

Shabsi Walfish

Courant Institute of Mathematical Sciences
New York University
251 Mercer Street, New York, NY 10012

Voice: Available by request
Email: walfish AT cs DOT nyu DOT edu
URL: <http://www.cs.nyu.edu/~walfish>

Curriculum Vitae, February 2007

Research Interests

Theoretical and Applied Cryptography, and Computer Security.

Education

New York University	2001 – 2007
<i>Ph.D. in Computer Science</i>	Summer 2007 (anticipated)
Advisor: Professor Yevgeniy Dodis	
Thesis topic: “Enhanced Security Models for Network Protocols”	
<i>Master of Science in Computer Science</i>	January 2004
The Cooper Union for the Advancement of Science and Art	1997 – 2001
<i>Bachelor of Engineering in Electrical Engineering</i>	June 2001

Honors & Awards

NYU Dean’s Dissertation Fellowship	2006 – 2007
The Harold Grad Memorial Prize	2005
NYU McCracken Fellow	2002 – 2006
The Jesse Sherman Award	2001
NCIIA Commercial Innovation Award	2001
VLSI (Integrated Circuit Engineering) Design Award	2000
3rd Place, ACM Programming Competition (Greater New York Region)	2000
Cooper Union Full Tuition Scholarship	1997 – 2001

Research Experience

Research Assistant	New York University	Fall 2002 – present
Cryptography research (see active Projects).		
Applied Research Intern	Telcordia Technologies	Summer 2004
Security and cryptography research and development for the Internet Services group.		
Applied Research Intern	Telcordia Technologies	Summer 2001
Biometrics and home networking research and development for the Home Networking group.		
Research Intern, Dept. of Chemistry	Cooper Union	1999 – 2001
Research and development of pattern matching algorithms. A patent was issued for this work.		
Research Intern	Cooper Union	Summer 2000
Chaos theory and cryptography research. Funded by the National Security Agency.		

Teaching Experience

New York University

Adjunct Instructor of Computer Science Summer 2006

Taught G22.1170 — *Fundamental Algorithms*, a graduate level course in algorithms.

Teaching Assistant Spring 2006

V22.0102 — *Introduction to Computer Science II*, an undergraduate course in data structures (with Prof. Dan Melamed). Taught weekly Java programming lectures.

Adjunct Instructor of Computer Science Summer 2005

Taught G22.1170 — *Fundamental Algorithms*.

Teaching Assistant Fall 2003

G22.1170 — *Fundamental Algorithms*, with Prof. Victor Shoup. Taught bi-weekly recitation sessions.

Teaching Assistant Summer 2003

Cryptographic Protocols (graduate), with Prof. Markus Jakobsson.

Teaching Assistant Fall 2002

V22.0480 — *Introduction to Cryptography* (undergraduate), with Prof. Yevgeniy Dodis.

Cooper Union

Adjunct Instructor of Electrical Engineering Spring 2005

Taught and designed curriculum for new graduate elective ECE409 — *Advanced Cryptography*.

Adjunct Instructor of Electrical Engineering Fall 2004

Taught 3-credit undergraduate elective ECE309 — *Introduction to Cryptography* (formerly EE360).

Adjunct Instructor of Electrical Engineering Fall 2002

Taught and designed curriculum for new 3-credit upper level undergraduate elective, EE360 — *Introduction to Cryptography*.

Instructor Spring 2001

Taught a course in Matlab for Electrical Engineers.

Instructor Spring 2001

Taught a C programming seminar associated with a course in Numerical Analysis.

Bnai Zion, Russian Scientists Division

Instructor 2004

Taught two week course titled *Cryptography and Computer Security*.

Instructor 2003

Taught two week course titled *Cryptography and Computer Security*.

Papers

Published Works

- [1] Ran Canetti, Yevgeniy Dodis, Rafael Pass, and Shabsi Walfish. Universal Composability with Global Setup. To appear, *Theory of Cryptography Conference (TCC 2007)*, Amsterdam, The Netherlands, Feb. 2007.
- [2] David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard Lipton, and Shabsi Walfish. Intrusion-Resilient Key Exchange in the Bounded Retrieval Model. To appear, *Theory of Cryptography Conference (TCC 2007)*, Amsterdam, The Netherlands, Feb. 2007.
- [3] Giovanni Di Crescenzo, Richard Lipton, and Shabsi Walfish. Perfectly Secure Password Protocols in the Bounded Retrieval Model. *Theory of Cryptography Conference (TCC 2006)*, New York, NY, Mar. 2006.
- [4] Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, and Shabsi Walfish. Versatile Padding Schemes for Joint Signature and Encryption. *ACM Conference on Computer and Communications Security (CCS 11)*, Washington, D.C., Oct. 2004
- [5] Shabsi Walfish, Timothy Sosnowski, Sara Shraibman, Lok Yung, and John Bove. Computer-aided Pattern Recognition of Organic Infrared Spectra. *Internet Journal of Vibrational Spectroscopy*, Vol. 5 ed. 2, 2001.

Unpublished Works

- [6] Yevgeniy Dodis, Victor Shoup, and Shabsi Walfish. On Efficient, Generalized Universally Composable Commitments and Zero-Knowledge. In submission to *Crypto 2007*.
- [7] Giovanni Di Crescenzo, and Shabsi Walfish. Public Key Encryption in the Bounded Retrieval Model. Manuscript.

