

# Mihir Bellare

## CURRICULUM VITAE

August 2018

Department of Computer Science & Engineering, Mail Code 0404  
University of California at San Diego  
9500 Gilman Drive, La Jolla, CA 92093-0404, USA.  
Phone: (858) 534-4544 ; E-mail: [mihir@eng.ucsd.edu](mailto:mihir@eng.ucsd.edu)  
Web Page: <http://cseweb.ucsd.edu/~mihir>

---

## Contents

<b>1</b>	<b>Research areas</b>	<b>2</b>
<b>2</b>	<b>Education</b>	<b>2</b>
<b>3</b>	<b>Distinctions and Awards</b>	<b>2</b>
<b>4</b>	<b>Impact</b>	<b>3</b>
<b>5</b>	<b>Grants</b>	<b>4</b>
<b>6</b>	<b>Professional Activities</b>	<b>5</b>
<b>7</b>	<b>Industrial relations</b>	<b>5</b>
<b>8</b>	<b>Work Experience</b>	<b>5</b>
<b>9</b>	<b>Teaching</b>	<b>6</b>
<b>10</b>	<b>Publications</b>	<b>6</b>
<b>11</b>	<b>Mentoring</b>	<b>19</b>
<b>12</b>	<b>Personal Information</b>	<b>21</b>

## 1 Research areas

- \* CRYPTOGRAPHY AND SECURITY: Provable security; authentication; key distribution; signatures; encryption; protocols.
- \* COMPLEXITY THEORY: Interactive and probabilistically checkable proofs; approximability ; complexity of zero-knowledge; randomness in protocols and algorithms; computational learning theory.

## 2 Education

- \* MASSACHUSETTS INSTITUTE OF TECHNOLOGY. Ph.D in Computer Science, September 1991. Thesis title: *Randomness in Interactive Proofs*. Thesis supervisor: Prof. S. Micali.
- \* MASSACHUSETTS INSTITUTE OF TECHNOLOGY. Masters in Computer Science, September 1988. Thesis title: *A Signature Scheme Based on Trapdoor Permutations*. Thesis supervisor: Prof. S. Micali.
- \* CALIFORNIA INSTITUTE OF TECHNOLOGY. B.S. with honors, June 1986. Subject: Mathematics. GPA 4.0. Class rank 4 out of 227. Summer Undergraduate Research Fellow 1984 and 1985.
- \* ECOLE ACTIVE BILINGUE, PARIS, FRANCE. Baccalauréat Série C, June 1981.

## 3 Distinctions and Awards

- \* PET (Privacy Enhancing Technologies) Award 2015 for publication [154].
- \* Fellow of the ACM (Association for Computing Machinery), 2014.
- \* ACM Paris Kanellakis Theory and Practice Award 2009.
- \* RSA Conference Award in Mathematics, 2003.
- \* David and Lucille Packard Foundation Fellowship in Science and Engineering, 1996. (Twenty awarded annually in all of Science and Engineering.)
- \* Test of Time Award, ACM CCS 2011, given for [81] as best paper from ten years prior.
- \* IACR Fellow, 2012 (IACR = International Association of Cryptologic Research. There were only 38 IACR fellows, including 5 Turing Award winners, at time award was made.)
- \* NSF CAREER award, 1996.
- \* h-index = 98 (Source: Google Scholar)
- \* Over 49,000 citations (Source: Google Scholar)
- \* Ranked number 1 in the world in terms of number of publications in Crypto, Eurocrypt and Asiacrypt, the tier 1 conferences in cryptography. (Source: IACR Crypto database)
- \* Co-designer of the Skein hash function which was selected as a finalist in the SHA3 competition for the next standard by NIST (National Institute of Standards and Technology).
- \* Publication [149] invited to Journal of Cryptology as one of the top-ranked papers at Crypto 2013.
- \* Publication [128] invited to Journal of Cryptology as one of the top-ranked papers at Eurocrypt 2009.

- \* Publication [22] was the highest ranked submission at the Crypto 93 conference, 1993.
- \* Publication [23] was the highest ranked submission at the 1st ACM Computer and Communications security conference, 1993.
- \* Publication [86] was the highest ranked submission at the 9th ACM Computer and Communications security conference, 2002.
- \* Publication [90] was the highest ranked submission at the CT-RSA conference, 2003.
- \* An IBM outstanding innovation award was given for HMAC (a data integrity algorithm presented in publication [40]), March 1997.
- \* An IBM outstanding technical achievement award was given for iKP (an electronic payment protocol presented in publication [67]), August 1996.
- \* IBM invention achievement awards: April 1993 and April 1995.
- \* IBM author recognition awards: January 1993, June 1993, and December 1993.
- \* IBM Faculty Partnership Award, 2001.
- \* Spencer Eaken Allmond Scholarship, 1986.
- \* Carnation Prize, Caltech, 1985.
- \* Member, Tau Beta Pi honor society

## 4 Impact

- \* HMAC, the message authentication scheme of publication [40], is implemented and used in BSAFE; SSL (3.0 and 3.1); TLS; IPsec; SSH; S-HTTP; NetBSD; CDSA (Hewlett-Packard). It is in the following standards: RFC 2104; ANSI X9.71; NIST FIPS 198 (Federal Information Processing Standard, US government); IEEE 802.11. You use HMAC every time you connect to gmail via `https:` or make a credit card-based Internet payment. HMAC is used billions of times a day.
- \* The RSA-OAEP (Optimal Asymmetric Encryption Padding) encryption scheme of publication [24] is included in the following standards: IEEE P1363a; ANSI X9.44; CRYPTREC; ISO/IEC 18033-2; RFC 3447; RFC 3560; RSA PKCS #1 v2.1. It is implemented in various products and systems including SET; CDSA. OAEP is mentioned in a New York Times on the web article by Peter Wayner, August 25th, 1998.
- \* The DHIES (Diffie-Hellman integrated encryption scheme) of publication [77] is included in the following standards: ANSI X9.63; ISO/IEC 18033-2; SEC; IEEE P1363a.
- \* Mastercard and Visa's SET standard for credit card based electronic commerce is based on the iKP family of electronic payment protocols, developed in publications [33, 67].
- \* The PSS (Probabilistic Signature Scheme) of publication [39] is included in the following standards: IEEE P1363a; ANSI X9.31; CRYPTREC; NESSIE; ISO/IEC 9796-2; RFC 3447; RSA PKCS#1 v2.1.
- \* The EAX authenticated encryption scheme of publication [95] is included in the following standards: ANSI C12.22; ISO/IEC 19772:2009.
- \* The OCB authenticated encryption scheme of publication [81] is included in the following standards: IEEE 802.11i; ISO/IEC 19772:2009.
- \* Developed encryption to protect against counterfeiting of drugs for PharmaSecure corporation; now in

wide use in India and Africa.

