Brian A. LaMacchia

14150 NE 20th St. Ste. F1 #246
Bellevue, WA 98007
bal@farcaster.com
(206) 726-4931
https://www.brianlamacchia.net/

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
Distinguished Engineer — September 2017 – present

Build, lead and manage the Security & Cryptography team within Microsoft Research, a cross-functional team of researchers, developers and program managers all specializing in cryptography and system security. Perform basic and intentional research on security & cryptography problems of interest to Microsoft business groups, and then develop, implement and tech-transfer solutions to those problems. Ship a suite of security- and cryptography-related libraries, including Microsoft's core cryptography libraries, on a quarterly cycle to over 40 business group customers across Microsoft. Perform custom cryptographic development for Microsoft product teams. Help recruit & hire world-class cryptography & security talent for Microsoft. Participate in establishment and enforcement of company-wide design, development, operations and compliance standards for cryptography, and participate in Severe Security Incident Response Plans (SSIRPs) when cryptography-related vulnerabilities are discovered in Microsoft products and services. Work with Microsoft's Global Trade Office on export and import issues related to cryptographic technologies. Represent Microsoft's interests in international standards organizations and academic outreach efforts. Serve on Microsoft's Cryptography Review Board and other cross-company special efforts on security & cryptography.

Prior titles/organizational positions in essentially the same role:

Director, Security & Cryptography, Microsoft Research	September 2010 – September 2017
Software Architect & Group Manager, Microsoft Research	June 2009 – September 2010
Software Architect & Group Manager, Office of the CRSO	September 2007– June 2009

Microsoft Corporation — Redmond, WA
Software Architect, Office of the Chief Research & Strategy Officer — February 2005 – September 2007

Provide architectural guidance, design expertise and technical review to various incubation projects within the Office of the CRSO, 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 Murray Hill, NJ
Senior Technical Staff Member September 1996 – August 1997

Major areas of research include trust management systems, trust policy specification languages, digital signature standards and meta-information labeling schemes.

Massachusetts Institute of Technology Cambridge, MA
Research Assistant March 1987 – June 1996

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."

LaMacchia Computer Consulting Cambridge, MA
Independent Consultant June 1994 – September 1996

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

Computer Sciences Research Center, AT&T Bell Laboratories Murray Hill, NJ
Member of Technical Staff June 1992 – August 1992

Researched transition system reduction algorithms for augmented finite state machines.

Mathematical Sciences Research Ctr., AT&T Bell Laboratories Murray Hill, NJ
Co-op Student June 1990 – December 1990

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.

Massachusetts Institute of Technology Cambridge, MA
Teaching Assistant January 1990 – May 1990

Recitation instructor for "Theory of Computation."

Mathematical Sciences Research Ctr., AT&T Bell Laboratories Murray Hill, NJ
Co-op Student May 1989 – August 1989

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.

Network Perf. Characterization Dpt., AT&T Bell Laboratories Holmdel, NJ
Co-op Student June 1988 – August 1988

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.

Publications

Books

[1] 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

[2] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, "XML Signature Syntax and Processing Version 1.1," W3C Recommendation, Donald Eastlake, Joseph Reagle, David Solo, Frederick Hirsch, Thomas Roessler, Kelvin Yiu, Pratik Datta, Scott Cantor, eds., July 23, 2015.

[3] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, "XML Signature Syntax and Processing Version 1.1," W3C Recommendation, Donald Eastlake, Joseph Reagle, David Solo, Frederick Hirsch, Magnus Nystrom, Thomas Roessler, Kelvin Yiu, eds., April 11, 2013.

[4] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, "XML Signature Syntax and Processing (Second Edition)," W3C Recommendation, Donald Eastlake, Joseph Reagle, David Solo, Frederick Hirsch and Thomas Roessler, eds., June 10, 2008.

[5] Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), A. Nadalin, C. Kaler, P. Hallam-Baker and R. Monzillo, eds. OASIS Standard 200401, March 2004.

[6] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, "XML Signature Syntax and Processing (XMLDSIG)," W3C Recommendation, Donald Eastlake, Joseph Reagle and David Solo, eds., February 12, 2002. Also available as IETF RFC 3275.

[7] W. Ford, P. Hallam-Baker, B. Fox, B. Dillaway, B. LaMacchia, J. Epstein and J. Lapp, "XML Key Management Specification (XKMS)," W3C Note, March 30, 2001.

