Full CV, 2023.03.05

Phillip Rogaway

Homepage: https://cs.ucdavis.edu/∼rogaway
Email: `rogaway@pm.me` — mail to rogaway@ucdavis.edu & rogaway@cs.ucdavis.edu forwarded here
Zoom: `https://ucdavis.zoom.us/j/4778298788`
Cell: +1 530 220 4843

California address:
1212 Purdue Dr.
Davis, California 95616 USA

Oregon address:
225 NW 97th Ave.
Portland, OR 97229 USA

Current Position

Professor, Department of Computer Science, University of California, Davis — since 1994

One Shields Avenue
University of California
Davis, CA 95616 USA

Research

Cryptography, Ethics and Technology, Theory of Computation, Privacy

Education

Massachusetts Institute of Technology — 1987–1991
Ph.D. in Electrical Engineering and Computer Science, 1991 — 1985–1986
Advisor: Silvio Micali
Thesis: *The Round Complexity of Secure Protocols*
S.M. in Electrical Engineering and Computer Science, 1988
Thesis: *Everything Provable is Provable in Zero-Knowledge*

University of California, Berkeley — 1980–1984
A.B. in Computer Science, 1985

Visiting Positions

École Normale Supérieure (ENS), Paris, France (2015)
ETH Zürich, Switzerland (2014)
Isaac Newton Institute, Cambridge, UK (2012)
Chiang Mai University, Thailand (1999–2005)
Chulalongkorn University, Bangkok, Thailand (2003)

Stats

h-index: **80** Google Scholar

Number of citations: **40,431** same

Number of CRYPTO/EUROCRYPT/AC papers: **41** Traditional tier-1 venues

Number of papers: **90**

Citation-ranking by research category: Google Scholar

▷ cryptography: **#16**

▷ privacy: **#8**

▷ ethics and technology: **#1**

Awards

▷ **Levchin Prize** (2016). Recipient of the first Levchin prize for real-world cryptography. Citation: "For groundbreaking practice-oriented research that has had an exceptional impact on real-world cryptography"

▷ **PET Award** (2015) (for top paper on privacy enhancing technology). For paper [A76] from CRYPTO 2015

▷ **IACR Fellow** (2012). Citation: "For fundamental contributions to the theory and practice of cryptography and for educational leadership in cryptography."

▷ **UCD CoE Distinguished Teaching Award** (2010). Awarded to a single UC Davis faculty member (from ∼225) in the College of Engineering.

▷ **ACM Paris Kanellakis Theory and Practice Award** (2009). For "specific theoretical accomplishments that have had a significant and demonstrable effect on the practice of computing." Citation: for the "development of the field of practice-oriented provable-security and its widespread impact on the theory and practice of cryptography and security."

▷ **RSA Award for Mathematics** (2003). For "innovation and ongoing contribution to the field of cryptography." Citation: for work that provides "assurances that cryptographic methods employed by implementers are secure"; for "the 'random oracle' model, . . . the primary paradigm for reasoning about the properties of cryptographic methods today"; and for "the introduction of several major methods used in the field today, including Optimal Asymmetric Encryption Padding (OAEP) and the Probabilistic Signature Scheme (PSS)."

▷ **ACM CCS Test of Time Award** (for paper [A36] from CCS 2011)

▷ **NSF CAREER Award** (1996). "Practice-Oriented Provable Security"

Impact

Most cited papers (Citation counts rounded to nearest 100) Google Scholar, 2020

6100	Random oracles are practical: A paradigm for designing efficient protocols (1993)
2200	Entity authentication and key distribution (1994)
1900	Authenticated key exchange secure against dictionary attacks (2000)
1900	OCB: A block-cipher mode of operation for efficient authenticated encryption (2001, 2003)
1700	Optimal asymmetric encryption (1996)
1500	Relations among notions of security for public-key encryption schemes (1998)
1400	A concrete security treatment of symmetric encryption (1997)
1300	The exact security of digital signatures—How to sign with RSA and Rabin (1996)
1300	The security of cipher block chaining (1994, 2000)
1100	The security of triple encryption and a framework for code-based game-playing proofs (2004, 2006)
900	Reconciling two views of cryptography (2000, 2002)
900	The round complexity of secure protocols (1990)
800	secure session key distribution: the three-party case (1995)
800	Cryptographic hash-function basics (2004)
700	The oracle Diffie-Hellman assumptions and an analysis of DHIES (1998, 2001)
700	The security of the cipher block chaining message authentication code (2000)
600	UMAC: Fast and secure message authentication (1999)
600	Authenticated-encryption with associated-data (2002)
600	Foundations of garbled circuits (2012)
500	Secure computation (1992)
500	Black-box analysis of the block-cipher-based hash-function constructions from PGV (2002)
500	Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC (2004)

Standardized schemes ▷ **CMAC** (message authentication): NIST 800-38B, RFC 4494 ▷ **DHIES** (public-key encryption): ANSI X9.63, IEEE P1363a, ISO/IEC 18033-2, SEC ▷ **EAX** (authenticated encryption): ANSI C12.22, ISO/IEC 19772 ▷ **EME2** (wide-block blockcipher): IEEE 1619.2 ▷ **FF1** (format-preserving encryption): NIST 800-38G ▷ **OAEP** (public-key encryption): ANSI X9.44, CRYPTREC, ISO/IEC 18033-2, RFC 3447, RFC 3560, RSA PKCS #1, v.2.1, SET ▷ **OCB** (authenticated encryption): RFC 7253, CAESAR ▷ **PSS** (digital signatures): ANSI X9.31, CRYPTREC, IEEE P1363a; ISO/IEC 9796-2, NESSIE, RFC 3447, RSA PKCS #1 v2.1 ▷ **SIV** (misuse-resistant authenticated encryption) RFC 5297 ▷ **UMAC** (message authentication): ISO/IEC 19772, NESSIE, RFC 4418 ▷ **XTS** (tweakable blockcipher): IEEE P1619.

Coverage in books Examples include: *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*, by Blanchette; *Protocols for Authentication and Key Establishment*, by Boyd and Mathuria; *Introduction to Cryptography*, by Buchmann; *Practical Signcryption*, by Dent, Zheng, and Yung; *Practical Cryptography*, by Ferguson and Schneier; *Foundations of Cryptography*, by Goldreich; *Introduction to Modern Cryptography*, by Katz and Lindell; *Handbook of Applied Cryptography*, by Menezes, Van Oorschott and Vanstone; *Modeling and Analysis of Security Protocols*, by Ryan and Schneider; *Applied Cryptography*, by Schneier; *Network Security, Principles and Practices*, by Stallings; *Cryptography Theory and Practice*, by Stinson; *Encyclopedia of Cryptography and Security*, by Tilborg; *A Classical Introduction to Cryptography*, by Vaudenday.

Introduced, formalized, or popularized ▷ algorithm-substitution attacks ▷ authenticated encryption ▷ concrete security analysis ▷ coupling arguments in cryptography ▷ cryptographic hash functions ▷ formal analysis of modes of operation ▷ formal cryptography *vs.* computation cryptography ▷ format-preserving encryption ▷ garbling schemes ▷ game-playing proofs ▷ ideal-cipher model ▷ misuse-resistant authenticated-encryption ▷ random-oracle model ▷ random-permutation model ▷ symmetric encryption

Publications

A1. M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali and P. Rogaway. EVERYTHING PROVABLE IS PROVABLE IN ZERO-KNOWLEDGE. *Advances in Cryptology — CRYPTO '88*, Lecture Notes in Computer Science, vol. 403, Springer, pp. 37–56, 1988.

A2. D. Beaver, S. Micali and P. Rogaway. THE ROUND COMPLEXITY OF SECURE PROTOCOLS. *Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing* (STOC 90), pp. 503–513, 1990.

A3. D. Beaver, J. Feigenbaum and J. Kilian and P. Rogaway. SECURITY WITH LOW COMMUNICATION OVERHEAD. *Advances in Cryptology — CRYPTO '90*, Lecture Notes in Computer Science, vol. 537, Springer, pp. 62–76, 1990.

A4. S. Micali and P. Rogaway. SECURE COMPUTATION. *Advances in Cryptology — CRYPTO '91*, Lecture Notes in Computer Science, vol. 576, Springer, pp. 392–404, 1991.

A5. M. Bellare and P. Rogaway. THE COMPLEXITY OF APPROXIMATING A NONLINEAR PROGRAM. *Complexity in Numerical Optimization*, Panos Pardalos, ed., World Scientific, pp. 16–32, 1993.

A6. M. Bellare and P. Rogaway. RANDOM ORACLES ARE PRACTICAL: A PARADIGM FOR DESIGNING EFFICIENT PROTOCOLS. *First ACM Conference on Computer and Communications Security*, pp. 62–73, 1993.

A7. M. Bellare and P. Rogaway. ENTITY AUTHENTICATION AND KEY DISTRIBUTION. *Advances in Cryptology — CRYPTO '93*, Lecture Notes in Computer Science, vol. 773, Springer, pp. 232-249, 1993.

A8. P. Rogaway and D. Coppersmith. A SOFTWARE-OPTIMIZED ENCRYPTION ALGORITHM. *Fast Software Encryption*, Lecture Notes in Computer Science, vol. 809, Springer, pp. 56–63, 1994.

A9. M. Bellare, J.Kilian and P. Rogaway. THE SECURITY OF CIPHER BLOCK CHAINING. *Advances in Cryptology — CRYPTO '94*, Lecture Notes in Computer Science, vol. 839, Springer, pp. 341–358, 1994.

A10. M. Bellare and P. Rogaway. OPTIMAL ASYMMETRIC ENCRYPTION. *Advances in Cryptology — EUROCRYPT '94*, Lecture Notes in Computer Science, vol. 950, Springer, pp. 92–111, 1994.

A11. M. Bellare and P. Rogaway. PROVABLY SECURE SESSION KEY DISTRIBUTION — THE THREE PARTY CASE. *Proceedings of the Twenty Seventh Annual ACM Symposium on the Theory of Computing* (STOC 95), pp. 57–66, 1995.