- \* Developed methods for Format-Preserving encryption now in use for encryption of credit-card numbers in millions of transactions by Voltage Security. Methods to be standardized by NIST.
- \* Member of design team for the Skein hash function that was selected as a finalist in the SHA3 competition for the next generation hash standard by NIST.
- \* Bellare's work and papers are discussed and cited in numerous textbooks including: *Cryptography and Network Security, Principles and Practices* by William Stallings; *Handbook of Applied Cryptography* by Menezes, Van Oorschott and Vanstone; *SSL and TLS* by Eric Rescorla; *Foundations of Cryptography* by Oded Goldreich; *Cryptography Theory and Practice* by Douglas Stinson; *Introduction to Cryptography* by Delfs and Knebl; *Introduction to Cryptography* by Johannes Buchmann; *Modern Cryptography, Probabilistic Proofs and Pseudo-Randomness* by Oded Goldreich; *Applied Cryptography* by Bruce Schneier; *Modeling and Analysis of Security Protocols* by Ryan and Schneider; *Rethinking Public-Key Infrastructure and Digital Certificates – Building in Privacy* by Stefan Brands; *Protocols for Authentication and Key Establishment* by Boyd and Mathuria; *Electronic Payment Systems* by O'Mahoney, Peirce and Tewari; *Practical Cryptography* by Ferguson and Schneier; *Pseudo-Randomness and Cryptographic Applications* by Mike Luby; *A Computational Introduction to Number Theory and Algebra* by Victor Shoup; *Introduction to Computer Security* by Matt Bishop; *Computer Security* by Matt Bishop; *White-Hat Security Arsenal* by Aviel Rubin; *A Classical Introduction to Cryptography* by Serge Vaudendy; *Digital Signature Schemes* by Birgit Pfizmann; *Introduction to Modern Cryptography* by Katz and Lindell.

## 5 Grants

- \* David and Lucille Packard Foundation fellowship in science and Engineering. Period: 1996–2001. Amount: \$575,000.
- \* NSF CAREER award. Period: 1996–2000. Amount: \$200,000.
- \* NSF grant CCR-0098123, PI, Design and Analysis of Cryptographic Protocols for Secure Communication. Period: 2001–2004. Amount: \$236,830.
- \* IBM Faculty Partnership Development Award. Period: 2001. Amount: \$40,000.
- \* NSF grant ANR-0129617, PI, Cryptographic Mechanisms for Internet Security. 2002–2005. Amount: \$218,585.
- \* NSF grant CCR-0208842, coPI, Practice-Oriented Provable Security for Higher-Layer Protocols: Models, Analyses and Solutions, 2002–2005. Amount: \$400,000.
- \* NSF grant CNS-0524765, PI, CT-ISG: Practice-Oriented Provable-Security for Emerging Cryptographic Applications, 2005–2008. Amount: \$450,000.
- \* NSF grant CNS-0627779, PI, CT-ISG: Cryptography for Computational Grids, 2006–2009. Amount: \$300,000.
- \* NSF grant CCF-0915675, PI, TC:Small:Systems-sensitive cryptography, 2009–2012. Amount: \$499,030
- \* NSF grant CNS-1116800, PI, TC:Small:A cryptographic treatment of the wiretap channel, 2011–2014. Amount: \$493,995
- \* NSF grant CNS-1228890, coPI, TWC:Medium:Collaborative:Deconstructing encryption, 2012–2016. Amount: \$400,000.
- \* NSF grant CNS-1526801, PI, TWC:Small:Subversion-resistant cryptography, 2015–2018. Amount: \$500,000.

- \* NSF grant CNS-1526801, PI, SaTC:Core:Small:Foundations of applied cryptography, 2017–2019. Amount: \$325,000.

## 6 Professional Activities

- \* Program chair, Crypto 2000 conference
- \* Program committee member for the following conferences: Crypto 93; Eurocrypt 95; Crypto 96; 29th Annual ACM Symposium on the theory of computing (STOC), 1997; 39th IEEE Symposium on Foundations of Computer Science (FOCS), 1998; Eurocrypt 99; Principles of Distributed Computing (PODC), 1999; Symposium on Discrete Algorithms (SODA), 2000; IEEE conference on Security and Privacy, 2001; Sigcomm 2001; ACM Conference on Computer and Communications Security, 2002; Crypto 2003; ACM Conference on Computer and Communications Security, 2003; Theory of Cryptography Conference (TCC) 2006; Asiacrypt 2006; Crypto 2011; Crypto 2013; Privacy Enhancing Technologies 2016; Crypto 2017; PKC 2017; ACM Conference on Computer and Communications Security, 2018.
- \* Member of the Advisory Editorial Board for the book *CRC Handbook of Applied Cryptography* by A. Menezes, P. Van Oorschot, and S. Vanstone, CRC Press, 1996.
- \* Refereed papers for numerous journals including: Journal of the ACM; SIAM Journal on Computing; Journal of Cryptology; IEEE/ACM Transactions on Networking; IEEE Transactions on Systems, Man and Cybernetics; Information and Computation; IEEE Transactions on Information Theory; IEEE Journal on Special Areas in Communications; Wireless Network Journal; Computational Complexity; Information Processing Letters; Mathematical and Computer Modelling; Information Systems; Theoretical Computer Science A; IBM J. of Research and Development.
- \* Reviewed grant proposals for various funding agencies including: NSF; Israel Science Foundation; Research Grants Council of Hong Kong.

## 7 Industrial relations

- \* Chief Cryptographer, Tricipher Corporation.
- \* Scientific advisory board member, Corestreet corporation.
- \* Consultant for numerous corporations including: Semtek (since acquired by Verifone); Ziva; PharmaSecure; Baffle.

## 8 Work Experience

- \* Professor, Dept. of Computer Science and Engineering, University of California at San Diego, July 01–Present.
- \* Associate Professor, Dept. of Computer Science and Engineering, University of California at San Diego, June 97–June 01.
- \* Assistant Professor, Dept. of Computer Science and Engineering, University of California at San Diego, September 1995–May 97.
- \* Research Staff Member, IBM T.J. Watson Research Center, New York, September 1991 – September 1995. Groups: Network security (Manager Dr. A. Herzberg) and Network System Design (Manager Dr. R. Guérin). Responsible for design of secure systems.

- \* Undergraduate research fellow at the California Institute of Technology, June – August 1984. Designed and implemented a spread sheet application in the ASK natural language system. Supervisor: Prof. F. B. Thompson.

