Curriculum Vitae for Matt Franklin

Education

Feb 1994 Ph.D. in Computer Science, Columbia University, New York, NY.
Thesis Advisors: Zvi Galil, Moti Yung.
Thesis: Efficiency and Security of Distributed Protocols.

May 1985 M.A. in Mathematics, University of California, Berkeley, CA.
Thesis Advisors: Elwyn Berlekamp, Gilles Brassard.
Thesis: Mathematical Investigations of the Data Encryption Standard.

May 1983 B.A. in Mathematics, Pomona College, Claremont, CA.

Recent Professional Experience

July 2000-present U. C. Davis, CS Dept (Professor 2004, Assoc Prof 2002).
1998-2000 Xerox PARC, Palo Alto, CA, Member of Research Staff.
1994-98 AT&T Research (aka Bell Labs), Principal Technical Staff Member.

Fellowships and Awards

Godel Prize (2013), ACM SIGACT / EATCS.
Packard Foundation Fellowship in Science and Engineering (2001-08).
NSF CAREER Award (2001-06).
AT&T Bell Labs Ph.D. Scholar (1990-94).

Editorial Boards

J. Cryptology 2000-present (Editor in Chief 2009-14);
J. Computer Security 2001-08; IET Information Security 2005-08;
Int. J. Inf. and Comp. Security 2006-08; Int. J. Applied Crypto 2007-08;
Int. J. Security and Networks 2006-08.

Conference Chairs

CANS 2008 (Co-Chair); Crypto 2004 (Chair); Financial Crypto 1999 (Chair).

Program Committees

Mathematical Foundations of Computer Science (2015);
Crypto (2008,2007,2002,1998); Eurocrypt (2006, 2001); Asiacrypt (2002); Theory of Cryptography (2009); Public Key Cryptography (2008); Financial Crypto (2001,1998,1997); ACM Security (1999,1996); Computer Security Foundations (2000); Selected Areas in Cryptography (2001); ACM E-Commerce (2001); Network and Distributed Systems Security (2003); ACM Digital Rights Management (2003), ICDCS Security Track (2005), ICALP Crypto/Security Track (2005).

Journal Articles

M. Lee, J. Kim, M. Franklin. "Enhancing Security of Personal Identification Numbers with 3-D Displays," J. Mobile Information Systems, March 2016.

M. Franklin, R. Gelles, R. Ostrovsky, L. Schulman, Optimal coding for streaming authentication and interactive comm, IEEE Trans Inf Th (2015).

J. Hong, J. Kim, J. Kim, M. Franklin, K. Park, Fair threshold decryption with semi-trusted third parties, Int. J. Applied Cryptography (2010).

M. Franklin, A survey of key evolving cryptosystems, Int. J. Security and Networks 1(2006):46–53.

J. Considine, M. Fitzi, M. Franklin, L. Levin, U. Maurer, D. Metcalf, Byzantine Agreement given partial broadcast, J. Cryptology 3 (2005):191–217.

M. Franklin, M. Yung, Secure hypergraphs: privacy from partial broadcast, SIAM J. Discrete Math 18(2004):437–450.

D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, SIAM J. Computing 32(2003):586–615.

D. Dean, M. Franklin, A. Stubblefield, An algebraic approach to IP traceback, ACM Trans. Information and System Security, 5(2002):119–137.

D. Boneh, M. Franklin, Efficient generation of shared RSA keys, J. ACM, 48(4):702–722, 2001.

M. Franklin, Z. Galil, M. Yung, Eavesdropping games, J. ACM 47(2):225-243, 2000.

M. Franklin, R. Wright, Secure communication in minimal connectivity models, J. Cryptology, 13(1):9–30, 2000 (special issue).

H. Buhrman, M. Franklin, J. Garay, J. Hoepman, J. Tromp, P. Vitanyi, Mutual search, J. ACM, 46(4):517–536, 1999.

A. Beimel, M. Franklin, Reliable communication over partially authenticated networks, Theor. Computer Science, 220(1)185–210, 1999 (special issue).

M. Franklin, D. Malkhi, Auditable metering with lightweight security, J. Comp. Sec. 6(4), 1998.

M. Reiter, M. Franklin, R. Wright, J. Lacy, Key management in the Omega system, J. Comp. Sec. 4(4):267–287, 1996.

M. Franklin, M. Reiter, The design and implementation of a secure auction service, IEEE Trans. Software Engineering, 22(5):302–312, 1996.

