Berkeley, CA, 2000-2001

Developed an elliptic curve cryptosystem in Java security framework. Implemented a multi-party threshold digital signature package. Evaluated and optimized the performance of several digital signature schemes. Contributed to a utility-model, wide-area storage infrastructure project.

Developer **Cisco Systems** San Jose, CA, Summer 1999

Programmed web-based network administration applications. Designed a secure cryptographic licensing system, created a prototype user interface, and developed authentication and authorization modules using JSP, JCE, JAAS and Java Swing technology.

EDUCATION

	Massachusetts Institute of Technology		
PhD	Computer Science, Financial Theory (minor)		2003-2006
MS	Computer Science		2001-2003
	University of California, Berkeley		
AB	Computer Science	Magna Cum Laude	1996-2001
BA	Applied Mathematics	Summa Cum Laude	1996-2001

Publications

"Private Disjointness Testing", with Susan Hohenberger, in submission, 2006

"Authenticating Pervasive Devices with Human Protocols", with Ari Juels, *Advances in Cryptology--CRYPTO '05*, Lecture Notes in Computer Science, volume 3621, pages 293-308, 2005

"Security Parallels Between People and Pervasive Devices", *IEEE International Conference on Pervasive Computing and Communications*, 2005

"RFID Security", in *Handbook of Information Security*, edited by Hossein Bidgoli, Wiley, 2005

"PGP", in *Handbook of Information Security*, edited by Hossein Bidgoli, Wiley, 2005

"Conference Reports: Crypto 2004", *IEEE Security and Privacy Magazine*, volume 3, number 2, pages 11-13, March/April 2005

"RFID Privacy Workshop: Concerns, Consensus, and Questions", *IEEE Security and Privacy Magazine*, volume 2, number 2, pages 34-36, March/April 2004

"Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", with Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels, *International Conference on Security in Pervasive Computing*, Lecture Notes in Computer Science, volume 2802, pages 201-212, 2003

"Radio-Frequency Identification: Risks and Challenges", with Sanjay E. Sarma and Daniel W. Engels,, *RSA CryptoBytes*, volume 6, number 1, Winter/Spring 2003

"RFID Systems and Security and Privacy Implications", with Sanjay E. Sarma and Daniel W. Engels, *Workshop on Cryptographic Hardware and Embedded Systems*, Lecture Notes in Computer Science, volume 2523, pages 454-470, 2002

References

Prof. Ronald Rivest
MIT CSAIL
32 Vassar Street, 32-G692
Cambridge, MA 02139
(617) 253-5880
rivest@mit.edu

Prof. Shafi Goldwasser
MIT CSAIL
32 Vassar Street, 32-G682
Cambridge, MA 02139
(617) 253-5914
shafi@csail.mit.edu

Prof. Sanjay Sarma
MIT Dept. of Mechanical Engineering
77 Massachusetts Avenue, 35-010
Cambridge, MA 02139
(617) 253-1925
sesarma@mit.edu

Dr. Ari Juels
RSA Laboratories
174 Middlesex Turnpike
Bedford, MA 01730
(781) 515-7069
ajuels@rsasecurity.com