## 9 Teaching

- \* Computability and complexity (CSE 200)– Graduate core course in the CSE Dept., UCSD.
- \* Cryptography and network security (CSE207)– Graduate Introduction to modern cryptography, CSE Dept., UCSD.
- \* Cryptography and Information Security– A one week summer course, taught jointly with Shafi Goldwasser at MIT annually.
- \* Introduction to the theory of computation (CSE 105)– Undergraduate course in the CSE Dept. at UCSD.
- \* Mathematics for algorithms and systems analysis (CSE 21)– Undergraduate course in the CSE Dept. at UCSD.
- \* Introduction to modern cryptography (CSE107)– Undergraduate course in the CSE Dept. at UCSD.
- \* Advanced topics in cryptography (CSE291, CSE208)– Graduate seminar in cryptography, CSE Dept., UCSD. Topics vary from year to year and have included: electronic payment mechanisms, zero knowledge, pairing-based cryptography, obfuscation, random oracles.

## 10 Publications

### 10.1 Summary

The following table summarizes the number of publications in different venues:

Venue	Number
1st tier cryptography conferences (Crypto, Eurocrypt, Asiacrypt)	81
Other cryptography conferences (PKC, TCC, FSE, FC, CT-RSA, ICALP, ... )	28
1st tier security conferences (CCS, S&P, Usenix Security)	15
1st tier theory conferences (FOCS, STOC)	18

### 10.2 Editor

- [1] M. BELLARE. Advances in Cryptology – Crypto 2000, 20th Annual International Cryptology Conference, August 2000, Proceedings. Lecture Notes in Computer Science Vol. 1880, Springer-Verlag, 2000.

### 10.3 Survey Articles

- [2] M. BELLARE. Proof Checking and Approximation: Towards Tight Results. Sigact News, Vol 27, No 1, March 1996.

- [3] M. BELLARE, R. CANETTI AND H. KRAWCZYK. Message authentication using hash functions: The HMAC construction. *RSA Laboratories' CryptoBytes*, Vol. 2, No. 1, Spring 1996.
- [4] M. BELLARE. Practice-oriented provable-security. *Proceedings of First International Workshop on Information Security (ISW 97)*, Lecture Notes in Computer Science Vol. 1396, E. Okamoto, G. Davida and M. Mambo eds., Springer Verlag, 1998. Also in *Modern Cryptology in Theory and Practice*, Lectures on Data Security series, Lecture Notes in Computer Science Tutorial, Ivan Damgård, ed., Springer, 1999.

## 10.4 Conference and journal publications

- [5] M. BELLARE AND S. MICALI. How to sign given any trapdoor function. *Proceedings of the 20th Annual Symposium on the Theory of Computing*, ACM, 1988 and *Advances in Cryptology – CRYPTO '88*, Lecture Notes in Computer Science Vol. 403, S. Goldwasser ed., Springer, 1988.
- [6] M. BELLARE AND S. MICALI. Non-interactive oblivious transfer and its applications. *Advances in Cryptology – CRYPTO '89*, Lecture Notes in Computer Science Vol. 435, G. Brassard ed., Springer, 1989.
- [7] M. BELLARE AND S. GOLDWASSER. New paradigms for digital signatures and message authentication based on non-interactive zero-knowledge proofs. *Advances in Cryptology – CRYPTO '89*, Lecture Notes in Computer Science Vol. 435, G. Brassard ed., Springer, 1989.
- [8] M. BELLARE, L. COWEN AND S. GOLDWASSER. On the structure of secret key exchange protocols. *Distributed Computing and Cryptography*, Dimacs Series in Discrete Mathematics and Theoretical Computer Science Volume 2, AMS/ACM, 1991.
- [9] M. BELLARE, S. MICALI AND R. OSTROVSKY. Perfect zero-knowledge in constant rounds. *Proceedings of the 22nd Annual Symposium on the Theory of Computing*, ACM, 1990.
- [10] M. BELLARE, S. MICALI AND R. OSTROVSKY. The (true) complexity of statistical zero-knowledge. *Proceedings of the 22nd Annual Symposium on the Theory of Computing*, ACM, 1990.
- [11] M. BELLARE, O. GOLDREICH AND S. GOLDWASSER. Randomness in interactive proofs. *Proceedings of the 31st Symposium on Foundations of Computer Science*, IEEE, 1990.
- [12] R. BEIGEL, M. BELLARE, J. FEIGENBAUM AND S. GOLDWASSER. Languages that are easier than their proofs. *Proceedings of the 32nd Symposium on Foundations of Computer Science*, IEEE, 1991.
- [13] M. BELLARE AND S. MICALI. How to sign given any trapdoor permutation. *Journal of the Association for Computing Machinery*, Vol. 39, No. 1, January 1992, pp. 214-233. [Journal version of [5].]
- [14] M. BELLARE AND O. GOLDREICH. On defining proofs of knowledge. *Advances in Cryptology – CRYPTO '92*, Lecture Notes in Computer Science Vol. 740, E. Brickell ed., Springer, 1992.
- [15] M. BELLARE AND M. YUNG. Certifying permutations: Non-interactive zero-knowledge based on any trapdoor permutation. *Advances in Cryptology – CRYPTO '92*, Lecture Notes in Computer Science Vol. 740, E. Brickell ed., Springer, 1992.
- [16] M. BELLARE AND E. PETRANK. Making zero-knowledge provers efficient. *Proceedings of the 24th Annual Symposium on the Theory of Computing*, ACM, 1992.
- [17] M. BELLARE. A technique for upper bounding the spectral norm with applications to learning. *Proceedings of the Fifth Annual Workshop on Computational Learning Theory*, ACM, 1992.
- [18] M. BELLARE AND P. ROGAWAY. The complexity of approximating a nonlinear program. *Journal of Mathematical Programming B*, Vol. 69, No. 3, pp. 429–441, September 1995. Also in *Complexity of Numerical Optimization*, Ed. P. M. Pardalos, World Scientific, 1993.