A12. M. Bellare, R. Guérin and P. Rogaway. XOR MACs: NEW METHODS FOR MESSAGE AUTHENTICATION USING FINITE PSEUDORANDOM FUNCTIONS. *Advances in Cryptology —CRYPTO '95.* Lecture Notes in Computer Science, vol. 963, Springer, pp. 15–28, 1995.

A13. P. Rogaway. BUCKET HASHING AND ITS APPLICATION TO FAST MESSAGE AUTHENTICATION. *Advances in Cryptology —CRYPTO '95*, Lecture Notes in Computer Science, vol. 963, Springer, pp. 29–42, 1995.

Publications

A14. M. Bellare and P. Rogaway. THE COMPLEXITY OF APPROXIMATING A NONLINEAR PROGRAM. *Mathematical Programming*, vol. 69, No. 3, pp. 429–441, 1995.

A15. M. Bellare and P. Rogaway. THE EXACT SECURITY OF DIGITAL SIGNATURES — HOW TO SIGN WITH RSA AND RABIN. *Advance in Cryptology — EUROCRYPT '96,* Lecture Notes in Computer Science, vol. 1070, Springer, pp. 399–416, 1996.

A16. J. Kilian and P. Rogaway. HOW TO PROTECT DES AGAINST EXHAUSTIVE KEY SEARCH. *Advances in Cryptology — CRYPTO '96*, Lecture Notes in Computer Science, vol. 1109, Springer, pp. 252–267, 1996.

A17. P. Rogaway. THE SECURITY OF DESX. RSA Laboratories' *CryptoBytes*, vol. 2, no. 2, 1996.

A18. D. Beaver, J. Feigenbaum, J. Kilian and P. Rogaway. LOCALLY RANDOM REDUCTIONS: IMPROVEMENTS AND APPLICATIONS. *Journal of Cryptology,* vol. 10, no. 1, pp. 17-36, 1997.

A19. M. Bellare and P. Rogaway. COLLISION-RESISTANT HASHING: TOWARDS MAKING UOWHFs PRACTICAL. *Advances in Cryptology — CRYPTO '97*, Lecture Notes in Computer Science, vol. 1294, Springer, pp. 470–484, 1997.

A20. M. Bellare, A. Desai, E. Jokipii and P. Rogaway. A CONCRETE SECURITY TREATMENT OF SYMMETRIC ENCRYPTION. *38th Annual Symposium on Foundations of Computer Science* (FOCS '97), pp. 394–403, October 1997.

A21. M. Bellare and P. Rogaway. MINIMIZING THE USE OF RANDOM ORACLES IN AUTHENTICATED ENCRYPTION SCHEMES. *International Conference on Information and Communications Security*, Lecture Notes in Computer Science, vol. 1334, Springer, pp. 1–16. November 1997.

A22. P. Rogaway and D. Coppersmith. A SOFTWARE-OPTIMIZED ENCRYPTION ALGORITHM. *Journal of Cryptology*, vol. 11, no. 4, pp. 273–287, 1998. (Journal version of A8.)

A23. P. Rogaway. BUCKET HASHING AND ITS APPLICATION TO FAST MESSAGE AUTHENTICATION. *Journal of Cryptology*, vol. 12, no. 2, pp. 91–115, 1998. (Journal version of A13.)

A24. M. Bellare, T. Krovetz and P. Rogaway. LUBY-RACKOFF BACKWARDS: INCREASING SECURITY BY MAKING BLOCK CIPHERS NON-INVERTIBLE. *Advances in Cryptology — EUROCRYPT '98.* Lecture Notes in Computer Science, vol. 1403, K. Nyberg, ed., Springer, pp. 266–280, 1998.

A25. M. Bellare, A. Desai, D. Pointcheval and P. Rogaway. RELATIONS AMONG NOTIONS OF SECURITY FOR PUBLIC-KEY ENCRYPTION. *Advances in Cryptology — CRYPTO '98*, Lecture Notes in Computer Science, vol. 1462, H. Krawczyk, ed., Springer, pp. 26–45, 1998.

A26. M. Bellare and P. Rogaway. ON THE CONSTRUCTION OF VARIABLE-INPUT-LENGTH CIPHERS. *Fast Software Encryption, 6th International Workshop–FSE '99*, Lecture Notes in Computer Science, vol. 1636. Springer, pp. 231–244, 1999.

Publications

A27. J. Black, S. Halevi, H. Krawczyk, T. Krovetz and P. Rogaway. UMAC: FAST AND SECURE MESSAGE AUTHENTICATION. *Advances in Cryptology — CRYPTO '99.* Lecture Notes in Computer Science, vol. 1666, M. Wiener, ed., Springer, pp. 216–233.

A28. M. Bellare, J. Kilian and P. Rogaway. THE SECURITY OF THE CIPHER BLOCK CHAINING MESSAGE AUTHENTICATION CODE. *Journal of Computer and System Sciences* (JCSS), vol. 61, No. 3, pp. 362–399, December 2000. (Journal version of A9.)

A29. M. Abadi and P. Rogaway. RECONCILING TWO VIEWS OF CRYPTOGRAPHY (THE COMPUTATIONAL SOUNDNESS OF FORMAL ENCRYPTION). *IFIP International Conference on Theoretical Computer Science,* Lecture Notes in Computer Science, vol. 1872, pp. 3–22. Springer, 2000.

A30. T. Krovetz and P. Rogaway. FAST UNIVERSAL HASHING WITH SMALL KEYS AND NO PREPROCESSING: THE POLYR CONSTRUCTION. *Information Security and Cryptology — ICICS 2000.* Lecture Notes in Computer Science, vol. 2015, pp. 73–89, D.H. Won, ed., Springer, 2000. Seoul, South Korea, December 2000.

A31. M. Bellare, D. Pointcheval and P. Rogaway. AUTHENTICATED KEY EXCHANGE SECURE AGAINST DICTIONARY ATTACKS. *Advances in Cryptology — Eurocrypt '00.* Lecture Notes in Computer Science, vol. 1807, B. Preneel, ed., Springer, pp. 139–155, 2000.

A32. J. Black and P. Rogaway. CBC MACS FOR ARBITRARY-LENGTH MESSAGES: THE THREE-KEY CONSTRUCTIONS. *Advances in Cryptology — CRYPTO 00.* Lecture Notes in Computer Science, vol. 1880, M. Bellare, ed., Springer, pp. 197–215, 2000.

A33. M. Bellare and P. Rogaway. ENCODE-THEN-ENCIPHER ENCRYPTION: HOW TO EXPLOIT NONCES OR REDUNDANCY IN PLAINTEXTS FOR EFFICIENT CRYPTOGRAPHY. *Advances in Cryptology — ASIACRYPT 2000.* Lecture Notes in Computer Science, vol. 1976 pp. 317–330, T. Okamoto, ed., Springer, 2000.

A34. J. Kilian and P. Rogaway. HOW TO PROTECT DES AGAINST EXHAUSTIVE KEY SEARCH (AN ANALYSIS OF DESX). *Journal of Cryptology*, vol. 14, no. 1, pp. 17–35, 2001. (Journal version of A16.)

A35. M. Abdalla, M. Bellare, and P. Rogaway. THE ORACLE DIFFIE-HELLMAN ASSUMPTION AND AN ANALYSIS OF DHIES. *Topics in Cryptology — CT-RSA 2001.* Lecture Notes in Computer Science, vol. 2020, pp. 143–158, D. Naccache (ed.), Springer 2001.

A36. P. Rogaway, M. Bellare, J. Black, and T. Krovetz. OCB: A BLOCK-CIPHER MODE OF OPERATION FOR EFFICIENT AUTHENTICATED ENCRYPTION. *ACM Conference on Computer and Communications Security* (CCS-8). pp. 195–205, ACM Press, 2001.

A37. M. Abadi and P. Rogaway. RECONCILING TWO VIEWS OF CRYPTOGRAPHY (THE COMPUTATIONAL SOUNDNESS OF FORMAL ENCRYPTION). *Journal of Cryptology*, vol. 15, no. 2, pp. 103-127, 2002. (Journal version of A29.)

A38. J. Black and P. Rogaway. CIPHERS WITH ARBITRARY FINITE DOMAINS. *Topics in Cryptology — CT-RSA 2002.* Lecture Notes in Computer Science, vol. 2271, Springer, pp. 114-130, 2002.

A39. J. Black and P. Rogaway. A BLOCK-CIPHER MODE OF OPERATION FOR PARALLELIZABLE MESSAGE AUTHENTICATION. *Advances in Cryptology — Eurocrypt 2002.* Lecture Notes in Computer Science, vol. 2332, Springer, pp. 384-397, 2002.

Publications

A40. J. Black and P. Rogaway and T. Shrimpton. ENCRYPTION-SCHEME SECURITY IN THE PRESENCE OF KEY-DEPENDENT MESSAGES. *Selected Areas in Cryptography — SAC 2002.* Lecture Notes in Computer Science, vol. 2595, Springer, pp. 62–75, 2002.

A41. J. Black and P. Rogaway and T. Shrimpton. BLACK-BOX ANALYSIS OF THE BLOCK-CIPHER-BASED HASH-FUNCTION CONSTRUCTIONS FROM PGV. *Advance in Cryptology — CRYPTO '02,* Lecture Notes in Computer Science, vol. 2442, pp. 320-335 Springer, 2002.

A42. P. Rogaway. AUTHENTICATED-ENCRYPTION WITH ASSOCIATED-DATA. *ACM Conference on Computer and Communications Security* (CCS-9). ACM Press, 2002.

A43. S. Halevi and P. Rogaway. A TWEAKABLE ENCIPHERING MODE. *Advance in Cryptology — CRYPTO 03.* Lecture Notes in Computer Science, vol. 2729, D. Boneh, ed., pp. 482–499, Springer, 2003.

A44. P. Rogaway, M. Bellare, and J. Black OCB: A BLOCK-CIPHER MODE OF OPERATION FOR EFFICIENT AUTHENTICATED ENCRYPTION. *ACM Transactions on Information Systems and Security* (ACM TISSEC), vol. 6, no. 3, pp. 365–403, 2003. Journal version of A36.

