
Phillip Rogaway

http://www.cs.ucdavis.edu/~rogaway
 rogaway@cs.ucdavis.edu

Address	Department of Computer Science	office:	+1 530 752 7583
	Kemper Hall of Engineering	FAX:	+1 530 752 4767
	One Shields Avenue	secretary:	+1 530 752 7004
	University of California	home:	+1 530 753 0987
	Davis, California 95616 USA	cell:	+1 530 220 4843

Position Professor, Dept. of Computer Science, University of California at Davis, USA *since 8/94*

Research Cryptography

Education **Massachusetts Institute of Technology** *9/87–6/90*
 Ph.D. in Electrical Engineering and Computer Science, 1991 *9/85–6/86*
 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 *9/80–12/84*
 A.B. in Computer Science, 1985

Awards

- ▷ **ACM Paris Kanellakis Theory and Practice Award** (2009) (joint with Mihir Bellare). The award is given for “specific theoretical accomplishments that have had a significant and demonstrable effect on the practice of computing.” The citation acknowledges our “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) (joint with Mihir Bellare). The award “recognizes innovation and ongoing contribution to the field of cryptography.” The citation explains that our work provides “assurances that cryptographic methods employed by implementers are secure. They co-developed the ‘random oracle’ model, ... the primary paradigm for reasoning about the properties of cryptographic methods today ... [T]heir body of work [includes] the introduction of several major methods used in the field today, including Optimal Asymmetric Encryption Padding (OAEP) and the Probabilistic Signature Scheme (PSS).”
- ▷ **NSF CAREER Award** (1996)

Stats

h-index: **42**

Number of citations: **13,495**

Number of papers: **62**

Number of CRYPTO + EUROCRYPT pubs: **26**

Data from Google Scholar with Harzing's Publish or Perish frontend; 5/1/10

The world's most-cited cryptographers (Lipmaa, 4/1/10) are, in order: Shamir, Rivest, Bellare, Goldreich, Boneh, Micali, Chaum, Naor, **Rogaway**, Canetti, Yao, Goldwasser, ... Only DBLP-indexed papers are included in this count

The traditional tier-1 venues for cryptography

- 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-Verlag, 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-Verlag, 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-Verlag, pp. 392–404, 1991.
- A5.** M. Bellare and P. Rogaway. THE COMPLEXITY OF APPROXIMATING A NON-LINEAR 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-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, pp. 29–42, 1995.

- Publications (cont)**
- 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-Verlag, 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-Verlag, 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-Verlag, pp. 470–484, 1997.
- A20.** M. Bellare, A. Desai, E. Jorjipii 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 Verlag, 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-Verlag, 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-Verlag, 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-Verlag, pp. 231–244, 1999.

**Publications
(cont)**

- 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-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, 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-Verlag 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.** J. Black and P. Rogaway. CIPHERS WITH ARBITRARY FINITE DOMAINS. *Topics in Cryptology — CT-RSA 2002*. Lecture Notes in Computer Science, vol. 2271, Springer-Verlag, pp. 114–130, 2002.
- A38.** 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-Verlag, pp. 384–397, 2002.
- A39.** 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.)

- Publications (cont)**
- A40.** J. Black and P. Rogaway and T. Shrimpton. ENCRYPTION-SCHEME SECURITY IN THE PRESENCE OF KEY-DEPENDENT MESSAGES. *Proceedings of SAC 2002*. to appear in Lecture Notes in Computer Science, Springer-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, pp. 389–407, 2004.
- A47.** P. Rogaway. NONCE-BASED SYMMETRIC ENCRYPTION. *Fast Software Encryption*, Lecture Notes in Computer Science, vol. 3017, Springer-Verlag, 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-Verlag, 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-Verlag, 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-Verlag, 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 (cont)**
- A53.** 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.
- A54.** 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.
- A55.** T. Krovetz and P. Rogaway. VARIATIONALLY UNIVERSAL HASHING. *Information Processing Letters (IPL)*, vol. 100, no. 1, Elsevier Scientific, pp. 36–39, 2006.
- A56.** 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.
- A57.** M. Abadi and P. Rogaway. RECONCILING TWO VIEWS OF CRYPTOLOGY (THE COMPUTATIONAL SOUNDNESS OF FORMAL ENCRYPTION). *Journal of Cryptology*, vol. 20, no. 3, p. 395, 2007. Errata A39.
- A58.** 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.
- A59.** 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.
- A60.** 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.
- A61.** 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.
- 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.** 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.
- A65.** V. Hoang and P. Rogaway. ON GENERALIZED FEISTEL NETWORKS. *Advances in Cryptology – CRYPTO 2010*. Lecture Notes in Computer Science, Springer, 2010.