- [19] M. BELLARE, O. GOLDBREICH AND S. GOLDWASSER. Randomness in interactive proofs. *Computational Complexity*, Vol. 3, No. 4, 1993, pp. 319–354. [Journal version of [11].]
- [20] M. BELLARE, S. GOLDWASSER, C. LUND AND A. RUSSELL. Efficient probabilistically checkable proofs and applications to approximation. *Proceedings of the 25th Annual Symposium on the Theory of Computing*, ACM, 1993.
- [21] M. BELLARE. Interactive proofs and approximation: reductions from two provers in one round. *Proceedings of the Second Israel Symposium on Theory and Computing Systems*, IEEE, 1993.
- [22] M. BELLARE AND P. ROGAWAY. Entity authentication and key distribution. *Advances in Cryptology – CRYPTO '93*, Lecture Notes in Computer Science Vol. 773, D. Stinson ed., Springer, 1993.
- [23] M. BELLARE AND P. ROGAWAY. Random oracles are practical: a paradigm for designing efficient protocols. *Proceedings of the 1st Annual Conference on Computer and Communications Security*, ACM, 1993.
- [24] M. BELLARE AND P. ROGAWAY. Optimal asymmetric encryption. *Advances in Cryptology – EUROCRYPT '94*, Lecture Notes in Computer Science Vol. 950, A. De Santis ed., Springer, 1994.
- [25] 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, Y. Desmedt ed., Springer, 1994.
- [26] M. BELLARE, O. GOLDBREICH AND S. GOLDWASSER. Incremental cryptography: The case of hashing and signing. *Advances in Cryptology – CRYPTO '94*, Lecture Notes in Computer Science Vol. 839, Y. Desmedt ed., Springer, 1994.
- [27] M. BELLARE, O. GOLDBREICH AND S. GOLDWASSER. Incremental cryptography with application to virus protection. *Proceedings of the 27th Annual Symposium on the Theory of Computing*, ACM, 1995.
- [28] M. BELLARE AND M. SUDAN. Improved non-approximability results. *Proceedings of the 26th Annual Symposium on the Theory of Computing*, ACM, 1994.
- [29] M. BELLARE AND S. GOLDWASSER. The complexity of decision versus search. *SIAM J. on Computing*, Vol. 23, No. 1, February 1994.
- [30] M. BELLARE AND J. ROMPEL. Randomness-efficient oblivious sampling. *Proceedings of the 35th Symposium on Foundations of Computer Science*, IEEE, 1994.
- [31] M. BELLARE AND P. ROGAWAY. Provably secure session key distribution– the three party case. *Proceedings of the 27th Annual Symposium on the Theory of Computing*, ACM, 1995.
- [32] 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, D. Coppersmith ed., Springer, 1995.
- [33] M. BELLARE, J. GARAY, R. HAUSER, A. HERZBERG, H. KRAWCZYK, M. STEINER, G. TSUDIK AND M. WAIDNER. iKP – A Family of Secure Electronic Payment Protocols. *Proceedings of the First USENIX Workshop on Electronic Commerce*, USENIX, 1995.
- [34] M. BELLARE, U. FEIGE AND J. KILIAN. On the role of shared randomness in two prover proof systems. *Proceedings of the Third Israel Symposium on Theory and Computing Systems*, IEEE, 1995.
- [35] W. AIELLO, M. BELLARE, AND R. VENKATESAN. Knowledge on the average— perfect, statistical and logarithmic. *Proceedings of the 27th Annual Symposium on the Theory of Computing*, ACM, 1995.
- [36] M. BELLARE, O. GOLDBREICH AND M. SUDAN. Free bits, PCPs and non-approximability– Towards tight results. *Proceedings of the 36th Symposium on Foundations of Computer Science*, IEEE, 1995.
- [37] M. BELLARE, D. COPPERSMITH, J. HÅSTAD, M. KIWI AND M. SUDAN. Linearity testing in characteristic two. *Proceedings of the 36th Symposium on Foundations of Computer Science*, IEEE, 1995.



- [38] M. BELLARE AND M. YUNG. Certifying permutations: Non-interactive zero-knowledge based on any trapdoor permutation. *Journal of Cryptology*, Vol. 9, No. 1, pp. 149–166, Winter 1996. [Journal version of [15].]
- [39] M. BELLARE AND P. ROGAWAY. The exact security of digital signatures: How to sign with RSA and Rabin. *Advances in Cryptology – EUROCRYPT ’96*, Lecture Notes in Computer Science Vol. 1070, U. Maurer ed., Springer, 1996.
- [40] M. BELLARE, R. CANETTI AND H. KRAWCZYK. Keying hash functions for message authentication. *Advances in Cryptology – CRYPTO ’96*, Lecture Notes in Computer Science Vol. 1109, N. Koblitz ed., Springer, 1996.
- [41] M. BELLARE, R. CANETTI AND H. KRAWCZYK. Pseudorandom functions revisited: The cascade construction and its concrete security. *Proceedings of the 37th Symposium on Foundations of Computer Science*, IEEE, 1996.
- [42] M. BELLARE, D. COPPERSMITH, J. HÅSTAD, M. KIWI AND M. SUDAN. Linearity testing in characteristic two. *IEEE Transactions on Information Theory* Vol. 42, No. 6, pp. 1781–1795, November 1996. [Journal version of [37].]
- [43] M. BELLARE, J. GARAY AND T. RABIN. Distributed pseudo-random bit generators: A new way to speed-up shared coin tossing. *Proceedings of the 15th Symposium on the Principles of Distributed Computing*, ACM, 1996.
- [44] M. BELLARE AND S. GOLDWASSER. Verifiable partial key escrow. *Proceedings of the 4th Annual Conference on Computer and Communications Security*, ACM, 1997.
- [45] M. BELLARE AND D. MICCIANCIO. A new paradigm for collision-free hashing: Incrementality at reduced cost. *Advances in Cryptology – EUROCRYPT ’97*, Lecture Notes in Computer Science Vol. 1233, W. Fumy ed., Springer, 1997.
- [46] M. BELLARE, M. JAKOBSSON AND M. YUNG. Round-optimal zero-knowledge arguments based on any one-way function. *Advances in Cryptology – EUROCRYPT ’97*, Lecture Notes in Computer Science Vol. 1233, W. Fumy ed., Springer, 1997.
- [47] M. BELLARE, S. GOLDWASSER AND D. MICCIANCIO. “Pseudo-random” number generation within cryptographic algorithms: The DSS case. *Advances in Cryptology – CRYPTO ’97*, Lecture Notes in Computer Science Vol. 1294, B. Kaliski ed., Springer, 1997.
- [48] M. BELLARE AND P. ROGAWAY. Collision-resistant hashing: towards making UOWHFs practical. *Advances in Cryptology – CRYPTO ’97*, Lecture Notes in Computer Science Vol. 1294, B. Kaliski ed., Springer, 1997.
- [49] M. BELLARE, R. IMPAGLIAZZO AND M. NAOR. Does parallel repetition lower the error in computationally sound protocols? *Proceedings of the 38th Symposium on Foundations of Computer Science*, IEEE, 1997.
- [50] M. BELLARE, A. DESAI, E. JOKIPII AND P. ROGAWAY. A concrete security treatment of symmetric encryption. *Proceedings of the 38th Symposium on Foundations of Computer Science*, IEEE, 1997.
- [51] M. BELLARE AND P. ROGAWAY. Minimizing the use of random oracles in authenticated encryption schemes. *First International Conference on Information and Communication Security (ICICS’97)*, Lecture Notes in Computer Science Vol. 1334, T. Okamoto and S. Qing, ed., Springer-Verlag, 1997.
- [52] 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, 1998.
- [53] M. BELLARE, J. GARAY AND T. RABIN. Fast batch verification for modular exponentiation and digital signatures. *Advances in Cryptology – EUROCRYPT ’98*, Lecture Notes in Computer Science Vol. 1403, K. Nyberg ed., Springer, 1998.

