

## **Brian A. LaMacchia**

14150 NE 20th St., #246  
Bellevue, WA 98007  
bal@farcaster.com  
(206) 726-4931  
<http://www.farcaster.com/>

### **Degrees Awarded**

Massachusetts Institute of Technology

- Ph.D. Electrical Engineering and Computer Science June 1996  
Thesis under Professor G. J. Sussman on “Internet Fish,” automated resource discovery on the World Wide Web. Minor in theoretical mathematics; related courses on “Copyright” and “Law, Internet and Society” taken at Harvard Law School.
- S.M. Electrical Engineering and Computer Science June 1991  
Advanced courses in programming languages, theory of computation, architecture, and cryptography. Thesis research on public-key cryptosystems.
- S.B. Electrical Engineering June 1990  
S.B. Computer Science June 1990  
Minor in economics. Thesis research on chaotic electrical circuits.

### **Professional History**

- Microsoft Corporation Redmond, WA  
Software Architect, Office of the Chief Technology Officer February, 2005 – present  
Provide architectural guidance, design expertise and technical review to various incubation projects within the Office of the CTO, including projects related to grid computing, concurrency, wireless mesh networking and malware defenses. Serve as a founding member of the Microsoft Cryptography Review Board, providing technical guidance for Windows and other Microsoft products in their uses of cryptography. Represent Microsoft in external technical forums and academic outreach efforts.
- Microsoft Corporation Redmond, WA  
Software Architect, Windows Security May 2002 – January, 2005  
Provided architectural guidance, design expertise and technical review to the Windows Security Business Unit (and other Microsoft product teams) in the areas of cryptography, public key infrastructure, trust models and management, security threats, and managed code security. Helped drive a consistent architectural framework for the Windows security platform that addressed the Microsoft strategic vision and broader industry requirements. Provided technical coordination and support with other Microsoft teams to ensure proper alignment of their effort with the Windows security platform. Supported marketing and technical teams in communication about, and evangelization of, the Windows security platform and its features.
- Microsoft Corporation Redmond, WA  
Development Lead, .NET Framework Security April 1999 - April 2002  
Led and managed the development team responsible for implementation of the security infrastructure for the .NET Framework. Architected the “evidence-based security” trust management model, and designed and built managed APIs for cryptographic services. Co-authored the IETF/W3C XMLDSIG proposed standard for digitally-signed XML objects.
- Microsoft Corporation Redmond, WA  
Program Manager, Windows NT Security August 1997 - March 1999  
Managed development of core cryptographic and PKI components for Windows 2000, including trust management systems based on public key credentials and digital signatures. Represent

Microsoft public key development at the IETF and designed the cryptographic protocols for IETF RFC 2797, Certificate Management Messages over CMS (CMC).

Public Policy Research, AT&T Labs-Research  
Senior Technical Staff Member  
Major areas of research include trust management systems, trust policy specification languages, digital signature standards and meta-information labeling schemes.

Murray Hill, NJ

September 1996 - August 1997

Massachusetts Institute of Technology  
Research Assistant  
Supported the research activities of Project MAC, the Mathematics and Computation group of the MIT AI Lab, including intelligent network navigation tools, chaotic dynamical systems, and cryptographic applications. Aided in the development of the Scheme programming environment. Supported the introductory undergraduate computer science class at MIT, 6.001, "Structure and Interpretation of Computer Programs."

Cambridge, MA

March 1987 - June 1996

LaMacchia Computer Consulting  
Independent Consultant  
Provide short-term technical consulting in a variety of areas, including local area networking, network security, cryptography, and general PC/Macintosh assistance.

Cambridge, MA

June 1994 - September 1996

Computer Sciences Research Center, AT&T Bell Laboratories  
Member of Technical Staff  
Researched transition system reduction algorithms for augmented finite state machines.

Murray Hill, NJ

June 1992 - August 1992

Mathematical Sciences Research Ctr., AT&T Bell Laboratories  
Co-op Student  
Researched new algorithms for performing lattice basis reduction and applications to public key cryptosystems. Designed new basis reduction algorithms particularly effective at solving problems arising from integer knapsack-based cryptosystems. Implemented several algorithms and analyzed their theoretical and practical performance bounds.

Murray Hill, NJ

June 1990 - December 1990

Massachusetts Institute of Technology  
Teaching Assistant  
Recitation instructor for "Theory of Computation."

Cambridge, MA

January 1990 - May 1990

Mathematical Sciences Research Ctr., AT&T Bell Laboratories  
Co-op Student  
Designed, implemented and analyzed algorithms for computing discrete logarithms in finite fields. As a practical example, computed a database of selected logarithms for a finite field used in a commercial authentication protocol. The database allows the discrete logarithms of any number in the field to be computed in a reasonable amount of time, thus invalidating the security of the authentication scheme.

Murray Hill, NJ

May 1989 - August 1989

Network Perf. Characterization Dpt., AT&T Bell Laboratories  
Co-op Student  
Developed performance threshold values for the #4 Electronic Switching System and the Network Control Point switch. Analyzed voice quality and analog impairment data for AT&T's Public Switched Network and the networks of other interexchange carriers. Developed various computer-related tools to assist in the publication and presentation of competitive assessment results.

Holmdel, NJ

June 1988 - August 1988

## Publications

### Books

Brian A. LaMacchia, Sebastian Lange, Matthew Lyons, Rudi Martin and Kevin T. Price. “.NET Framework Security.” Addison Wesley Professional: New York, April 2002. (ISBN 067232184X)

### Standards

Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, “XML-Signature Syntax and Processing,” W3C Recommendation, Donald Eastlake, Joseph Reagle and David Solo, eds., February 12, 2002. Also available as IETF RFC 3275.