Patents

- H1.** D. Coppersmith and P. Rogaway. SOFTWARE-EFFICIENT PSEUDORANDOM FUNCTION AND THE USE THEREOF FOR ENCRYPTION. US Patent #5,454,039. September 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 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 1996.
- H4.** P. Rogaway. SOFTWARE-EFFICIENT MESSAGE AUTHENTICATION. US Patent #5,651,069. July 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 1997.
- H6.** M. Bellare and P. Rogaway. BLOCK CIPHER MODE OF OPERATION FOR SECURE, LENGTH-PRESERVING ENCRYPTION. US Patent #5,673,319. September 1997.
- H7.** M. Blakley and P. Rogaway. COMPUTER READABLE DEVICE IMPLEMENTING A SOFTWARE-EFFICIENT PSEUDORANDOM FUNCTION. US Patent #5,675,652. October 1997.
- H8.** B. Blakley and P. Rogaway. METHOD TO PROTECT INFORMATION ON A COMPUTER STORAGE DEVICE. US Patent #5,677,952. October 1997.
- H9.** M. Bellare, P. Guerin, and P. Rogaway. METHOD AND APPARATUS FOR DATA AUTHENTICATION IN A DATA COMMUNICATION ENVIRONMENT. US Patent #5,757,913, May 26. (See also H5)
- H9.** B. Bellare and P. Rogaway. PROBABILISTIC SIGNATURE SCHEME. US Patent #06266771, July 2001.
- H10.** D. Coppersmith, and P. Rogaway. SOFTWARE-EFFICIENT PSEUDORANDOM FUNCTION AND THE USE THEREOF FOR DECRYPTION. US Patent #5,835,597. November 1998. (See also H1)
- H11.** M. Bellare, and P. Rogaway. PROBABILISTIC SIGNATURE SCHEME. US Patent #6,266,771, July 2001.
- H12.** M. Bellare, and P. Rogaway. PROBABILISTIC SIGNATURE SCHEME. US Patent #7,036,014. April 2005. (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 2007.

**Invited
talks at
conferences,
keynotes**

K1. RECONCILING TWO VIEWS OF CRYPTOGRAPHY (THE COMPUTATIONAL SOUNDNESS OF FORMAL CRYPTOGRAPHY). Invited 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. Invited 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. Invited talk at ASIAN '04, Ninth Asian Computing Science Conference. Invited talk. Chiang Mai, Thailand. December 2004. (See also A49.)

K4. FORMALIZING KNOWLEDGE AND IGNORANCE. Invited 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. Invited talk 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. Invited talk at SBSeg 2009, the Brazilian Symposium on Information and Computer System Security. Campinas, Brazil. September 2010.

**Invited
talks at
symposia**

- S1.** THE COMPLEXITY OF APPROXIMATING A NONLINEAR PROGRAM. Invited talk at the Fourth SIAM Conference on Optimization, Chicago, Illinois, USA. May 1992. (See also A5)
- S2.** PROVABLY-SECURE KEY DISTRIBUTION — THE THREE PARTY CASE. Invited talk at RSA Seminar Series, Redwood City, California, USA. August 1995.
- S3.** DESIGN AND ANALYSIS OF MESSAGE AUTHENTICATION CODES. Invited talk at the 1996 RSA Data Security Conferences, San Francisco, California, USA. January 1996.
- S4.** PRACTICE-ORIENTED PROVABLE SECURITY. Invited talk at the 1996 RSA Cryptographers' Colloquium. Palo Alto, California, USA. August 1996.
- S5.** RANDOM ORACLES AND ASYMMETRIC ENCRYPTION. Invited talk at Public Key Solutions '97. Toronto, Canada. April 1997. (See also A21.)
- S6.** TARGET COLLISION-RESISTANT HASHING. Invited talk at the 1997 RSA Laboratories Seminar Series. San Francisco, California, USA. August 1997. (See also A21.)
- S7.** ADVANCES IN DIGITAL SIGNATURES. Invited talk at Public Key Solutions '99. Toronto, Canada. April 1999.
- S8.** STOPPING DICTIONARY ATTACKS. Invited talk at the Fourth Workshop on Elliptic Curve Cryptography (ECC 2000). Essen, Germany. October 2000.
- S9.** SOME RECENT WORK ON DESIGNING EFFICIENT MODES OF OPERATION. Invited talk at a meeting of the American Mathematics Society (AMS) and the Sociedad Matematica Mexicana (SMM), Special Section on Coding Theory and Cryptography. Houston, Texas. May 2004.
- S10.** SOME RECENT WORK ON DESIGNING BLOCKCIPHER MODES OF OPERATION. Invited talk at RSA Conference Japan. Tokyo, Japan. June 2004.
- S11.** 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.