- [54] M. BELLARE, R. CANETTI AND H. KRAWCZYK. A modular approach to the design and analysis of authentication and key exchange protocols. *Proceedings of the 30th Annual Symposium on the Theory of Computing*, ACM, 1998.
- [55] M. BELLARE, S. HALEVI, A. SAHAI AND S. VADHAN. Many-to-one trapdoor functions and their relation to public-key cryptosystems. *Advances in Cryptology – CRYPTO '98*, Lecture Notes in Computer Science Vol. 1462, H. Krawczyk ed., Springer, 1998.
- [56] M. BELLARE, A. DESAI, D. POINTCHEVAL AND P. ROGAWAY. Relations among notions of security for public-key encryption schemes. *Advances in Cryptology – CRYPTO '98*, Lecture Notes in Computer Science Vol. 1462, H. Krawczyk ed., Springer, 1998.
- [57] W. AIELLO, M. BELLARE, G. DI CRESCENZO AND R. VENKATESAN. Security amplification by composition: The case of doubly-iterated, ideal ciphers. *Advances in Cryptology – CRYPTO '98*, Lecture Notes in Computer Science Vol. 1462, H. Krawczyk ed., Springer, 1998.
- [58] M. BELLARE, J. GARAY, C. JUTLA AND M. YUNG. *VarietyCash*: a Multi-purpose electronic payment system. *Proceedings of the 3rd Usenix Workshop on Electronic Commerce*, Usenix, 1998.
- [59] M. BELLARE, O. GOLDREICH AND M. SUDAN. Free bits, PCPs and non-approximability– Towards tight results. *SIAM J. on Computing*, Vol. 27, No. 3, 1998, pp. 804–915. [Journal version of [36].]
- [60] A. BAR-NOY, M. BELLARE, M. HALLDÓRSSON, H. SHACHNAI AND T. TAMIR. On chromatic sums and distributed resource allocation. *Information and Computation*, Vol. 140, No. 2, February 1998, pp. 183–202.
- [61] M. BELLARE AND P. ROGAWAY. On the construction of variable-input-length ciphers. *Proceedings of the 6th Workshop on Fast Software Encryption*, 1999.
- [62] M. BELLARE AND R. RIVEST. Translucent cryptography – An alternative to key escrow, and its implementation via fractional oblivious transfer. *Journal of Cryptology*, Vol. 12, No. 2, 1999, pp. 117–140.
- [63] J. AN AND M. BELLARE. Constructing VIL-MACs from FIL-MACs: Message authentication under weakened assumptions. *Advances in Cryptology – CRYPTO '99*, Lecture Notes in Computer Science Vol. 1666, M. Wiener ed., Springer, 1999.
- [64] M. BELLARE, O. GOLDREICH AND H. KRAWCZYK. Stateless evaluation of pseudorandom functions: Security beyond the birthday barrier. *Advances in Cryptology – CRYPTO '99*, Lecture Notes in Computer Science Vol. 1666, M. Wiener ed., Springer, 1999.
- [65] M. BELLARE AND S. MINER. A forward-secure digital signature scheme. *Advances in Cryptology – CRYPTO '99*, Lecture Notes in Computer Science Vol. 1666, M. Wiener ed., Springer, 1999.
- [66] M. BELLARE AND A. SAHAI. Non-Malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization. *Advances in Cryptology – CRYPTO '99*, Lecture Notes in Computer Science Vol. 1666, M. Wiener ed., Springer, 1999.
- [67] M. BELLARE, J. GARAY, R. HAUSER, A. HERZBERG, H. KRAWCZYK, M. STEINER, G. TSUDIK, E. VAN HERREVEGHEN AND M. WAIDNER. Design, implementation and deployment of the iKP secure electronic payment system. *IEEE Journal on Selected Areas in Communications*, Vol. 18, No. 4, 2000, pp. 611–627.
- [68] M. BELLARE, A. BOLDYREVA AND S. MICALI. Public-key Encryption in a Multi-User Setting: Security Proofs and Improvements. *Advances in Cryptology – EUROCRYPT '00*, Lecture Notes in Computer Science Vol. 1807, B. Preneel ed., Springer, 2000.
- [69] 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, 2000.

- [70] M. ABDALLA AND M. BELLARE. Increasing the lifetime of a key: A comparative analysis of the security of rekeying techniques. *Advances in Cryptology – ASIACRYPT '00*, Lecture Notes in Computer Science Vol. 1976, T. Okamoto ed., Springer, 2000.
- [71] M. BELLARE AND A. BOLDYREVA. The Security of Chaffing and Winnowing. *Advances in Cryptology – ASIACRYPT '00*, Lecture Notes in Computer Science Vol. 1976, T. Okamoto ed., Springer, 2000.
- [72] M. BELLARE AND P. ROGAWAY. Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. *Advances in Cryptology – ASIACRYPT '00*, Lecture Notes in Computer Science Vol. 1976, T. Okamoto ed., Springer, 2000.
- [73] M. BELLARE AND C. NAMPREMPRE. Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. *Advances in Cryptology – ASIACRYPT '00*, Lecture Notes in Computer Science Vol. 1976, T. Okamoto ed., Springer, 2000.
- [74] M. BELLARE, J. KILIAN AND P. ROGAWAY. The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences*, Vol. 61, No. 3, Dec 2000, pp. 362–399. [Journal version of [25].]
- [75] M. BELLARE, O. GOLDBREICH AND E. PETRANK. Uniform Generation of NP-witnesses using an NP-oracle. *Information and Computation*, Vol. 163, 2000, pp. 510–526.
- [76] M. BELLARE, C. NAMPREMPRE, D. POINTCHEVAL AND M. SEMANKO. The Power of RSA Inversion Oracles and the Security of Chaum’s RSA-Based Blind Signature Scheme. *Financial Cryptography '01*, Lecture Notes in Computer Science Vol. 2339, P. Syverson ed., Springer, 2001.
- [77] M. ABDALLA, M. BELLARE AND P. ROGAWAY. The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES. *Topics in Cryptology – CT-RSA '01*, Lecture Notes in Computer Science Vol. 2020, D. Naccache ed., Springer, 2001.
- [78] J. AN AND M. BELLARE. Does encryption with redundancy provide authenticity? *Advances in Cryptology – EUROCRYPT '01*, Lecture Notes in Computer Science Vol. 2045, B. Pfitzmann ed., Springer, 2001.
- [79] M. BELLARE, M. FISCHLIN, S. GOLDWASSER, AND S. MICALI. Identification Protocols Secure Against Reset Attacks. *Advances in Cryptology – EUROCRYPT '01*, Lecture Notes in Computer Science Vol. 2045, B. Pfitzmann ed., Springer, 2001.
- [80] M. BELLARE, A. BOLDYREVA, L. KNUDSEN AND C. NAMPREMPRE. On-line ciphers and the Hash-CBC construction. *Advances in Cryptology – CRYPTO '01*, Lecture Notes in Computer Science Vol. 2139, J. Kilian ed., Springer, 2001.
- [81] P. ROGAWAY, M. BELLARE, J. BLACK AND T. KROVETZ. OCB: A block cipher mode of operation for efficient authenticated encryption. *Proceedings of the 8th Annual Conference on Computer and Communications Security*, ACM, 2001.
- [82] M. BELLARE, A. BOLDYREVA, A. DESAI AND D. POINTCHEVAL. Key-privacy in public-key encryption. *Advances in Cryptology – ASIACRYPT '01*, Lecture Notes in Computer Science Vol. 2248, C. Boyd ed., Springer, 2001.
- [83] M. ABDALLA, J. AN, M. BELLARE AND C. NAMPREMPRE. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. *Advances in Cryptology – EUROCRYPT '02*, Lecture Notes in Computer Science Vol. 2332, L. Knudsen ed., Springer, 2002.
- [84] M. BELLARE AND A. PALACIO. GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attack. *Advances in Cryptology – CRYPTO '02*, Lecture Notes in Computer Science Vol. 2442, M. Yung ed., Springer, 2002.
- [85] M. BELLARE. A note on negligible functions. *Journal of Cryptology* Vol. 15, No. 4, 2002, pp. 271–284.