M. Franklin, S. Haber, Joint encryption and message-efficient secure computation, J. Cryptology 9(4):217–232, 1996.

A. Gabrielian, M. Franklin, Multi-level specification and verification of real-time software, CACM 34(5):50–60, 1991 (invited from ICSE 1990).

Refereed Conference Publications

Practical Dual-Receiver Encryption,
RSA-CT 2014, with S. Chow, H. Zhang.

Optimal Coding for Streaming Authentication and Interactive Comm,
Crypto 2013, with R. Gelles, R. Ostrovsky, L. Schulman.

Unique Ring Signatures: A Practical Construction,
Financial Crypto 2013, with H. Zhang.

Unique Group Signatures,
ESORICS 2012, with H. Zhang.

Privacy-Preserving Alibi Systems,
ASIACCS 2012, with H. Chen, B. Davis.

Secure and Efficient Evaluation of Multivariate Polys and Applications.
ACNS 2010, with P. Mohassel.

Fair Threshold Decryption with Semi-trusted Third Parties.
ACISP 2009, with J. Hong, J. Kim, J. Kim, K. Park.

Communication-Efficient Private Protocols for Longest Common Subsequence.
RSA-CT 2009, with M. Gondree, P. Mohassel.

Multi-party indirect indexing and applications.
Asiacrypt 2007, with M. Gondree, P. Mohassel.

Secure linear algebra using linearly recurrent sequences.
TCC 2007, with E. Kiltz, P. Mohassel, E. Weinreb.

Towards optimal and efficient perfectly secure message transmission.
TCC 2007, with M. Fitzi, J. Garay, S. Harsha Vardhan.

Weakly-private secret sharing schemes.
TCC 2007, with A. Beimel.

Improved efficiency for private stable matching.
RSA-CT 2007, with M. Gondree, P. Mohassel.

Edge eavesdropping games.
Security and Cryptography for Networks (SCN) 2006, with A. Beimel.

Efficient polynomial operations in the shared-coefficients setting.
PKC 2006, with P. Mohassel.

Efficiency tradeoffs for malicious two-party computation.
PKC 2006, with P. Mohassel.

A generic approach to intrusion-resilient encryption.
RSA-CT 2004, with Y. Dodis, J. Katz, A. Miyaji, M. Yung.

Intrusion-resilient public key encryption.
RSA-CT 2003, with Y. Dodis, J. Katz, A. Miyaji, M. Yung.

Self-healing key distribution with revocation.
IEEE Oakland 2002, J. Staddon, S. Miner, D. Balfanz, M. Malkin, D. Dean.

Identity-based encryption from the Weil Pairing.
Crypto 2001, with D. Boneh.

Lower bounds for multicast MACs.
Eurocrypt 2001, with D. Boneh, G. Durfee.

An algebraic approach to IP traceback.
NDSS 2001, with D. Dean, A. Stubblefield.

Cryptography as a network service.
NDSS 2001, with T. Berson, D. Dean, M. Spreitzer, D. Smetters.

Distribution chain security.
ACM Security 2000, with G. Durfee.

Deniable payments and electronic campaign finance.
AsiaCrypt 2000, with T. Sander.

Anonymous authentication with subset queries.
ACM CCS 1999, with D. Boneh.

An efficient public key traitor tracing scheme.
Crypto 1999, with D. Boneh.

Privacy and trust in electronic communities.
ACM E-Commerce 1999, with B. Huberman, T. Hogg.

Self-testing/correcting protocols.
DISC 1999, with J. Garay, M. Yung.

Secure communication in minimal connectivity models.
Eurocrypt 1998, with R. Wright.

Mutual search.
ACM SODA 1998, with Buhrman, Garay, Hoepman, Tromp, Vitanyi.

Reliable communication over partially authenticated networks.
WDAG 1997, with A. Beimel.

Efficient generation of shared RSA keys.
Crypto 1997, with D. Boneh.

Fair exchange with a semi-trusted third party.
ACM Security 1997, with M. Reiter.

Auditable metering with lightweight security.
Financial Crypto 1997, with D. Malkhi.

Key management in the Omega system.
ACM CCS 1996, with M. Reiter, R. Wright, J. Lacy.