**Conference
talks**

- T1.** EVERYTHING PROVABLE IS PROVABLE IN ZERO-KNOWLEDGE. Presented at CRYPTO '88, Santa Barbara, California, USA. August 1988. (See also A1)
- T2.** 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)
- T3.** ENTITY AUTHENTICATION AND KEY DISTRIBUTION. Presented at CRYPTO '93, Santa Barbara, California, USA. August 1993. (See also A7)
- T4.** 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)
- T5.** THE SECURITY OF CIPHER BLOCK CHAINING. Presented at CRYPTO '94, Santa Barbara, California, USA. August 1994. (See also A9)
- T6.** BUCKET HASHING AND ITS APPLICATION TO FAST MESSAGE AUTHENTICATION. Presented at CRYPTO '95, Santa Barbara, California, USA. August 1995. (See also A23.)
- T7.** HOW TO PROTECT DES AGAINST EXHAUSTIVE KEY SEARCH. Presented at CRYPTO '96, Santa Barbara, California, USA. August 1996. (See also A16)
- T8.** COLLISION-RESISTANT HASHING: TOWARDS MAKING UOWHFs PRACTICAL. Presented at CRYPTO '97, Santa Barbara, California, USA. August 1997. (See also A19)
- T9.** 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)
- T10.** AUTHENTICATED KEY EXCHANGE SECURE AGAINST DICTIONARY ATTACKS. Presented at EUROCRYPT 2000. Brugge, Belgium. May 2000. (See also A31.)
- T11.** OCB: A BLOCK-CIPHER MODE OF OPERATION FOR EFFICIENT AUTHENTICATED ENCRYPTION. Presented at the *ACM Conference on Computer and Communications Security (CCS-8)*. Philadelphia, Pennsylvania, USA. November 2001. (See also A36.)
- T12.** 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.)
- T13.** NONCE-BASED SYMMETRIC ENCRYPTION. Presented at *Fast Software Encryption (FSE 2004)*. Delhi, India. February 2004. (See also A47.)
- T14.** 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. EUROCRPYT 2006, St. Petersburg, Russia. May 2006. (See also A54.)

**Workshop
talks**

- W1.** THE ROUND COMPLEXITY OF SECURE PROTOCOLS. Presented at the DIMACS Workshop on Cryptography, Princeton, New Jersey, USA. October 1989. (See also A2)
- W2.** SECURITY WITH LOW COMMUNICATION OVERHEAD. Presented at the DIMACS Workshop on Cryptography, Princeton, New Jersey, USA. October 1990. (See also A3)
- W3.** SECURE COMPUTATION. Presented at the Colloque Cryptographie, Luminy, France, USA. September 1991. (See also A4)
- W4.** THE COMPLEXITY OF APPROXIMATING A NONLINEAR PROGRAM. Presented at the Colloque Cryptographie, Luminy, France. September 1991. (See also A5)
- W5.** ENTITY AUTHENTICATION AND KEY DISTRIBUTION. Presented at the Fourth IBM Security ITL. New York, USA. October 1992. (See also A11)
- W6.** A SOFTWARE-OPTIMIZED ENCRYPTION ALGORITHM. Presented at the 1993 Cambridge Algorithms Workshop, Cambridge, England. December 1993. (See also A8)
- W7.** A SOFTWARE-OPTIMIZED ENCRYPTION ALGORITHM. Presented at the Mobile Computing Workshop, Austin, Texas, USA. January 1994.
- W8.** A CONCRETE SECURITY TREATMENT OF SYMMETRIC ENCRYPTION. Dagstuhl Seminar on Cryptography, Schloss Dagstuhl, Germany. September 1997. (See also A20)
- W9.** “ACCIDENTS” AND SELECTED OPEN PROBLEMS IN MODERN CRYPTOGRAPHY. Presented at “Cryptography and Mathematics” workshop, Mathematical Sciences Research Institute (MSRI), Berkeley, California, USA. January 1998.
- W10.** CTR-MODE ENCRYPTION. Presented at the National Institute of Standards (NIST) Modes of Operation Workshop. Baltimore, Maryland, USA. October 2000.
- W11.** 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.
- W12.** 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.)
- W13.** PMAC. Presented at the Second NIST Modes of Operation Workshop. Santa Barbara, California, USA. August 2001. (See also A38.)
- W14.** SOME RECENT WORK CONSTRUCTING BLOCK-CIPHER MODES OF OPERATION. Presented at the Dagstuhl Seminar on Cryptography, Schloss Dagstuhl, Germany. September 2002.
- W15.** FORMALIZING HUMAN IGNORANCE. Dagstuhl Seminar on Cryptography, Schloss Dagstuhl, Germany. Wadern, Germany, January 2007.
- W16.** FORMALIZING HUMAN IGNORANCE and PERMUTATION-BASED CRYPTOGRAPHIC HASHING. Dagstuhl Seminar on Cryptography, Schloss Dagstuhl, Germany. Wadern, Germany, September 2007.
- W17.** FORMAT-PRESERVING ENCRYPTION: HOW TO ENCIPHER CCNs, SSNs, AND THE LIKE. RSA Conference 2010, Applications and Development Track, San Francisco, USA. March 2010.