- [86] M. BELLARE, T. KOHNO AND C. NAMPREMPRE. Authenticated Encryption in SSH: Provably Fixing the SSH Binary Packet Protocol. *Proceedings of the 9th Annual Conference on Computer and Communications Security*, ACM, 2002.
- [87] M. BELLARE AND G. NEVEN. Transitive Signatures based on Factoring and RSA. *Advances in Cryptology – ASIACRYPT '02*, Lecture Notes in Computer Science Vol. 2501, Y. Zheng ed., Springer, 2002.
- [88] R. SANDHU, M. BELLARE AND R. GANESAN. Password-Enabled PKI: Virtual Smart-Cards versus Virtual Soft Tokens. *Proceeding of the 1st Annual PKI Research Workshop*, 2002.
- [89] M. BELLARE, A. BOLDYREVA AND J. STADDON. Randomness-reuse in multi-recipient encryption schemes. *Public-Key Cryptography '03*, Lecture Notes in Computer Science Vol. 2567, Y. Desmedt ed., Springer, 2003.
- [90] M. BELLARE AND B. YEE. Forward-security in private-key cryptography. *Topics in Cryptology – CT-RSA '03*, Lecture Notes in Computer Science Vol. 2612, M. Joye ed., Springer, 2003.
- [91] M. BELLARE AND T. KOHNO. A theoretical treatment of related-key attacks. *Advances in Cryptology – EUROCRYPT '03*, Lecture Notes in Computer Science Vol. 2656, E. Biham ed., Springer, 2003.
- [92] M. BELLARE, D. MICCIANCIO AND B. WARINSCHI. Foundations of group signatures: Formal definitions, simplified requirements and a construction based on general assumptions. *Advances in Cryptology – EUROCRYPT '03*, Lecture Notes in Computer Science Vol. 2656, E. Biham ed., Springer, 2003.
- [93] M. BELLARE, C. NAMPREMPRE, D. POINTCHEVAL AND M. SEMANKO. The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme. *Journal of Cryptology* Vol. 16, No. 3, 2003, pp. 185–215. [Journal version of [76].]
- [94] P. ROGAWAY, M. BELLARE AND J. BLACK. OCB: A block cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security (TISSEC)*, Vol. 6, Iss. 3, August 2003, pp. 365–403. [Journal version of [81].]
- [95] M. BELLARE, P. ROGAWAY AND D. WAGNER. The EAX Mode of Operation. *Fast Software Encryption '04*, Lecture Notes in Computer Science Vol. 3017, M. Robshaw ed., Springer, 2004.
- [96] M. BELLARE, A. BOLDYREVA AND A. PALACIO. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. *Advances in Cryptology – EUROCRYPT '04*, Lecture Notes in Computer Science Vol. 3027, C. Cachin and J. Camenisch ed., Springer, 2004.
- [97] M. BELLARE AND T. KOHNO. Hash function balance and its impact on birthday attacks. *Advances in Cryptology – EUROCRYPT '04*, Lecture Notes in Computer Science Vol. 3027, C. Cachin and J. Camenisch ed., Springer, 2004.
- [98] M. BELLARE, C. NAMPREMPRE AND G. NEVEN. Security proofs for identity-based identification and signature schemes. *Advances in Cryptology – EUROCRYPT '04*, Lecture Notes in Computer Science Vol. 3027, C. Cachin and J. Camenisch ed., Springer, 2004.
- [99] M. BELLARE, T. KOHNO AND C. NAMPREMPRE. Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm. *ACM Transactions on Information and System Security (TISSEC)*, Vol. 7, Iss. 2, May 2004, pp. 206–241. [Journal version of [86].]
- [100] M. BELLARE AND A. PALACIO. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. *Advances in Cryptology – CRYPTO '04*, Lecture Notes in Computer Science Vol. 3152, M. Franklin ed., Springer, 2004.
- [101] M. BELLARE AND A. PALACIO. Towards Plaintext-Aware Public-Key Encryption without Random Oracles. *Advances in Cryptology – ASIACRYPT '04*, Lecture Notes in Computer Science Vol. 3329, P. J. Lee ed., Springer, 2004.