Patents

1. Giovanni Di Crescenzo, Richard Lipton, and Shabsi Walfish. A method and system for password protocols in the bounded retrieval model with security against dictionary attacks and intrusions. Patent pending.
2. John Bove and Shabsi Walfish. System and method for identifying unknown compounds using spectra pattern recognition. *US Patent No. 6,947,848 (Sep. 20, 2005)*.

Professional Activities

Conference Reviews

EuroCrypt 2003, EuroCrypt 2004, PET 2004, Crypto 2004, EuroCrypt 2005, CCS 2005, EuroCrypt 2006, RSA 2006, TCC 2007, PKC 2007, STOC 2007.

Journal Reviews

Computers & Electrical Engineering.

Memberships

IACR, ACM, IEEE, Order of the Engineer.

Projects and Research Topics

Security Models for Network Protocols (active)

Designed a new security model for network protocols that ensures security will be preserved even when the protocols are running concurrently in a highly complex environment, such as the internet. In particular, secure protocols in the new model may even make use of external, globally available information (such as a standard Public Key Infrastructure) that is also being used simultaneously by other protocols running in the network. Previous models did not properly capture interactions between protocols that share global information. The new security model, and a result demonstrating that it is feasible to construct provably secure protocols in this model for any task (under reasonable assumptions) is detailed in [1]. Ongoing research involves new applications of this security model, such as the efficient protocols for “commitments” and “zero-knowledge proofs” we present in [6]. This work is being conducted at NYU.

Security from Bandwidth-Limited Channels (active)

Devised a new mathematical model for achieving provable security by modeling the bandwidth-limited nature of communication channels. Designed password login protocols provably secure in this model without relying upon any computational assumptions [3]. Additionally designed a secure key exchange protocol in this model that is even resilient to compromises of a user’s secret key, under some standard computational assumptions [2]. Current research involves the construction of new public key encryption schemes in this model [7]. This work was initiated while at Telcordia Technologies (Summer 2004), and is ongoing at NYU. Telcordia has filed a patent application covering the password protocols presented in [3] (see Patents).

Internet Worm Mitigation 2004

Developed a novel software-based technique for limiting the spread of internet worms in corporate LANs (which Telcordia Technologies may patent). Implemented a specialized kernel-mode software firewall driver for Windows NT/2000 to support a prototype of this technique. This project was performed while at Telcordia Technologies (Summer 2004).

Signcryption 2003

Researched new methods for simultaneously providing both privacy and authenticity guarantees (*i.e.* “signcryption”). Developed new bandwidth-optimal signcryption schemes that are compatible with existing infrastructure (such as the PKCS#1 standard infrastructure). Designed, implemented, and benchmarked a new key exchange protocol based on signcryption. Using the aforementioned signcryption techniques, the resulting implementation was several times faster than standard SSL key exchange when offering comparable levels of security. (Implementation was done via extensions to the OpenSSL library source code.) The details of the signcryption schemes, the new key exchange protocol, and the benchmarking results all appear in [4]. This work was done at NYU.

Biometrics 2001

Researched biometrics technologies and emergent biometrics standards for Telcordia Technologies. Analyzed the suitability of biometrics systems for home networking environments, and contributed text for Telcordia deliverables. Developed a fully functional prototype software solution (written in C and embedded Java) for networking fingerprint scanners and maintaining access control databases.

Pattern Matching of Spectra

2001

Designed and implemented computer based pattern matching techniques for use in the identification of chemical compounds from infrared spectra (see [5]). A patent held jointly in my name has been issued based on this work (see Patents). This work was performed for the Department of Chemistry at Cooper Union.

Cooper Union Senior Thesis

2001

Served as project leader (team of four engineers) for a year long project to develop a *Fire Fighting Robot*. Designed and programmed a first generation autonomous robot to compete in the 8-th Annual Trinity College Fire Fighting Home Robot competition. Devised and implemented an original navigation system (software and hardware). Final placement at the competition was 8-th place out of 54 qualified entrants. The navigation system was awarded First Prize by the National Collegiate Inventors and Innovators Alliance, for its commercial innovation potential.

VLSI (Integrated Circuit Engineering)

2000

Working with a single partner, used HSpice and Cadence software to design a complete *3-bit Flash A/D Converter* chip. The chip was actually fabricated and tested, then compared to other fabricated chips. This project was required coursework in the Electrical Engineering major at Cooper Union. Based on relative performance, this design received a departmental *Best VLSI Design Award*.

Chaos and Cryptography

2000

Studied chaotic synchronization phenomena and conducted original research in chaos theory applied to cryptography. This research was performed at Cooper Union under the auspices of the Cooper Union Research Foundation (CURF), and was funded by the National Security Agency (NSA).

Skills

Operating Systems: System administration for Microsoft Windows, UNIX, and Linux.

Programming Languages: Intel x86 Assembly, Ada95, BASIC, C/C++, Java, LISP, Prolog. Experienced with network sockets and kernel mode programming in both Windows and Linux. Proficient at debugging software and identifying security vulnerabilities in source code.

Engineering Software: AutoCAD, Cadence, HSpice, Protel, Matlab.

References

Available by request.