**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
(cont)**

- 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.

**Teaching
at summer
schools
and the like**

S1. BASIC CRYPTOGRAPHIC PRIMITIVES. Three lectures. Presented at the Summer school on Distributed Systems and Cryptography, Lipari, Italy. July 1998.

S2. FOUNDATIONS OF APPLICABLE CRYPTOGRAPHY. Two lectures. Presented at Winter School on Chaotic Communications, UC San Diego, San Diego, California, USA. January 1999.

S3. USING PROVABLE SECURITY TO DESIGN PRACTICAL CRYPTOGRAPHIC PROTOCOLS. Four lectures. Presented at the Estonian Winter School in Computer Science. Lahemaa, Estonia. March 2001.

S4. PRACTICAL CRYPTOGRAPHY. Three lectures. Presented at the Summer School on Foundations of Internet Security. Duszynki Zdroj, Poland. June 2002.

S5. SYMMETRIC TECHNIQUES. ECRYPT Summer School on Provable Security. Barcelona, Spain. September 2009.

**Mini-classes
taught**

M1. DISCRETE MATHEMATICS FOR COMPUTER SCIENCE. Seven lectures, in Thai. Presented to students competing in the International Computer Science Olympiad. Chiang Mai, Thailand. October 2000.

M2. CRYPTOGRAPHY AND NP-COMPLETENESS. Twelve lectures. Presented at Chulalongkorn University, Faculty of Science, Department of Mathematics, Bangkok, Thailand. November–December 2000.

M3. ALGORITHM ANALYSIS AND GRAPH ALGORITHMS. Four lectures, in Thai. Presented to students competing in the International Computer Science Olympiad. Chiang Mai, Thailand, March 2001.

M4. CRYPTOGRAPHY AND COMPUTER SECURITY. Two-day mini-course, 12 hours. Chiang Mai, Thailand. September 2002.

M5. 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 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.

**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 OCB 2.0 [A50] 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]
- ▷ 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]
- ▷ RSA PKCS #1, v.2.1 — RSAES-OAEP [A10], RSASSA-PSS [A15], EMSA-PSS [A15]
- ▷ SET — specifies OAEP [A10]

- Current funding**
- ▷ “Reimagining cryptography by identifying its culturally-rooted assumptions.” PI: Phillip Rogaway. Co-PI: Mihir Bellare, Ted Krovetz. TC medium. NSF CNS 0904380. **\$850,000**. Four years, 2009-2013.
- Past funding**
- ▷ “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: July 2000–June 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.

Professional history	University of California at Davis <i>8/94–present</i>
	Assistant Professor (1994–1997), Associate Professor (1997–2002), Professor (2002–present). Department of Computer Science. Teaching history below.
	Consultant <i>9/95–present</i>
	Private consulting on cryptography. Clients such as IBM, Microsoft, Security First, Voltage Security, the government of Japan, and a large financial institution.
	Advisory Boards
	Member of the Technical Advisory Board for Voltage Security and Core Street. Voltage has done well productizing format-preserving encryption, using methods based on my work.
	Chulalongkorn University, Thailand <i>10/02–03/03</i>
	Visiting professor at the Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok, Thailand.
	Chiang Mai University, Thailand <i>6/99–12/99, 6/00–9/01, 6/02–9/02</i>
	Visiting professor at the Department of Computer Science, Faculty of Science, Chiang Mai University, Chiang Mai, Thailand. Also 6/98–12/98 at the Computer Service Center, Chiang Mai University, Chiang Mai, Thailand.
	IBM <i>10/91–6/94</i>
	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 <i>9/90–6/91</i>
	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 <i>9/85–5/86 and 9/87–6/90</i>
	Research Assistant and Teaching Assistant (alternate semesters) under S. Micali, A. Meyer, and R. Rivest.
Courses taught	▷ Discrete Math for Computer Science (UG) (ecs 20)
	▷ Data Structures and Programming (UG) (ecs 110)
	▷ Introduction to the Theory of Computation (UG) (ecs 120)
	▷ Design and Analysis of Algorithms (UG) (ecs 122A)
	▷ Ethics in an Age of Technology (UG) (ecs 188)
	▷ Theory of Computation (Grad) (ecs 220)
	▷ Modern Cryptography (Grad) (ecs 227)
▷ <i>Teaching materials available from my URL.</i>	
▷ <i>188 is unique course I designed; see www.cs.ucdavis.edu/~rogaway/classes/188/teaching</i>	
Member	Computer Professionals for Social Responsibility (CPSR)
	International Association for Cryptologic Research (IACR)