- [102] M. BELLARE, H. SHI AND C. ZHANG. Foundations of Group Signatures: The Case of Dynamic Groups. *Topics in Cryptology – CT-RSA '05*, Lecture Notes in Computer Science Vol. 3376, A. Menezes ed., Springer, 2005.
- [103] M. BELLARE AND G. NEVEN. Transitive Signatures: New Schemes and Proofs. *IEEE Transactions on Information Theory*, Vol. 51, No. 6, June 2005, pp. 2133–2151. [Journal version of [87].]
- [104] M. ABDALLA, M. BELLARE, D. CATALANO, E. KILTZ, T. KOHNO, T. LANGE, J. MALONE-LEE, G. NEVEN, P. PAILLIER, AND H. SHI. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. *Advances in Cryptology – CRYPTO '05*, Lecture Notes in Computer Science Vol. 3621, V. Shoup ed., Springer, 2005.
- [105] M. BELLARE, K. PIETRZAK AND P. ROGAWAY. Improved Security Analyses for CBC MACs. *Advances in Cryptology – CRYPTO '05*, Lecture Notes in Computer Science Vol. 3621, V. Shoup ed., Springer, 2005.
- [106] M. BELLARE AND A. PALACIO. Protecting against key-exposure: Strongly key-insulated encryption with optimal threshold. *Applicable Algebra in Engineering, Communication and Computing*, Vol. 16, No. 6, February 2006, pp. 379–396.
- [107] M. BELLARE AND P. ROGAWAY. Code-based game-playing and the security of triple encryption. *Advances in Cryptology – EUROCRYPT '06*, Lecture Notes in Computer Science Vol. 4004, S. Vaudenay ed., Springer, 2006.
- [108] M. BELLARE. New proofs for NMAC and HMAC: Security without collision-resistance. *Advances in Cryptology – CRYPTO '06*, Lecture Notes in Computer Science Vol. 4117, C. Dwork ed., Springer, 2006.
- [109] M. BELLARE AND G. NEVEN. Multi-signatures in the plain public-key model and a generalized forking lemma. *Proceedings of the 13th Annual Conference on Computer and Communications Security*, ACM, 2006.
- [110] M. BELLARE, T. KOHNO AND V. SHOUP. Stateful public-key cryptosystems: How to encrypt with one 160-bit exponentiation. *Proceedings of the 13th Annual Conference on Computer and Communications Security*, ACM, 2006.
- [111] M. BELLARE AND T. RISTENPART. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. *Advances in Cryptology – ASIACRYPT '06*, Lecture Notes in Computer Science Vol. 4284, X. Lai and K. Chen ed., Springer, 2006.
- [112] M. BELLARE AND S. SHOUP. Two-Tier Signatures, Strongly Unforgeable Signatures, and Fiat-Shamir Without Random Oracles. *Public-Key Cryptography '07*, Lecture Notes in Computer Science Vol. 4450, T. Okamoto, X. Wang ed., Springer, 2007.
- [113] M. BELLARE, C. NAMPREMPRE, AND G. NEVEN. Unrestricted Aggregate Signatures. *ICALP '07*, Lecture Notes in Computer Science Vol. 4596, L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki ed., Springer, 2007.
- [114] M. BELLARE AND T. RISTENPART. Hash Functions in the Dedicated-Key Setting: Design Choices and MPP Transforms. *ICALP '07*, Lecture Notes in Computer Science Vol. 4596, L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki ed., Springer, 2007.
- [115] M. BELLARE AND G. NEVEN. Identity-Based Multi-signatures from RSA. *Topics in Cryptology – CT-RSA '07*, Lecture Notes in Computer Science Vol. 4377, M. Abe ed., Springer, 2007.
- [116] M. BELLARE, A. BOLDYREVA, A. O'NEILL. Deterministic and Efficiently Searchable Encryption. *Advances in Cryptology – CRYPTO '07*, Lecture Notes in Computer Science Vol. 4622, A. Menezes ed., Springer, 2007.
- [117] M. BELLARE AND P. ROGAWAY. Robust Computational Secret Sharing and a Unified Account of Classical Secret-Sharing Goals. *Proceedings of the 14th Annual Conference on Computer and Communications Security*, ACM, 2007.

- [118] M. BELLARE, A. BOLDYREVA, K. KUROSAWA AND J. STADDON. Multirecipient Encryption Schemes: How to Save on Bandwidth and Computation Without Sacrificing Security. *IEEE Transactions on Information Theory*, Vol. 53, No. 11, November 2007, pp. 3927–3943.
- [119] M. BELLARE AND S. SHOUP. Two-Tier Signatures from the Fiat-Shamir Transform, with Applications to Strongly Unforgeable and One-Time Signatures. *IET Information Security*, Vol. 2, No. 2, June 2008, pp. 47–63. [Journal version of [112].]
- [120] M. BELLARE, M. FISCHLIN, A. O’NEILL AND T. RISTENPART. Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. *Advances in Cryptology – CRYPTO ’08*, Lecture Notes in Computer Science Vol. 5157, D. Wagner ed., Springer, 2008.
- [121] M. ABDALLA, J. AN, M. BELLARE AND C. NAMPREMPRE. From Identification to Signatures Via the Fiat-Shamir Transform: Necessary and Sufficient Conditions for Security and Forward-Security. *IEEE Transactions on Information Theory*, Vol. 54, No. 8, August 2008, pp. 3631–3646. [Journal version of [83].]
- [122] M. ABDALLA, M. BELLARE, D. CATALANO, E. KILTZ, T. KOHNO, T. LANGE, J. MALONE-LEE, G. NEVEN, P. PAILLIER, AND H. SHI. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. *Journal of Cryptology* Vol. 21, No. 3, 2008, pp. 350–391. [Journal version of [104].]
- [123] M. BELLARE AND T. RISTOV. Hash Functions from Sigma Protocols and Improvements to VSH. *Advances in Cryptology – ASIACRYPT ’08*, Lecture Notes in Computer Science Vol. 5350, J. Pieprzyk ed., Springer, 2008.
- [124] M. BELLARE AND C. NAMPREMPRE. Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. *Journal of Cryptology* Vol. 21, No. 4, 2008, pp. 469–491. [Journal version of [73].]
- [125] M. BELLARE, C. NAMPREMPRE AND G. NEVEN. Security proofs for identity-based identification and signature schemes. *Journal of Cryptology* Vol. 22, No. 1, 2009, pp. 1–61. [Journal version of [98].]
- [126] M. BELLARE, S. DUAN AND A. PALACIO. Key insulation and intrusion resilience over a public channel. *Topics in Cryptology – CT-RSA ’09*, Lecture Notes in Computer Science Vol. 5473, M. Fischlin ed., Springer, 2009.
- [127] M. BELLARE AND T. RISTENPART. Simulation without the artificial abort: Simplified proof and improved concrete security for Waters’ IBE scheme. *Advances in Cryptology – EUROCRYPT ’09*, Lecture Notes in Computer Science Vol. 5479, A. Joux ed., Springer, 2009.
- [128] M. BELLARE, D. HOFHEINZ AND S. YILEK. Possibility and impossibility results for encryption and commitment secure under selective opening. *Advances in Cryptology – EUROCRYPT ’09*, Lecture Notes in Computer Science Vol. 5479, A. Joux ed., Springer, 2009.
- [129] M. BELLARE, T. RISTENPART, P. ROGAWAY AND T. STEGERS. Format-Preserving Encryption. *Selected Areas in Cryptography, 16th Annual International Workshop, SAC 2009*, Lecture Notes in Computer Science Vol. 5867, Springer 2009.
- [130] M. BELLARE, Z. BRAKERSKI, M. NAOR, T. RISTENPART, G. SEGEV, H. SHACHAM AND S. YILEK. Hedged Public-Key Encryption: How to Protect against Bad Randomness. *Advances in Cryptology – ASIACRYPT ’09*, Lecture Notes in Computer Science Vol. 5912, M. Matsui ed., Springer, 2009.
- [131] M. ABDALLA, M. BELLARE AND G. NEVEN. Robust Encryption. *Theory of Cryptography – TCC ’10*, Lecture Notes in Computer Science Vol. 5978, D. Micciancio ed., Springer, 2010.
- [132] T. ACAR, M. BELENKIY, M. BELLARE AND D. CASH. Cryptographic Agility and Its Relation to Circular Encryption. *Advances in Cryptology – EUROCRYPT ’10*, Lecture Notes in Computer Science Vol. 6110, H. Gilbert ed., Springer, 2010.