A45. S. Halevi and P. Rogaway. A PARALLELIZABLE ENCIPHERING MODE. *Topics in Cryptology — CT-RSA 2004.* Lecture Notes in Computer Science, vol. 2964, T. Okamoto, ed., Springer, pp. 292–304, 2004.

A46. M. Bellare, P. Rogaway, and D. Wagner. THE EAX MODE OF OPERATION. *Fast Software Encryption*, Lecture Notes in Computer Science, vol. 3017, Springer, pp. 389–407, 2004.

A47. P. Rogaway. NONCE-BASED SYMMETRIC ENCRYPTION. *Fast Software Encryption*, Lecture Notes in Computer Science, vol. 3017, Springer, pp. 348–359, 2004.

A48. P. Rogaway and T. Shrimpton. CRYPTOGRAPHIC HASH-FUNCTION BASICS: DEFINITIONS, IMPLICATIONS, AND SEPARATIONS FOR PREIMAGE RESISTANCE, SECOND-PREIMAGE RESISTANCE, AND COLLISION-RESISTANCE. *Fast Software Encryption*, Lecture Notes in Computer Science, vol. 3017, Springer, pp. 371–388, 2004.

A49. P. Rogaway and T. Shrimpton. ON THE ROLE OF DEFINITIONS IN AND BEYOND CRYPTOGRAPHY. *Advances in Computer Science — ASIAN 2004.* Lecture Notes in Computer Science, vol. 3321, Springer, pp. 13–32, 2004.

A50. P. Rogaway. EFFICIENT INSTANTIATIONS OF TWEAKABLE BLOCKCIPHERS AND REFINEMENTS TO MODES OCB AND PMAC. *Advances in Cryptology — ASIACRYPT 2004.* Lecture Notes in Computer science, vol. 3329, Springer, pp. 16-31, 2004.

A51. J. Black and P. Rogaway. CBC MACs FOR ARBITRARY-LENGTH MESSAGES: THE THREE-KEY CONSTRUCTIONS. *J. Cryptology*, vol. 18, no. 2, pp. 111–131, 2005. (See also A32)

A52. M. Bellare, K. Pietrzak, and P. Rogaway. IMPROVED SECURITY ANALYSES FOR CBC MACs. *Advances in Cryptology —CRYPTO 2005.* Lecture Notes in Computer Science, vol. 3621, pp. 527–545, 2005.

Publications

A53. T. Krovetz and P. Rogaway. VARIATIONALLY UNIVERSAL HASHING. *Information Processing Letters* (IPL), vol. 100, no. 1, Elsevier Scientific, pp. 36–39, 2006.

A54. P. Rogaway. FORMALIZING HUMAN IGNORANCE: COLLISION-RESISTANT HASHING WITHOUT THE KEYS. *Vietcrypt 2006*, Lecture Notes in Computer Science, vol. 4341, Springer, pp. 211–228, 2007.

A55. M. Bellare and P. Rogaway. THE SECURITY OF TRIPLE ENCRYPTION AND A FRAMEWORK FOR CODE-BASED GAME-PLAYING PROOFS. *Advances in Cryptology — EUROCRYPT 2006.* Lecture Notes in Computer Science, vol. 4004, Springer, pp. 409–426, 2006.

A56. P. Rogaway and T. Shrimpton. A PROVABLE-SECURITY TREATMENT OF THE KEY-WRAP PROBLEM. *Advances in Cryptology — EUROCRYPT 2006.* Lecture Notes in Computer Science, vol. 4004, Springer, pp. 373–390, 2006.

A57. P. Rogaway and T. Ristenpart. HOW TO ENRICH THE MESSAGE SPACE OF A CIPHER. *Fast Software Encryption 2007 (FSE).* Lecture Notes in Computer Science, vol. 4593, Springer, pp. 101–118, 2007

A58. M. Bellare and P. Rogaway. ROBUST COMPUTATIONAL SECRET SHARING AND A UNIFIED ACCOUNT OF CLASSICAL SECRET-SHARING GOALS. *ACM Computer and Communications Security 2007 (ACM CCS).* ACM Press, 2007.

A59. P. Rogaway and J. Steinberger. SECURITY/EFFICIENCY TRADEOFFS FOR PERMUTATION-BASED HASHING. *Advances in Cryptology — EUROCRYPT 2008.* Lecture Notes in Computer Science, vol. 4965, Springer, pp. 220–236, 2008.

A60. P. Rogaway and J. Steinberger. CONSTRUCTING CRYPTOGRAPHIC HASH FUNCTIONS FROM FIXED-KEY BLOCKCIPHERS. *Advances in Cryptology — CRYPTO 2008.* Lecture Notes in Computer Science, vol. 5157, pp. 433–450, Springer, 2008.

A61. M. Bellare, T. Ristenpart, and P. Rogaway. FORMAT-PRESERVING ENCRYPTION. *Selected Areas in Cryptography* (SAC 2009). Lecture Notes in Computer Science, vol. 5867, Springer, pp. 295–312, 2009.

A62. P. Rogaway and T. Stegers. AUTHENTICATION WITHOUT ELISION: PARTIALLY SPECIFIED PROTOCOLS, ASSOCIATED DATA, AND CRYPTOGRAPHIC MODELS DESCRIBED BY CODE. *Computer Security Foundations Symposium — CSF 2009.* IEEE Press, pp. 26–39, 2009.

A63. B. Morris, P. Rogaway, and T. Stegers. HOW TO ENCIPHER MESSAGES ON A SMALL DOMAIN: DETERMINISTIC ENCRYPTION AND THE THORP SHUFFLE. *Advances in Cryptology — CRYPTO 2009.* Lecture Notes in Computer Science, vol. 5677, Springer, 2009.

A64. V. Hoang and P. Rogaway. ON GENERALIZED FEISTEL NETWORKS. *Advances in Cryptology — CRYPTO 2010.* Lecture Notes in Computer Science, vol. 6223, Springer, pp. 613–630, 2010.

A65. J. Black, P. Rogaway, T. Shrimpton, and M. Stam: AN ANALYSIS OF THE BLOCKCIPHER-BASED HASH FUNCTIONS FROM PGV. *Journal of Cryptology*, 23(4), pp. 519–545, 2010.

A66. T. Krovetz and P. Rogaway. THE SOFTWARE PERFORMANCE OF AUTHENTICATED-ENCRYPTION MODES. *Fast Software Encryption* (FSE) 2011. Lecture Notes in Computer Science, vol. 6733, Springer, pp. 306–327, 2011.

Publications

A67. P. Rogaway and H. Zhang. ONLINE CIPHERS FROM TWEAKABLE BLOCKCIPHERS. *Topics in Cryptology — CT-RSA 2011.* Lecture Notes in Computer Science, vol. 6558, pp. 237–249, 2011.

A68. P. Rogaway. CONSTRUCTING CRYPTOGRAPHIC DEFINITIONS. *The ISC International Journal of Information Security*, 3(2), July 2011.

A69. P. Rogaway, M. Wooding, and H. Zhang. THE SECURITY OF CIPHERTEXT STEALING. *Fast Software Encryption* (FSE 2012), Springer, pp. 180–195, 2012.

A70. V. Hoang, B. Morris, and P. Rogaway. AN ENCIPHERING SCHEME BASED ON A CARD SHUFFLE. *Advances in Cryptology — CRYPTO 2012.* Lecture Notes in Computer Science, vol. 7417, Springer, pp. 1–13, 2012.

A71. M. Bellare, V. Hoang, and P. Rogaway. FOUNDATIONS OF GARBLED CIRCUITS. *ACM Conference on Computer and Communications Security* (CCS 2012), ACM Press, pp. 784–796, 2012.

A72. M. Bellare, V. Hoang, and P. Rogaway. ADAPTIVELY SECURE GARBLING WITH APPLICATIONS TO ONE-TIME PROGRAMS AND SECURE OUTSOURCING. *Advances in Cryptology — ASIACRYPT 2012.* Lecture Notes in Computer Science, vol. 7658, Springer, pp. 134–153, 2012.

A73. M. Bellare, V. Hoang, S. Keelveedhi, and P. Rogaway. EFFICIENT GARBLING FROM A FIXED-KEY BLOCKCIPHER. *IEEE Security and Privacy 2013*, IEEE Press, 2013.

A74. B. Morris and P. Rogaway. SOMETIMES-RECURSE SHUFFLE: ALMOST-RANDOM PERMUTATIONS IN LOGARITHMIC EXPECTED TIME. *Advances in Cryptology — EUROCRYPT 2014.* Springer, pp. 311–326, 2014.

A75. C. Namprempre, P. Rogaway, and T. Shrimpton. RECONSIDERING GENERIC COMPOSITION. *Advances in Cryptology — EUROCRYPT 2014.* Springer, pp. 257–274, 2014.

A76. M. Bellare, K. Paterson, and P. Rogaway. SECURITY OF SYMMETRIC ENCRYPTION AGAINST MASS SURVEILLANCE. *Advances in Cryptology — CRYPTO 2014, Part 1.* Springer, pp. 1–19, 2014.

A77. C. Badertscher, C. Matt, U. Maurer, P. Rogaway, and B. Tackmann. AUGMENTED SECURE CHANNELS AND THE GOAL OF THE TLS 1.3 RECORD LAYER. *Provable Security — ProvSec 2015.* Springer, pp. 85–104, 2015.

A78. C. Badertscher, C. Matt, U. Maurer, P. Rogaway, and B. Tackmann. ROBUST AUTHENTICATED ENCRYPTION AND THE LIMITS OF SYMMETRIC CRYPTOGRAPHY. *Cryptography and Coding — IMA International Conference.* Springer, pp. 112–129, 2015.

A79. V. Hoang, T. Krovetz, and P. Rogaway. ROBUST AUTHENTICATED-ENCRYPTION: AEZ AND THE PROBLEM THAT IT SOLVES. *Advances in Cryptology — EUROCRYPT 2015, Part 1.* Springer, pp. 15–44, Springer, 2015.