### Journal Papers

Barbara L. Fox and Brian A. LaMacchia. “Encouraging Recognition of Fair Uses in DRM systems.” Communications of the ACM, Vol. 46, No. 4 (April 2003), 74-83.

Lorrie Faith Cranor and Brian A. LaMacchia. “Spam!,” Communications of the ACM, Vol. 41, No. 8 (Aug. 1998), 74-83.

M. Coster, A. Joux, B. LaMacchia, A. Odlyzko, C. P. Schnorr and J. Stern. “Improved Low-density Subset Sum Algorithms,” Computational Complexity 2(2) (1992), 111-128.

B. A. LaMacchia and A. M. Odlyzko, “Computation of Discrete Logarithms in Prime Fields,” Designs, Codes and Cryptography 1 (1991), 47-62.

### Conference and Workshop Papers

[\*] refereed

Brian A. LaMacchia, “Key Challenges in DRM: An Industry Perspective,” Proceedings of the 2002 ACM Workshop on Digital Rights Management, J. Feigenbaum, ed., Lecture Notes in Computer Science 2696, Springer-Verlag, NY (2003), 51-60.

Barbara L. Fox and Brian A. LaMacchia, “Online Certificate Status Checking in Financial Transactions: The Case for Re-issuance,” Advances in Cryptology: Proceedings of Financial Cryptography '99, M. Franklin, ed., Lecture Notes in Computer Science 1648, Springer-Verlag, NY (1999), 104-117. [\*]

Barbara L. Fox and Brian A. LaMacchia, “Cooperative Security: A Model for the New Enterprise,” Proceedings of the Seventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '98), Stanford, CA, June 1998, 314-319. [\*]

Barbara L. Fox and Brian A. LaMacchia, “Certificate Revocation: Mechanics and Meaning,” Advances in Cryptology: Proceedings of Financial Cryptography '98, R. Hirschfeld, ed., Lecture Notes in Computer Science 1465, Springer-Verlag, NY (1998). [\*]

Yang-Hua Chu, Joan Feigenbaum, Brian LaMacchia, Paul Resnick and Martin Strauss, “REFEREE: Trust Management for Web Applications,” Proceedings of the Sixth International World Wide Web Conference, Santa Clara, CA, April 1997. Reprinted in Computer Networks and ISDN Systems 29 (1997), 953-964. [\*]

Brian A. LaMacchia, “The Internet Fish Construction Kit,” Proceedings of the Sixth International World Wide Web Conference, Santa Clara, CA, April 1997. Reprinted in Computer Networks and ISDN Systems 29 (1997), 1237-1248 [\*]

M. J. Coster, B. A. LaMacchia, A. M. Odlyzko and C.-P. Schnorr, An improved low-density subset sum algorithm, Advances in Cryptology: Proceedings of Eurocrypt '91, D. W. Davies, ed., Lecture Notes in Computer Science 547, Springer-Verlag, NY (1991), 54-67. [\*]

Brian A. LaMacchia and Andrew M. Odlyzko, Solving Large Sparse Linear Systems over Finite Fields, *Advances in Cryptology: Proceedings of Crypto '90*, A. Menezes, S. Vanstone, eds., Lecture Notes in Computer Science 537, Springer-Verlag, NY (1991), 109-133. [\*]

#### Theses and Technical Reports

“Internet Fish.” PhD Dissertation, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA (1996). Also available as AI Technical Report 1579, MIT Artificial Intelligence Laboratory, Cambridge, MA (1996).

“Basis Reduction Algorithms and Subset Sum Problems.” SM Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA (1991). Also available as AI Technical Report 1283, MIT Artificial Intelligence Laboratory, Cambridge, MA (1991).

“Precision Measurements of Chaotic Circuits.” SB Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA (1990).

B. A. LaMacchia and J. Nieh. “The Standard Map Machine.” AI Memo 1165, Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA (1989).

#### Patents

Barbara L. Fox, and Brian A. LaMacchia, “Intelligent trust management method and system,” U.S. Patent #6,965,999, issued November 15, 2005.

Barbara L. Fox, and Brian A. LaMacchia, “Certificate reissuance for checking the status of a certificate in financial transactions,” U.S. Patent # 6,842,863, issued January 11, 2005.

#### Recent Professional Activities

MTW 2006 (Program Committee)  
ACM DRM 2005 (Program Committee)  
ACM DIM 2005 (Program Committee)  
ICSOC 2005 (Program Committee)  
SECURECOMM 2005 (Program Committee)  
DIMACS 2005 Security of Web Services and E-Commerce (Workshop Organizer)  
ACM DRM 2004 (Program Committee)  
ACM CCS 2004 (Program Committee)  
WWW2004 (Security and Privacy Track Chair)  
ACM CCS 2003, Industry Track (Program Committee)  
WWW2003 (E-Commerce and Security Track Deputy Chair)  
DIMACS 2003 Workshop (Program Committee)  
ICEC03 (Program Committee)  
11th USENIX Security Symposium (Program Committee)  
XMLSec2002 (Program Committee)  
WWW2002, Electronic Commerce & Security Track (Program Committee)

#### Honors and Accomplishments

AT&T Foundation PhD Fellowship, 1991-1995  
Eta Kappa Nu, Member  
Tau Beta Pi, Member  
Sigma Xi, Full Member  
Ernst A. Guillemin Thesis Competition, First Prize (1990)  
David A. Chanen Writing Award, 1990  
George C. Newton Undergraduate Laboratory Prize, 1989