Low exponent RSA with related messages.
Eurocrypt 1996, with D. Coppersmith, J. Patarin, M. Reiter.

Multi-authority secret ballot elections with linear work.
Eurocrypt 1996, with R. Cramer, B. Schoenmakers, M. Yung.

The design and implementation of a secure auction service.
IEEE Oakland 1995, with M. Reiter.

Privacy from partial broadcast.
ACM STOC 1995, with M. Yung.

Verifiable signature sharing.
Eurocrypt 1995, with M. Reiter.

The blinding of weak signatures.
Eurocrypt 1994, with M. Yung.

Eavesdropping games.
IEEE FOCS 1993, with Z. Galil, M. Yung.

Joint encryption and message-efficient secure computation.
Crypto 1993, with S. Haber.

Secure and efficient off-line digital money.
ICALP 1993, with M. Yung.

Communication complexity of secure computation.
ACM STOC 1992, with M. Yung.

Varieties of secure distributed computation.
Sequences II, 1991, with M. Yung.

Contributions and Editions

Proc. CANS 2008, Springer LNCS 5339 (co-editor); Proc. Crypto 2004, Springer LNCS 3152 (editor); Proc. Financial Crypto 1999, Springer LNCS 1648 (editor); Data Security (chapter), Computer Eng. Handbook, CRC Press 2002; Mix Networks (long entry), Encyc. Crypt/Sec, Springer 2005.

Funding Sources

NSF-CT, Practical privacy preserving technologies (with H. Chen), 2008-11.
NSF-ITR, Deployment-oriented security (with Boneh, Reiter), 2002-06.
NSF CAREER, New directions in cryptography for e-commerce, 2001-06.
Packard Foundation Fellowship for Science and Engineering, 2001-08.

Recent Invited Talks

Tsinghua/Shandong Univ 2011; ISAAC 2010 (Jeju Island, Korea); Nanyang Tech Univ 2009; NIST IBE Workshop 2008; Univ Calgary 2007; HP Labs 2006 (Princeton); CANS 2005 (Fujian); Aarhus Univ 2003; École normale supérieure 2002 (5-lecture series); IBM Research 2001 (Zurich); Microsoft Research 2001 (Redmond).

Ph.D. Students

Haibin Zhang 2014, Mark Gondree 2009, Payman Mohassel 2009, Martin Gagne 2008.

Extended Visits and Internships

Tsinghua Univ (Summer 2011); Nanyang Tech Univ (Summer 2010); IPAM, UCLA (Fall 2006); HP Labs, Princeton, NJ (Jan–April 2006); École normale supérieure (March 2002); CWI, Amsterdam (Jan–June 1994); IBM Research, Hawthorne, NY (summer 1993); Bellcore, Morristown, NJ (summer 1992); Bell Labs, Murray Hill, NJ (summer 1991).

Other Professional Activities

Board of Directors, IACR (2009-present,1999-2000); Participant, NAE Frontiers of Engineering (2002); Best Paper Award, NDSS 2001; General Chair, Crypto 2000. Steering Committee, CANS 2005-2011.

Doctoral Thesis Examiner

A. Patra (2010), A. Choudhury (2010), K. Srinathan (2006): I. I. T. Madras; S. Chatterjee (2006): Indian Statistical Institute; J. Monnerat (2006): Ecole Polytechnique Fédérale de Lausanne; M. Koprowski (2003): Aarhus Universitet; E. Bresson (2002): École normale supérieure.

U. S. Patents

9356779/8130964/7634087/7113594 Identity-based encryption, 7421583 Price of crypto services, 7400732 Noninteractive session keys, 7110541 Policy based printing, 7051199 Crypto services, 7006999 Privacy in e-communities, 6990468 Cryptoserver auction, 6970259 Forgery detection, 6938154 Crypto key infrastructure, 6898579 Contract term certification, 6754821 Transition state crypto, 6728376 Encrypting with stencils, 6263436 fair exchange, 6115742 Auditable metering, 6055518 Secure auctions.

Other Professional Experience

1987-89 Thomson-CSF, Inc., Palo Alto, CA.
1985-87 Lockheed Software Technology Center, Palo Alto, CA.
1995-98 co-taught 4 graduate crypto courses at NYU and Columbia.