A80. V. Hoang, R. Reyhanitabar, P. Rogaway, and D. Vizár. ONLINE AUTHENTICATED-ENCRYPTION AND ITS NONCE-REUSE MISUSE-RESISTANCE. *Advances in Cryptology — CRYPTO 2015, Part 1.* Springer, pp. 493–517, 2015.

Publications

A81. B. Preneel, P. Rogaway, M. Ryan, P. Ryan: PRIVACY AND SECURITY IN AN AGE OF SURVEILLANCE. Dagstuhl Perspectives Workshop 14401. Dagstuhl Manifestos 5(1), pp. 25–37, 2015.

A82. M. Bellare, D. Kane, and P. Rogaway. BIG-KEY SYMMETRIC ENCRYPTION: RESISTING KEY EXFILTRATION. *Advances in Cryptology — CRYPTO 2016, Part 1.* Springer, pp. 373-402, 2016.

A83. Phillip Rogaway: PRACTICE-ORIENTED PROVABLE SECURITY AND THE SOCIAL CONSTRUCTION OF CRYPTOGRAPHY. *IEEE Security & Privacy* 14(6), pp. 10–17, 2016.

A84. Phillip Rogaway and Yusi Zhang. SIMPLIFYING GAME-BASED DEFINITIONS: INDISTINGUISHABILITY UP TO CORRECTNESS AND ITS APPLICATION TO STATEFUL AE. *CRYPTO*(2), pp. 3–32, 2018.

A85. Phillip Rogaway and Yusi Zhang: ONION-AE: FOUNDATIONS OF NESTED ENCRYPTION. PoPETs 2018(2), pp. 85–104, 2018.

A86. Ben Morris, Phillip Rogaway, and Till Stegers. DETERMINISTIC ENCRYPTION WITH THE THORP SHUFFLE. *J. of Cryptology*, 31(2), pp. 521–536, 2018.

A87. Anonymous AE. *ASIACRYPT* (2) 2019, pp. 183–208, 2019.

A88. Mihir Bellare, Wei Dai, and Phillip Rogaway. REIMAGINING SECRET SHARING: CREATING A SAFER AND MORE VERSATILE PRIMITIVE BY ADDING AUTHENTICITY, CORRECTING ERRORS, AND REDUCING RANDOMNESS REQUIREMENTS. *Proc. Priv. Enhancing Technol.* (PETS), 2020(4), pp. 461–490, 2020.

A89. Ted Krovetz and Phillip Rogaway. THE DESIGN AND EVOLUTION OF OCB. *J. of Cryptology*, 34(4), 36 pages, 2021.

A90. John Chan and Phillip Rogaway. ON COMMITTING AUTHENTICATED-ENCRYPTION. *ESORICS* (2), pp. 275–294, 2022.

Patents

H1. D. Coppersmith and P. Rogaway. SOFTWARE-EFFICIENT PSEUDORANDOM FUNCTION AND THE USE THEREOF FOR ENCRYPTION. US Patent #5,454,039. September 26, 1995.

H2. P. Rogaway. METHOD AND APPARATUS FOR ENTITY AUTHENTICATION AND KEY DISTRIBUTION SECURE AGAINST OFF-LINE ADVERSARIAL ATTACK. US Patent #5,491,749. February 13, 1996.

H3. M. Bellare and P. Rogaway. METHOD AND APPARATUS FOR THREE-PARTY ENTITY AUTHENTICATION AND KEY DISTRIBUTION USING MESSAGE AUTHENTICATION CODES. US Patent #5,491,750. February 13, 1996.

H4. P. Rogaway. SOFTWARE-EFFICIENT MESSAGE AUTHENTICATION. US Patent #5,651,069. July 22, 1997.

H5. M. Bellare, R. Guérin and P. Rogaway. METHOD AND APPARATUS FOR DATA AUTHENTICATION IN A DATA COMMUNICATION ENVIRONMENT. US Patent #5,673,318. September 30, 1997.

H6. M. Bellare and P. Rogaway. BLOCK CIPHER MODE OF OPERATION FOR SECURE, LENGTH-PRESERVING ENCRYPTION. US Patent #5,673,319. September 30, 1997.

H7. M. Coppersmith and P. Rogaway. COMPUTER READABLE DEVICE IMPLEMENTING A SOFTWARE-EFFICIENT PSEUDORANDOM FUNCTION. US Patent #5,675,652. October 7, 1997.

H8. B. Blakley and P. Rogaway. METHOD TO PROTECT INFORMATION ON A COMPUTER STORAGE DEVICE. US Patent #5,677,952. October 14, 1997.

H9. M. Bellare, P. Guérin, and P. Rogaway. METHOD AND APPARATUS FOR DATA AUTHENTICATION IN A DATA COMMUNICATION ENVIRONMENT. US Patent #5,757,913, May 26, 1998 (See also H5)

H10. D. Coppersmith, and P. Rogaway. SOFTWARE-EFFICIENT PSEUDORANDOM FUNCTION AND THE USE THEREOF FOR DECRYPTION. US Patent #5,835,597. November 10, 1998. (See also H1)

H11. M. Bellare, and P. Rogaway. PROBABILISTIC SIGNATURE SCHEME. US Patent #6,266,771. July 24, 2001.

H12. M. Bellare, and P. Rogaway. PROBABILISTIC SIGNATURE SCHEME. US Patent #7,036,014. April 25, 2006. (See also H11)

H13. P. Rogaway. METHOD AND APPARATUS FOR FACILITATING EFFICIENT AUTHENTICATED ENCRYPTION. US Patent #7,046,802. May 16, 2006.

H14. P. Rogaway. METHOD AND APPARATUS FOR FACILITATING EFFICIENT AUTHENTICATED ENCRYPTION. US Patent #7,200,227. April 3, 2007.

H15. M. Bellare and P. Rogaway. METHOD AND APPARATUS FOR FACILITATING EFFICIENT AUTHENTICATED ENCRYPTION. US Patent #7,949,129. May 24, 2011.

H16. P. Rogaway. SYSTEMS AND METHODS FOR DISTRIBUTING AND SECURING DATA. US Patent #8,155,322. April 10, 2012.

H17. P. Rogaway. METHOD AND APPARATUS FOR FACILITATING EFFICIENT AUTHENTICATED ENCRYPTION. US Patent #8,321,675. November 27, 2012.

Keynotes & distinguished lectures

K1. RECONCILING TWO VIEWS OF CRYPTOGRAPHY (THE COMPUTATIONAL SOUNDNESS OF FORMAL CRYPTOGRAPHY). Keynote talk at NCSEC 2000, The Fourth National Computer Science and Engineering Conference (NCSEC 2000). Bangkok, Thailand. November 2000.

K2. SOME EXAMPLES FROM PROVABLE-SECURITY CRYPTOGRAPHY. Keynote talk at NCSEC 2002, The Sixth National Computer Science and Engineering Conference. Bangkok, Thailand. October 2002.

K3. ON THE ROLE OF DEFINITIONS IN AND BEYOND CRYPTOGRAPHY. Keynote talk at ASIAN '04, Ninth Asian Computing Science Conference. Invited talk. Chiang Mai, Thailand. December 2004. (See also A49.)

K4. FORMALIZING KNOWLEDGE AND IGNORANCE. Keynote talk at SKIMA — Software Knowledge Information Management and Applications. Chiang Mai, Thailand, December 2006.

K5. BLOCKCIPHER MODES OF OPERATION: CULTURE AND COUNTER-CULTURE IN MODERN CRYPTOGRAPHY. Keynote at ProvSec 2008, Shanghai, China, October 30, 2008.

K6. PRACTICE-ORIENTED PROVABLE SECURITY AND THE SOCIAL CONSTRUCTION OF CRYPTOGRAPHY. Invited talk at EUROCRYPT 2009. Cologne, Germany. April 2009.

K7. ON THE ROLE OF DEFINITIONS IN AND BEYOND CRYPTOGRAPHY. Keynote talk at SBSeg 2009, the Brazilian Symposium on Information and Computer System Security. Campinas, Brazil. September 2010.

K8. CONSTRUCTING CRYPTOGRAPHIC DEFINITIONS. Keynote talk at ISCISC. Mashad, Iran. September 2011.

K9. ABSENCE CAN GO UNNOTICED: SOME LATE-TO-ARRIVE DEFINITIONS IN MODERN CRYPTOGRAPHY. Distinguished Colloquium Series, ETH Zürich. Switzerland. December 10, 2012.

K10. WHY MOST ACADEMIC CRYPTOGRAPHERS DON'T CARE ABOUT REAL-WORLD PROTOCOLS, MASS-SURVEILLANCE, OR ANYTHING ELSE THAT IMPACTS YOUR PRIVACY OR SECURITY. The twenty-fourth Hewlett-Packard Colloquium on Information Security. Royal Holloway — University of London. December 18, 2013.

K11. THE EMERGENCE OF AUTHENTICATED ENCRYPTION. Invited talk at ACNS 2014. Lausanne, Switzerland. June 12, 2014.

K12. WHY MOST ACADEMIC CRYPTOGRAPHERS DON'T CARE ABOUT REAL-WORLD PROTOCOLS, MASS-SURVEILLANCE, OR ANYTHING ELSE THAT IMPACTS YOUR PRIVACY OR SECURITY. Distinguished Lecture Series, UC San Diego, USA. November 10, 2014.

K13. WHY MOST ACADEMIC CRYPTOGRAPHERS DON'T CARE ABOUT REAL-WORLD PROTOCOLS, MASS-SURVEILLANCE, OR ANYTHING ELSE THAT IMPACTS YOUR PRIVACY OR SECURITY. Opening talk on "Surveillance Democracies?" UC Davis, USA. September 22, 2015.

Keynotes & distinguished lectures

K14. THE MORAL CHARACTER OF CRYPTOGRAPHIC WORK. IACR Distinguished Lecture. Auckland, New Zealand. December 2, 2015.

K15. MASS SURVEILLANCE AND THE CRISIS OF SOCIAL RESPONSIBILITY. Public lecture organized by Auckland University, New Zealand. December 9, 2015.