Journal Papers

[8] Brian A. LaMacchia. "The Long Road Ahead to Transition to Post-Quantum Cryptography" Communications of the ACM, Vol. 65, No. 1 (January 2022), 28-30. DOI: 10.1145/3498706

[9] Brian A. LaMacchia and John L. Manferdelli. "New Vistas in elliptic curve cryptography." Information Security Technical Report, Vol. 11, No 4 (2006), 186-192.

[10] 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.

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

[12] 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.

[13] 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

[14] Michael Naehrig, Erdem Alkim, Joppe Bos, Leo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila. "FrodoKEM." Third Round Candidate Algorithm, Post-Quantum Cryptography Standardization, US National Institute of Standards and Technology (2020). (Available online at https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.) [*]

[15] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, and Aaron Hutchinson. "SIKE." Third Round Candidate Algorithm, Post-Quantum Cryptography Standardization, US National Institute of Standards and Technology (2020). (Available online at https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.) [*]

[16] Brian A. LaMacchia, Kristin Lauter and Anton Mityagin, "Stronger security of authenticated key exchange," Proceedings of Provable Security, First International Conference (ProvSec 2007), M. Susilo, J. K. Liu, Y. Mu, eds., Lecture Notes in Computer Science 4784, Springer-Verlag, NY (2007), 1-16. [*]

[17] Marty Humphrey, Sang-min Park, Jun Feng, Norm Beekwilder, Glenn S. Wasson, Jason Hogg, Brian LaMacchia and Blair Dillaway, "Fine-grained access control for GridFTP using SecPAL," Proceedings of the Eighth IEEE/ACM International Conference on Grid Computing (GRID 2007), IEEE 2007, 217-225. [*]

[18] 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.

[19] 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. [*]

[20] 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. [*]

[21] 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). [*]

[22] 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. [*]

[23] 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 [*]

[24] 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. [*]

[25] 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

[26] “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).

[27] “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).

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

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

Patents

Inventor or co-inventor on 35 issued United States patents, multiple international patents, and many in-process patent applications (US and international).

Professional Activities

Adjunct Associate Professor, School of Informatics and Computing, Indiana University Bloomington, October 2014 – present

Affiliate Faculty, Department of Computer Science and Engineering, University of Washington, September 2002 – present

International Association for Cryptologic Research (IACR)
Treasurer, 2017 – present (current term expires December 31, 2022)
CRYPTO 2016 General Chair and *ex officio* Board Member, 2015-2016
Steering Committee Member, Symposium on Real World Cryptography, 2015 – present

Member, Forum on Cyber Resilience, National Academies of Science, Engineering, and Medicine, May 2021 – present

Member, Committee on the Future of Encryption, National Academies of Science, Engineering, and Medicine, August 2020 – present

Council Member, Computing Community Consortium, Computing Research Association, July 2020 – present

PhD Thesis Committee Member for the following students:
Zheng Dong, Indiana University Bloomington, graduated 2015
Rich Shay, CMU, graduated 2015
Mihaela Ion, University of Trento, graduated 2014
Fangfei Zhou, Northeastern University, graduated 2012

Program Committee member and reviewer for many professional conferences, journals and grant evaluation panels, including: IACR Symposium on Real World Cryptography (RWC), IEEE Symposium on Security & Privacy ("IEEE Oakland"), ACM Conference on Computer and Communications Security ("ACM CCS"), Usenix Security Symposium ("Usenix Security"), International World Wide Web Conference ("WWW"), ACM Workshop on Digital Identity Management (DIM), ACM Workshop on Digital Rights Management (DRM), Workshop on Usable Security (USEC), SECURECOMM, ACM Computing Surveys, ACM Transactions on Internet Technology, IEEE Transactions on Computers, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Knowledge and Database Engineering, International Journal of Information Security, Journal of Communications and Networks, Journal of Computer Security, Journal of Digital Libraries, U.S. National Science Foundation, DARPA, Hong Kong Research Grants Council (HK RCG).

Honors and Accomplishments

Board of Directors, Seattle Opera — January 2018 – present
Vice President, July 2019 – present

Board of Directors, Seattle International Film Festival — September 2009 – December 2019
President, January 2015 – December 2016
Vice President, September 2012 – December 2014
Treasurer, September 2010 – August 2012
Secretary, September 2009 – August 2010

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