K16. THE MORAL CHARACTER OF CRYPTOGRAPHIC WORK. NSF WATCH talk. Arlington, Virginia, USA. March 24, 2016.

K17. THE MORAL CHARACTER OF CRYPTOGRAPHIC WORK. MIT. Distinguished Lecture at the MIT Institute for Data, Systems, and Society. October 18, 2016.

K18. CRYPTOGRAPHY VS. MASS SURVEILLANCE. Keynote for Crypto vs. Mass Surveillance: The Uneasy Relationship workshop. Event organized in response to my essay "The Moral Character of Cryptographic Work." Trondheim, Norway. November 14, 2016.

K19. THE RISE OF AUTHENTICATED ENCRYPTION. Invited talk at CTCrypt 2018. Suzdal, Russia. May 28, 2018.

Invited talks at conferences & special events

L1. THE COMPLEXITY OF APPROXIMATING A NONLINEAR PROGRAM. Invited talk at the Fourth SIAM Conference on Optimization, Chicago, Illinois, USA. May 1992. (See also A5)

L2. PROVABLY-SECURE KEY DISTRIBUTION — THE THREE PARTY CASE. Invited talk at RSA Seminar Series, Redwood City, California, USA. August 1995.

L3. DESIGN AND ANALYSIS OF MESSAGE AUTHENTICATION CODES. Invited talk at the 1996 RSA Data Security Conferences, San Francisco, California, USA. January 1996.

L4. PRACTICE-ORIENTED PROVABLE SECURITY. Invited talk at the 1996 RSA Cryptographers' Colloquium. Palo Alto, California, USA. August 1996.

L5. RANDOM ORACLES AND ASYMMETRIC ENCRYPTION. Invited talk at Public Key Solutions '97. Toronto, Canada. April 1997. (See also A21.)

L6. TARGET COLLISION-RESISTANT HASHING. Invited talk at the 1997 RSA Laboratories Seminar Series. San Francisco, California, USA. August 1997. (See also A21.)

L7. ADVANCES IN DIGITAL SIGNATURES. Invited talk at Public Key Solutions '99. Toronto, Canada. April 1999.

L8. STOPPING DICTIONARY ATTACKS. Invited talk at the Fourth Workshop on Elliptic Curve Cryptography (ECC 2000). Essen, Germany. October 2000.

L9. SOME RECENT WORK ON DESIGNING EFFICIENT MODES OF OPERATION. Invited talk at a meeting of the American Mathematics Society (AMS) and the Sociedad Mathematica Mexicana (SMM), Special Section on Coding Theory and Cryptography. Houston, Texas. May 2004.

L10. SOME RECENT WORK ON DESIGNING BLOCKCIPHER MODES OF OPERATION. Invited talk at RSA Conference Japan. Tokyo, Japan. June 2004.

L11. RECONCILING TWO VIEWS OF CRYPTOGRAPHY. Invited talk at Computational and Symbolic Proofs of Security (CosyProofs 2010). The 37th Spring School on theoretical computer science and French-Japanese collaboration workshop. Barbizon, France, April 2010.

L12. FOUNDATIONS OF GARBLED CIRCUITS. Invited talk at Semantics and Security: A Legacy of Alan Turing; Formal and Computational Cryptographic Proofs. Cambridge, England. April 2012.

L13. THE EVOLUTION OF AUTHENTICATED ENCRYPTION. Invited talk at DIAC – Directions in Authenticated Encryption. Stockholm, Sweden. July 2012.

L14. THE EVOLUTION OF AUTHENTICATED ENCRYPTION. Invited talk at the Workshop on Real World Cryptography. Stanford University. January 2013.

L15. THE EMERGENCE OF AUTHENTICATED ENCRYPTION. Invited talk at ACNS 2014. EPFL. Lausanne, Switzerland. July 2014.

L16. THE RISE OF AUTHENTICATED ENCRYPTION. Invited talk at ZISC 2014. ETH Zurich, Switzerland. September 12, 2014.

L17. A LONG ROAD FROM THEORY TO PRACTICE: THE CASE OF AUTHENTICATED ENCRYPTION. Theory of Cryptography. Tsinghua University. Beijing, China. October 2014.

Invited talks at conferences & special events

L18. ADVANCES IN AUTHENTICATED ENCRYPTION. Invited talk at Indocrypt 2014. New Delhi, India. December 16, 2014.

L19. ONLINE AUTHENTICATED-ENCRYPTION AND ITS NONCE-REUSE MISUSE RESISTANCE. Invited talk to COST CryptoAction IC-1306. Sofia, Bulgaria. April 26, 2015.

L20. ADVANCES IN AUTHENTICATED ENCRYPTION. Invited talk at ProvSec 2015. Kanazawa, Japan. November 24, 2015.

L21. SOME THOUGHTS ON COMMUNITY, RESPONSIBILITY, AND STANDARDS: TEN (RATHER OBVIOUS) CLAIMS. Invited talk at AWACS 2016 (A Workshop about Cryptographic Standards). Vienna, Austria. May 8, 2016.

L22. THE MORAL CHARACTER OF CRYPTOGRAPHIC WORK. Invited talk at USENIX Security. Austin, Texas, USA. August 11, 2016.

L23. THE LONG ROAD FROM THEORY TO PRACTICE: THE CASE OF AUTHENTICATED ENCRYPTION. Invited talk at Bay Area Crypto Day. Palo Alto, California, USA. April 21, 2017.

L24. CAN CRYPTOGRAPHY FRUSTRATE FASCISM? CypherCon 2.0. Milwaukee, Wisconsin, USA. March 30, 2017.

L25. CAN CRYPTOGRAPHY FRUSTRATE FASCISM? Security in Times of Surveillance. Eindhoven, TU/e, Netherlands. May 29, 2017.

L26. AN OBSESSION WITH DEFINITIONS. Latincrypt 2017. University of Havana, La Habana, Cuba. September 20, 2017.

L27. CRYPTOGRAPHERS VIEW OF THE POLITICAL SIGNIFICANCE OF CRYPTOGRAPHY. NextLEAP Presentation. Paris, France, May 5, 2018.

L28. SECRET SHARING FOR JOURNALISTS AND WHISTLEBLOWERS. SPY — Surveillance, Privacy, and You (Eurocrypt 2019 affiliated event). Darmstadt, Germany. May 19, 2019.

Conference talks

M1. EVERYTHING PROVABLE IS PROVABLE IN ZERO-KNOWLEDGE. Presented at CRYPTO '88, Santa Barbara, California, USA. August 1988. (See also A1)

M2. THE ROUND COMPLEXITY OF SECURE PROTOCOLS. Presented at STOC 1990, the Twenty Second Annual ACM Symposium on the Theory of Computing. Baltimore, Maryland, USA. May 1990. (See also A2)

M3. ENTITY AUTHENTICATION AND KEY DISTRIBUTION. Presented at CRYPTO '93, Santa Barbara, California, USA. August 1993. (See also A7)

M4. RANDOM ORACLES ARE PRACTICAL: A PARADIGM FOR DESIGNING EFFICIENT PROTOCOLS. Presented at the ACM CCS (Conference on Computers and Communications Security), Fairfax, Virginia, USA. November 1993. (See also A6)

M5. THE SECURITY OF CIPHER BLOCK CHAINING. Presented at CRYPTO '94, Santa Barbara, California, USA. August 1994. (See also A9)

M6. BUCKET HASHING AND ITS APPLICATION TO FAST MESSAGE AUTHENTICATION. Presented at CRYPTO '95, Santa Barbara, California, USA. August 1995. (See also A23.)

M7. HOW TO PROTECT DES AGAINST EXHAUSTIVE KEY SEARCH. Presented at CRYPTO '96, Santa Barbara, California, USA. August 1996. (See also A16)

M8. COLLISION-RESISTANT HASHING: TOWARDS MAKING UOWHFs PRACTICAL. Presented at CRYPTO '97, Santa Barbara, California, USA. August 1997. (See also A19)

M9. MINIMIZING THE USE OF RANDOM ORACLES IN AUTHENTICATED ENCRYPTION SCHEMES. Presented at ICICS 1997 (International Conference on Information and Communications Security), Beijing, China. November 1997. (See also A21)

M10. AUTHENTICATED KEY EXCHANGE SECURE AGAINST DICTIONARY ATTACKS. Presented at EUROCRYPT 2000. Brugge, Belgium. May 2000. (See also A31.)

M11. OCB: A BLOCK-CIPHER MODE OF OPERATION FOR EFFICIENT AUTHENTICATED ENCRYPTION. Presented at the *ACM Conference on Computer and Communications* (CCS-8). Philadelphia, Pennsylvania, USA. November 2001. (See also A36.)

M12. AUTHENTICATED-ENCRYPTION WITH ASSOCIATED DATA. Presented at the ACM Conference on Computer and Communications Security (CCS-9). Washington D.C., USA. November 2002. (See also A42.)

M13. NONCE-BASED SYMMETRIC ENCRYPTION. Presented at Fast Software Encryption (FSE 2004). Delhi, India. February 2004. (See also A47.)

M14. THE SECURITY OF TRIPLE ENCRYPTION AND A FRAMEWORK FOR CODE-BASED GAME-PLAYING PROOFS —or— CODE-BASED GAME-PLAYING PROOFS AND THE SECURITY OF TRIPLE ENCRYPTION. Presented at EUROCRYPT 2006. St. Petersburg, Russia. May 2006. (See also A54.)

M15. SOMETIMES-RECURSE SHUFFLE: ALMOST-RANDOM PERMUTATIONS IN LOGARITHMIC EXPECTED TIME. EUROCRYPT 2014. Presented at EUROCRYPT 2014. Copenhagen, Denmark. May 2014. (See also A75.)

M16. ONION-AE: FOUNDATIONS OF NESTED ENCRYPTION. Privacy Enhancing Technologies Symposium (PETS 2018). Barcelona, Spain. July 26, 2018.

Workshop talks

N1. THE ROUND COMPLEXITY OF SECURE PROTOCOLS. Presented at the DIMACS Workshop on Cryptography, Princeton, New Jersey, USA. October 1989. (See also A2)

N2. SECURITY WITH LOW COMMUNICATION OVERHEAD. Presented at the DIMACS Workshop on Cryptography, Princeton, New Jersey, USA. October 1990. (See also A3)

N3. SECURE COMPUTATION. Presented at the Colloque Cryptographie, Luminy, France, USA. September 1991. (See also A4)

N4. THE COMPLEXITY OF APPROXIMATING A NONLINEAR PROGRAM. Presented at the Colloque Cryptographie, Luminy, France. September 1991. (See also A5)

N5. ENTITY AUTHENTICATION AND KEY DISTRIBUTION. Presented at the Fourth IBM Security ITL. New York, USA. October 1992. (See also A11)

N6. A SOFTWARE-OPTIMIZED ENCRYPTION ALGORITHM. Presented at the 1993 Cambridge Algorithms Workshop, Cambridge, England. December 1993. (See also A8)

N7. A SOFTWARE-OPTIMIZED ENCRYPTION ALGORITHM. Presented at the Mobile Computing Workshop, Austin, Texas, USA. January 1994.

N8. A CONCRETE SECURITY TREATMENT OF SYMMETRIC ENCRYPTION. Dagstuhl Seminar on Cryptography, Schloss Dagstuhl, Germany. September 1997. (See also A20)

N9. "ACCIDENTS" AND SELECTED OPEN PROBLEMS IN MODERN CRYPTOGRAPHY. Presented at "Cryptography and Mathematics" workshop, Mathematical Sciences Research Institute (MSRI), Berkeley, California, USA. January 1998.

N10. CTR-MODE ENCRYPTION. Presented at the National Institute of Standards (NIST) Modes of Operation Workshop. Baltimore, Maryland, USA. October 2000.

N11. OCB: PARALLELIZABLE AUTHENTICATED ENCRYPTION, AND PMAC: PARALLELIZABLE MESSAGE AUTHENTICATION CODE. Presented at the National Institute of Standards (NIST) Modes of Operation Workshop. Baltimore, Maryland, USA. October 2000.

N12. OCB MODE. Presented to the IEEE 802.11 Standardization Committee. Portland, Oregon, July 2001. Presented again at the Second NIST Modes of Operation Workshop. Santa Barbara, California, USA. August 2001. (See also A36.)

N13. PMAC. Presented at the Second NIST Modes of Operation Workshop. Santa Barbara, California, USA. August 2001. (See also A38.)

N14. SOME RECENT WORK CONSTRUCTING BLOCK-CIPHER MODES OF OPERATION. Presented at the Dagstuhl Seminar on Cryptography, Schloss Dagstuhl, Germany. September 2002.

N15. FORMALIZING HUMAN IGNORANCE. Dagstuhl Seminar on Cryptography, Schloss Dagstuhl, Germany. Wadern, Germany, January 2007.

N16. FORMALIZING HUMAN IGNORANCE and PERMUTATION-BASED CRYPTOGRAPHIC HASHING. Dagstuhl Seminar on Cryptography, Schloss Dagstuhl. Wadern, Germany, September 2007.

N17. FORMAT-PRESERVING ENCRYPTION: HOW TO ENCIPHER CCNs, SSNs, AND THE LIKE. RSA Conference 2010, Applications and Development Track, San Francisco, USA. March 2010.

Workshop talks

N18. GARBLING SCHEMES. Workshop on Theory and Practice of Multiparty Computation. Aarhus University, Denmark. June, 2012.

N19. SOME COMMENTS ON APIs AND CRYPTOGRAPHY. Dagstuhl Seminar on Security APIs, Schloss Dagstuhl. Wadern, Germany. November 2012.

N20. RECONSIDERING GENERIC COMPOSITION. Directions in Authenticated Ciphers — DIAC Workshop 2013. Chicago, Illinois, USA. August 13, 2013.

N20. THE FUTURE OF CRYPTOGRAPHY: REMARKS FOR A PANEL DISCUSSION. Visions of Cryptography: Celebration of the work of Shafi Goldwasser. The Weizmann Institute of Science, Israel. December 12, 2013.

N21. AEZ v2: AUTHENTICATED ENCRYPTION BY ENCIPHERING. Directions in Authenticated Ciphers — DIAC Workshop 2014. Santa Barbara, California. August 23, 2014.

N22. SOME THOUGHTS ON AEZ v.4. Directions in Authenticated Ciphers — DIAC Workshop 2016. Nagoya, Japan. September 27, 2016.

Seminars at universities & institutes

U1. THE ROUND COMPLEXITY OF SECURE PROTOCOLS. Presented at the University of Alaska, Fairbanks, USA. May 1990. (See also A2)

U2. THE ROUND COMPLEXITY OF SECURE PROTOCOLS. Presented at Dartmouth College, Hanover, New Hampshire, USA. August 1990. (See also A2)

U3. SECURE COMPUTATION. Presented at Dartmouth College, Hanover, New Hampshire, USA. December 1990. (See also A4)

U4. THE ROUND COMPLEXITY OF SECURE PROTOCOLS. Presented at the National University of Singapore. September 1991. (See also A2)

U5. THE ROUND COMPLEXITY OF SECURE PROTOCOLS. Presented at the University of Illinois, Urbana, USA. May 1991. (See also A2)

U6. MODERN CRYPTOGRAPHY. Presented at the Asian Institute of Technology (AIT), Bangkok, Thailand. September 1991.

U7. THE COMPLEXITY OF APPROXIMATING A NONLINEAR PROGRAM. Presented at the National University of Singapore. September 1991. (See also A5)

U8. ENTITY AUTHENTICATION AND KEY DISTRIBUTION. Presented at the University of Texas at Austin, USA. October 1993. (See also A7)

U9. MODERN CRYPTOGRAPHY. Series of three lectures presented at Chiang Mai University, Chiang Mai, Thailand. July 1994.

U10. CRYPTOGRAPHY IN THE PRESENCE OF A PUBLIC RANDOM ORACLE. Presented at the Weizmann Institute Seminar on Randomness and Computation, Rehovot, Israel. January 1995.

U11. PROVABLY-SECURE KEY DISTRIBUTION — THE THREE PARTY CASE. Presented at Hong Kong University, Hong Kong. July 1995.

U12. PROVABLY-SECURE KEY DISTRIBUTION — THE THREE PARTY CASE. Presented at Hong Kong University of Science and Technology, Hong Kong. July 1995.

U13. PROVABLY SECURE KEY DISTRIBUTION — THE THREE PARTY CASE. Presented at MIT, Cambridge, Massachusetts, USA. September 1995.

U14. PROVABLY-SECURE SESSION KEY DISTRIBUTION. Presented at Tokyo University, Tokyo, Japan. September 1996. (See also A7, A11)

U15. PROVABLY-SECURE SESSION KEY DISTRIBUTION. Presented at the Japan Advanced Institute of Science and Technology (JAIST), Hokuriku, Japan. September 1996. (See also A7, A11)

U16. PROVABLY-SECURE SESSION KEY DISTRIBUTION. Presented at National Chung Cheng University, Chiayi, Taiwan R.O.C. March 1997. (See also A7, A11)

U17. A CONCRETE SECURITY TREATMENT OF SYMMETRIC ENCRYPTION: ANALYSIS OF THE DES MODES OF OPERATION. Presented at MIT, Cambridge, Massachusetts, USA. December 1997. (See also A20)

U18. INTRODUCTION TO CRYPTOGRAPHY (three lectures). Presented at Chiang Mai University, Chiang Mai, Thailand. August 1998.

U19. LECTURES ON CRYPTOGRAPHY (3 lectures). Presented at Yonsei University. Seoul, South Korea. October 1998.

Seminars at universities & institutes

U20. RECONCILING TWO VIEWS OF CRYPTOGRAPHY (THE COMPUTATIONAL SOUNDNESS OF FORMAL CRYPTOGRAPHY). Presented at MIT, as a joint Theory of Computation Seminar / Information-Security Seminar. Cambridge, Massachusetts, USA. October 2000.

U21. OCB: A BLOCK-CIPHER MODE OF OPERATION FOR EFFICIENT AUTHENTICATED ENCRYPTION. Presented at MIT seminar series. Cambridge, Massachusetts, USA. November 2001. (See also A36.)

U22. PROVABLE SECURITY AS A TOOL FOR PRACTICAL PROTOCOL DESIGN. (three lectures). Presented at the Helsinki University of Science and Technology, Finland. April 2002.

U23. A GLIMPSE OF PROVABLE-SECURITY CRYPTOGRAPHY, and RECONCILING TWO VIEWS OF CRYPTOGRAPHY (THE COMPUTATIONAL SOUNDNESS OF FORMAL ENCRYPTION). Two lectures. Presented at the Institute for Theoretical Physics and Mathematics, Tehran, Iran. May 2003.

U24. PROVABLE SECURITY AS A TOOL FOR DESIGNING PRACTICAL CRYPTOGRAPHIC PROTOCOLS. Three lectures. Presented at Amirkabir University of Technology. Tehran, Iran. May 2003.

U25. WHAT DOES IT MEAN TO COMPUTE? Center for Neuroscience, UC Davis, California, USA. April 2004.

U26. ON THE ROLE OF DEFINITIONS IN AND BEYOND CRYPTOGRAPHY. Math Colloquium, Department of Mathematics, UC Davis, California, USA. May 2005.

U27. THE GAME-PLAYING TECHNIQUE AND ITS APPLICATION TO TRIPLE ENCRYPTION. Portland State University, Oregon, USA. March 2006.

U28. THINKING ABOUT WHAT COMPUTERS CAN'T DO: THREE CELEBRATED IDEAS FROM COMPUTER SCIENCE (1936, 1971, 1982). Invited talk at Mae Fah Lueng University. Chiang Rai, Thailand. July 2006.

U29. TOPICS IN PROVABLE-SECURITY CRYPTOGRAPHY: LECTURE 1 — MESSAGE AUTHENTICATION — PROVABLY-SECURE BLOCKCIPHER-BASED MACs; LECTURE 2 — ON THE FORMALIZATION OF COLLISION-BASED HASHING; LECTURE 3 — AUTHENTICATED ENCRYPTION — DEFINITIONS, METHODS, AND PROOFS. Eight hours of invited lectures for at NSRI, Korea. Daejeon, South Korea. October 2006.

U30. CODE-BASED GAME-PLAYING PROOFS AND THE SECURITY OF TRIPLE ENCRYPTION. Invited lecture to Korea University. Seoul, South Korea. October 2006.

U31. FORMALIZING KNOWLEDGE AND IGNORANCE. University of Moratuwa. Mount Lavinia, Sri Lanka. July 14, 2007.

U32. CODE-BASED GAME-PLAYING PROOFS AND THE SECURITY OF TRIPLE ENCRYPTION. Presented at MIT (CIS seminar series). Cambridge, Massachusetts, USA. October 19, 2007.

U33. PRACTICE-ORIENTED PROVABLE SECURITY AND THE SOCIAL CONSTRUCTION OF CRYPTOGRAPHY. Calgary, Canada. May 22, 2009.

U34. CONSTRUCTING CRYPTOGRAPHIC DEFINITIONS. King Monkut's University of Technology, Thonburi (KMUTT) Bangkok, Thailand. August 23, 2012.

Seminars at universities & institutes

U35. FORMALIZING KNOWLEDGE AND IGNORANCE. Thammasat University. August 29, 2012. (Joint KMUTT/Thammasat lecture; see also U34.)

U36. SOME TRENDS AND IDEA IN MODERN CRYPTOGRAPHY. Mahidol University. August 7, 2013.

U37. RECONCILING TWO VIEWS OF CRYPTOGRAPHY: A DESCRIPTION OF [ABADI-ROGAWAY 2000]. ETH Zurich. October 7, 2014.

U38. FORMAT-PRESERVING ENCRYPTION. ETH Zurich. December 10, 2014.

U39. THE EMERGENCE OF AUTHENTICATED ENCRYPTION. Bern University of Applied Sciences. Biel, Switzerland. December, 2014.

U40. ONLINE AUTHENTICATED-ENCRYPTION AND ITS NONCE-REUSE MISUSE RESISTANCE. Crypto seminar series. ENS Paris, France. June 25, 2015.

U41. FORMAT-PRESERVING ENCRYPTION. Crypto seminar series. ENS Paris, France. July 9, 2015.

U42. THE MORAL CHARACTER OF CRYPTOGRAPHIC WORK: AN ESSAY, ITS GENESIS, AND ITS RECEPTION. UC Berkeley. February 11, 2016.

U43. THE MORAL CHARACTER OF CRYPTOGRAPHIC WORK. University of Michigan. October 12, 2016.

U44. THE MORAL CHARACTER OF CRYPTOGRAPHIC WORK. University of Kentucky, USA. March 23, 2018.

U45. INDISTINGUISHABILITY UP TO CORRECTNESS and ADEPT SECRET-SHARING. Invited talk at EPFL. Lausanne, Switzerland. May 25, 2018.

U46. AN OBSESSION WITH DEFINITIONS. Boise State University. March 27, 2019.

U47. THE MORAL CHARACTER OF CRYPTOGRAPHIC WORK: AN ESSAY, ITS GENESIS, AND ITS RECEPTION. Oregon State University, Corvallis, Oregon, USA. Feb 20, 2020.

U48. ARE WE DOING THE WORK WE SHOULD? (A CRYPTOGRAPHER'S LAMENT). Joint seminar for CS@GSSI/ICE, Italy, and TCS@Reykjavik, Iceland. Virtual. Sept 17, 2020.

U49. BEING A COMPUTER SCIENTIST IN THE ERA OF COLLAPSE. Computer Science Colloquium, Pomona College, USA. Virtual. Nov 5, 2020.

U50. I DISSENT: SURVIVING A CAREER AS A CRYPTOGRAPHER AND COMPUTER SCIENTIST WHILE DISAGREEING WITH MOST EVERYTHING THAT GOES ON IN MY FIELD. Computer Science Colloquium, Reed College, USA. Oct 11, 2022.

Classes at special schools

V1. BASIC CRYPTOGRAPHIC PRIMITIVES. Three lectures. Presented at the Summer school on Distributed Systems and Cryptography, Lipari, Italy. July 1998.

V2. FOUNDATIONS OF APPLICABLE CRYPTOGRAPHY. Two lectures. Presented at Winter School on Chaotic Communications, UC San Diego, San Diego, California, USA. January 1999.

V3. USING PROVABLE SECURITY TO DESIGN PRACTICAL CRYPTOGRAPHIC PROTOCOLS. Four lectures. Presented at the Estonian Winter School in Computer Science. Lahemaa, Estonia. March 2001.

V4. PRACTICAL CRYPTOGRAPHY. Three lectures. Presented at the Summer School on Foundations of Internet Security. Duszniki Zdroj, Poland. June 2002.

V5. SYMMETRIC TECHNIQUES. ECRYPT Summer School on Provable Security. Two 75-minute lectures. Barcelona, Spain. September 2009.

V6. PROVABLY-SECURE SHARED-KEY ENCRYPTION. Penn State Joint Summer Schools on Cryptography and the Principles of Software Security (the one lecture for both groups). June, 2012.

V7. PROVABLY-SECURE SHARED-KEY ENCRYPTION. 12th International School on Foundations of Security Analysis and Design. Two two-hour lectures. Bertinoro, Italy. September 2012.

V8. PROVABLY-SECURE SHARED-KEY ENCRYPTION. International Summer School in Trends in Computing. Three two-hour lectures. Tarragona, Spain, July 2013.

V9. AUTHENTICATED ENCRYPTION (AE). Two one-hour lectures. Sibernik, Croatia. June 7, 2016.

V10. CRAFTING DEFINITIONS. SPOTNIQ (Symmetric Proof Techniques). Bertinoro Italy. July 30, 2018.

Mini-classes taught

W1. DISCRETE MATHEMATICS FOR COMPUTER SCIENCE. Seven lectures, in Thai. Presented to students competing in the International Computer Science Olympiad. Chiang Mai, Thailand. October 2000.

W2. CRYPTOGRAPHY AND NP-COMPLETENESS. Twelve lectures. Presented at Chulalongkorn University, Faculty of Science, Department of Mathematics, Bangkok, Thailand. November–December 2000.

W3. ALGORITHM ANALYSIS AND GRAPH ALGORITHMS. Four lectures, in Thai. Presented to students competing in the International Computer Science Olympiad. Chiang Mai, Thailand, March 2001.

W4. CRYPTOGRAPHY AND COMPUTER SECURITY. Two-day mini-course, 12 hours. Chiang Mai, Thailand. September 2002.

W5. PROSPECTS FOR SECURE COMPUTING. Two-part, seven-hour seminar. PART 1: WHY WE CAN'T BUILD SECURE COMPUTING SYSTEMS. PART 2: CRYPTOGRAPHIC APPROACHES TO IMPROVE SECURITY. Organized by by Mae Fah Lueng University, Chiang Rai, Thailand, and Software Park, Bangkok, Thailand. Lectures in Bangkok, Thailand. August 2005.

Talks at companies & standards bodies

X1. FOUNDATIONS OF EFFICIENT CRYPTOGRAPHY. Presented at RSA Data Security, Redwood City, California, USA. December 1994.

X2. PRACTICE-ORIENTED PROVABLE SECURITY. Series of twelve lectures. Presented at NTT Labs — Yokosuka, Japan. September 1996.

X3. PSS: PROVABLY SECURE ENCODING METHOD FOR DIGITAL SIGNATURES. Presented to an IEEE P1363 Standardization meeting. Santa Barbara, California, USA. August 1998.

X4. PRACTICE-ORIENTED PROVABLE SECURITY AS ILLUSTRATED BY SOME RECENT WORK CONSTRUCTING BLOCK-CIPHER MODES OF OPERATION. Presented to CISCO — Milpitas, California, USA. April 2003.

X5. SOME RECENT WORK ON DESIGNING EFFICIENT MODES OF OPERATION. Presented at IBM — Zurich, Switzerland. January 2004.

X6. SOME RECENT WORK ON DESIGNING EFFICIENT MODES OF OPERATION. Presented at NTT, Yokosuka, Japan. June 2004.

X7. SOME RECENT WORK ON DESIGNING EFFICIENT MODES OF OPERATION. Presented at Intel Corp. Portland, Oregon, USA. April 2005.

X8. THE SECURITY OF TRIPLE ENCRYPTION AND A PROVABLE-SECURITY TREATMENT OF THE KEY-WRAP PROBLEM. Presented at Intel — Portland, Oregon, USA. August 2006.

X9. THE OCB AUTHENTICATED-ENCRYPTION ALGORITHM: draft-krovetz-ocb-03. IETF 83 (Internet Engineering Task Force), CFRG. Paris, France. March 30, 2012.

X10. (1) SOME THOUGHTS ON MASS-SURVEILLANCE AND ON DESIGN INTENDED TO FRUSTRATE IT. (2) RECENT ADVANCES IN FORMAT-PRESERVING ENCRYPTION: THE SWAP-OR-NOT AND SOMETIMES-RECURSE SHUFFLES¿ Voltage Security. Palo Alto, California. October 25, 2013.

Standardized schemes

▷ ANSI C12.22 (pending) — specifies EAX [A46]
▷ ANSI X9.31 — specifies PSS [A15]
▷ ANSI X9.44 — specifies OAEP [A10]
▷ ANSI X9.63 — specifies DHIES [A35]
▷ CRYPTREC — specifies both RSA-OAEP [A10] and RSA-PSS [A15]
▷ IEEE P1363a — specifies DHIES [A35], and PSS / PSS-R [A15]
▷ IEEE P1619 — specifies XTS, which is derivative of XEX [A50]
▷ IEEE P1619.2 (pending) — specifies EME2, which is derivative of EME [A45]
▷ ISO/IEC 18033-2 — specifies OAEP [A10] and ECIES [A35]
▷ ISO/IEC 19772 — specifies OCB2 [A50] (now withdrawn) and EAX [A46]
▷ ISO/IEC 9796-2 — specifies PSS-R [A15]
▷ NESSIE — specifies RSA-PSS [A15] and UMAC [A27]
▷ NIST 800-38B — specifies CMAC, which is derivative of XCBC [A32, A51]
▷ NIST 800-38G — specifies FF1 [A38, A61]
▷ RFC 3447 — specifies RSAES-OAEP [A10], RSASSA-PSS [A15], EMSA-PSS [A15]
▷ RFC 3560 — specifies OAEP [A10]
▷ RFC 3566 — specifies AES-XCBC-MAC-96 [A32, A51]
▷ RFC 4308 — uses AES-XCBC-MAC-96 [A32, A51]
▷ RFC 4418 — specifies UMAC [A27]
▷ RFC 4434 (obsoletes RFC 3664) — specifies AES-XCBC-PRF-128 [A32,A51]
▷ RFC 4494 — specifies AES-CMAC-96, which is derivative of XCBC [A32, A51]
▷ RFC 5297 — specifies SIV [A56]
▷ RFC 7253 — specifies OCB3 [A66]
▷ RSA PKCS #1, v.2.1 — RSAES-OAEP [A10], RSASSA-PSS [A15], EMSA-PSS [A15]
▷ SET — specifies OAEP [A10]

Service

- Member, IACR Board of Directors, 2016, 2017, 2018
- Editorial Board, *Journal of Cryptology*, 2009–2017
- PETs Award Selection Committee, 2016
- Editorial Board, *Information and Computation*, 2005–2010
- Program Committee memberships

    PETS 2018, Mycrypt 2016, TCC 2014, Eurocrypt 2013, DIAC 2012, Crypto 2011 (Program Chair), Eurocrypt 2010, Asiacrypt 2009, FCC 2008, Asiacrypt 2008, ACNS 2007, Asiacrypt 2006, Vietcrypt 2006, FSE 2006, Eurocrypt 2004, PKC 2002, Crypto 2000, Asiacrypt 2000, Crypto 1999, Crypto 1998

- Member, IACR Fellows Committee (2012–2015)
- Chair, IACR Fellows Committee (2015)
- Chair, Campus' Committee on International Studies and Exchanges (2009–2010)
- Chair, Department's Undergraduate Affairs Committee (2008–2018)
- Chair, Department's Committee of Graduate Advisors (2010–2016)
- Chair, Department's Faculty Search Committee (2005–06)
- Organizer, Department's Distinguished Lecture Series (2007–08)
- Member, Department's Faculty Search Committee (various years)

Grant funding

▷ “Crypto-for-Privacy” PI: Phillip Rogaway. NSF CNS 1717542. **$500,000**. Five years: 2018-2022.

▷ “Authenticated ciphers.” PI: Phillip Rogaway. Co-PIs: Dan Bernstein, Kris Gaj. TWC Medium. NSF CNS 1314885. **$233,000**. Four years: 2013–2017.

▷ “Deconstructing encryption.” PI: Phillip Rogaway Co-PIs: Mihir Bellare. TWC medium. NSF CNS 1228890. **$400,000**. Four years: 2012–2016.

▷ “Reimagining cryptography by identifying its culturally-rooted assumptions.” PI: Phillip Rogaway. Co-PIs: Mihir Bellare, Ted Krovetz. TC medium. NSF CNS 0904380. **$850,000**. Five years (with one-year extension): 2009–2014.

▷ “Provable-Security Design and Analysis for Emerging Cryptographic Standards.” PI: Phillip Rogaway. MICRO Grant 97-150, **$64,600** ($20,000 from RSA; $20,000 from Certicom; $24,600 in matching funds) 1997–1998.

▷ “Provable-Security Design and Analysis for IEEE Cryptographic Standards” PI: Phillip Rogaway. MICRO Grant 98-129: **$40,000** From RSA Data Security, Inc., ORINCON Corp., and matching funds. 1998–1999.

▷ “Provable-Security Design and Analysis for IEEE Cryptographic Standards.” PI: Phillip Rogaway. MICRO Grant 99-103: **$36,000** ($20,000 from ORINCON Corp, $16,000 in matching funds.) 1999–2000.

▷ “Practice-Oriented Provable Security.” PI: Phillip Rogaway. NSF CAREER Award CCR-9624560. **$200,000**. Four years: July 1996 – June 2000, extended to 30 June 2002.

▷ “Scalable and Secure Information Republication.” PI: Prem Devanbu. Co-PIs: Michael Gertz, Charles Martel, Phillip Rogaway. NSF ITR Award 0085961. **$786,465**. Four years: 2000–2003.

▷ “Efficient and Proven-Secure Protocols for Message Authentication, Key Exchange, and Other Cryptographic Goals.” PI: Phillip Rogaway. Cisco Systems (University Research Program). **$80,000**. Gift, received November 2000.

▷ “Practice-Oriented Provable Security for Higher-Level Protocols.” PI: Phillip Rogaway. Co-PI: Mihir Bellare. NSF Award 0208842. **$400,000**. Three years: July 2002-June 2005, extended to June 2007.

▷ “A Practice-Oriented Provable-Security Treatment for Some Cryptographic Problems of Contemporary Interest.” PI: Phillip Rogaway. **$75,000/year for each of 2005, 2006, 2007**. Gift, Intel Corporation.

Positions

University of California at Davis, USA 1994–present
Assistant Professor (1994–1997), Associate Professor (1997–2002), Professor (2002–present). Department of Computer Science. Teaching history below.

Private tutoring Weekly tutoring of ∼10 gifted kids, for free, grades 6–12, in mathematics. Public-service. 2019–2022

ETH Zürich, Switzerland 2014
Visiting professor in the Computer Science Department. Six-month leave as a guest in Ueli Maurer's group.

Consultant 1995–present
Private consulting on cryptography. Clients such as IBM, Microsoft, Security First, the government of Japan, a large financial institution, a law firm.

Voltage Security
Member of the Technical Advisory Board. The company has done well productizing format-preserving encryption (notion and methods based on my work). Company acquired by HP (2014).

Chulalongkorn University, Thailand 2002–2003
Visiting Professor in the Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University.

Chiang Mai University, Thailand 1999, 2000–2001, 2002
Visiting Professor in the Department of Computer Science, Faculty of Science, Chiang Mai University. Also 6/98–12/98 at the Computer Service Center, Chiang Mai University, Chiang Mai, Thailand.

IBM, Austin, Texas, USA 1991–1994
Computer security architect, IBM LAN System Design. Develop new products, represent IBM at industry consortia, give advice on standards and protocols, participate in customer briefings, develop IBM security strategy.

Dartmouth College, Hanover, New Hampshire, USA 1990–1991
Visiting assistant professor, Department of Mathematics and Computer Science. Taught courses in theory of computation, introduction to computer science, modern cryptography.

Massachusetts Institute of Technology 1985–1986 and 1987–1990
Research Assistant and Teaching Assistant (alternate semesters) under Silvio Micali, Albert Meyer, and Ron Rivest.

University of Wisconsin, Madison *1986–1987*
Teaching Assistant for calculus, under Walter Rudin.

University of California, Berkeley *1982–1984*
Undergraduate tutor for CS self-paced center. How I supported myself back in undergrad days.

Classroom teaching

▷ Median evaluations of 10/10 (old system) and 5/5 (new system) for most classes over a many-year span
▷ College of Engineering Outstanding Teaching Award, 2010 (college-wide, ∼225 faculty)
▷ ASUCD Outstanding Teaching Award Finalist: 2014, 2015 (campus-wide, ∼2,000 faculty)
▷ Cryptography (UG) (ecs 127) ← **designed course**
▷ Cryptography and Surveillance (designed but canceled) (UG) (ecs 189L)
▷ Data Structures and Programming (UG) (ecs 110)
▷ Design and Analysis of Algorithms (UG) (ecs 122A)
▷ Discrete Math for Computer Science (UG) (ecs 20)
▷ Ethics in an Age of Technology (UG) (ecs 188) ← **designed course**
▷ Modern Cryptography (Grad) (ecs 227) ← **designed course**
▷ Theory of Computation (UG) (ecs 120)
▷ Theory of Computation (Grad) (ecs 220)

PhD students advised

▷ John Black — Professor at University of Colorado, Boulder
▷ John Chan — On job market
▷ Ted Krovetz — Professor at Sacramento State University
▷ Tom Ristenpart — Professor at Cornell Tech (Graduated from UCSD, not UCD)
▷ Tom Shrimpton — Professor at University of Florida
▷ Till Stegers — Scientist at Google
▷ John Steinberger — Consultant, independent researcher. Formerly: Tsinghua, China.
▷ Viet Tung Hoang — Professor at Florida State University
▷ Yusi (James) Zhang — Scientist at Google

Sample teaching evaluations

Teaching evaluation collected by the university, included in full
▷ ECS 127: Cryptography. Winter 2019. `tinyurl.com/rogaway-ecs127`
A mathematical course typical of my "technical" teaching

▷ ECS 188: Ethics in an Age of Technology. Spring 2019. `tinyurl.com/rogaway-ecs188`
The class I have focused on in recent years. More STS than moral philosophy

▷ Ratemyprofessor student reviews

References *I have updated my references to name not just people to evaluate my research, but people who know me and what I care about.*

Prof. Mihir Bellare *Closest collaborator for 30 years*
University of California at San Diego
`mihir@eng.ucsd.edu`
https://cseweb.ucsd.edu/∼mihir/

Prof. Norm Matloff *Senior professor in my home department*
University of California at Davis
`nsmatloff@ucdavis.edu`

Prof. Chanathip Namprempre *Closest colleague in Thailand*
Currently: Visiting Professor at Reed College, in Oregon, USA
Formerly: Professor at Thammasat University, Thailand
`cnamprem@gmail.com`

Prof. Ted Krovetz *Former student*
Chair, Department of Computer Science, Sacramento State
`ted@krovetz.net`