- [133] M. BELLARE AND D. CASH. Pseudorandom Functions and Permutations Provably Secure Against Related-Key Attack. *Advances in Cryptology – CRYPTO '10*, Lecture Notes in Computer Science Vol. 6223, T. Rabin ed., Springer, 2010.
- [134] M. BELLARE, B. WATERS AND S. YILEK. Identity-Based Encryption Secure against Selective Opening Attack. *Theory of Cryptography – TCC '11*, Lecture Notes in Computer Science Vol. 6597, Y. Ishai ed., Springer, 2011.
- [135] M. BELARE AND S. KEELVEEDHI. Authenticated and Misuse-Resistant Encryption of Key-Dependent Data. *Advances in Cryptology – CRYPTO '11*, Lecture Notes in Computer Science Vol. 6841, P. Rogaway ed., Springer, 2011.
- [136] M. BELLARE, D. CASH AND S. KEELVEEDHI. Ciphers that securely encipher their own keys. *Proceedings of the 18th Annual Conference on Computer and Communications Security*, ACM, 2011.
- [137] M. BELLARE, D. CASH AND R. MILLER. Cryptography Secure against Related-Key Attacks and Tampering. *Advances in Cryptology – ASIACRYPT '11*, Lecture Notes in Computer Science Vol. 7073, D. Lee and X. Wang ed., Springer, 2011.
- [138] M. BELLARE, R. DOWSLEY, B. WATERS AND S. YILEK. Standard security does not imply security against selective opening. *Advances in Cryptology – EUROCRYPT '12*, Lecture Notes in Computer Science Vol. 7237, D. Pointcheval and T. Johansson ed., Springer, 2012.
- [139] M. BELLARE, E. KILTZ, C PEIKERT AND B. WATERS. Identity-Based (Lossy) Trapdoor Functions and Applications. *Advances in Cryptology – EUROCRYPT '12*, Lecture Notes in Computer Science Vol. 7237, D. Pointcheval and T. Johansson ed., Springer, 2012.
- [140] M. BELLARE, S. TESSARO AND A. VARDY. Semantic Security for the Wiretap Channel. *Advances in Cryptology – CRYPTO '12*, Lecture Notes in Computer Science Vol. 7417, R. Safavi-Naini and R. Canetti ed., Springer, 2012.
- [141] M. BELLARE, T. RISTENPART AND S. TESSARO. Multi-Instance Security and its Application to Password-Based Cryptography. *Advances in Cryptology – CRYPTO '12*, Lecture Notes in Computer Science Vol. 7417, R. Safavi-Naini and R. Canetti ed., Springer, 2012.
- [142] M. BELLARE, V.T. HOANG AND P. ROGAWAY. Foundations of Garbled Circuits. *Proceedings of the 19th Annual Conference on Computer and Communications Security*, ACM, 2012.
- [143] M. BELLARE, K. PATERSON AND S. THOMSON. RKA-Security Beyond the Linear Barrier: IBE, Encryption and Signatures. *Advances in Cryptology – ASIACRYPT '12*, Lecture Notes in Computer Science Vol. 7658, X. Wang and K. Sako ed., Springer, 2012.
- [144] M. BELLARE, V.T. HOANG AND P. ROGAWAY. Adaptively Secure Garbling with Applications to One-Time Programs and Secure Outsourcing. *Advances in Cryptology – ASIACRYPT '12*, Lecture Notes in Computer Science Vol. 7658, X. Wang and K. Sako ed., Springer, 2012.
- [145] M. BELLARE, A. BOLDYREVA, L. KNUDSEN AND C. NAMPREMPRE. On-line ciphers and the hash CBC constructions. *Journal of Cryptology* Vol. 25, No. 4, 2012, pp. 640–679.
- [146] M. BELLARE, S. KEELVEEDHI AND T. RISTENPART. Message-locked encryption and secure deduplication. *Advances in Cryptology – EUROCRYPT '13*, Lecture Notes in Computer Science Vol. 7881, T. Johansson and P. Nguyen ed., Springer, 2013.
- [147] M. BELLARE, V.T. HOANG, S. KEELVEEDHI AND P. ROGAWAY. Efficient garbling from a fixed-key block-cipher. *Proceedings of the 2013 IEEE Symposium on Security and Privacy* .
- [148] M. BELLARE, S. KEELVEEDHI AND T. RISTENPART. DupLESS: Server-aided encryption for deduplicated storage. *Proceedings of the 22nd Usenix Security Symposium*, Usenix, 2013 .

- [149] M. BELLARE, V. T. HOANG AND S. KEELVEEDHI. Instantiating random oracles via UCEs. *Advances in Cryptology – CRYPTO '13*, Lecture Notes in Computer Science Vol. 8043, R. Canetti and J. Garay ed., Springer, 2013.
- [150] M. BELLARE AND A. O'NEILL. Semantically-secure functional encryption: Possibility results, impossibility results and the quest for a general definition. *Cryptology and Network Security, 12th International Conference (CANS 2013)*, *Proceedings*, Lecture Notes in Computer Science Vol. 8257, M. Abdalla, C. Nita-Rotaru and R. Dahab, eds., Springer, 2013.
- [151] M. BELLARE, S. MEIKLEJOHN AND S. THOMSON. Key-versatile signatures and applications: RKA, KDM and Joint Enc/Sig. *Advances in Cryptology – EUROCRYPT '14*, Lecture Notes in Computer Science Vol. 8441 , P. Nguyen and E. Oswald ed., Springer, 2014.
- [152] M. BELLARE AND G. FUCHSBAUER. Policy-based signatures. *Public-Key Cryptography '14*, Lecture Notes in Computer Science Vol. 8383, H. Krawczyk ed., Springer, 2014.
- [153] M. BELLARE, V. T. HOANG AND S. KEELVEEDHI. Cryptography from compression functions: The UCE bridge to the ROM. *Advances in Cryptology – CRYPTO '14*, Lecture Notes in Computer Science Vol. 8616/8617 , J. Garay and R. Gennaro ed., Springer, 2014.
- [154] M. BELLARE, K. PATERSON AND P. ROGAWAY. Security of symmetric encryption against mass surveillance. *Advances in Cryptology – CRYPTO '14*, Lecture Notes in Computer Science Vol. 8616/8617 , J. Garay and R. Gennaro ed., Springer, 2014.
- [155] M. BELLARE, I. STEPANOV AND S. TESSARO. Poly-Many Hardcore Bits for Any One-Way Function and a Framework for Differing-Inputs Obfuscation. *Advances in Cryptology - ASIACRYPT 14*, Lecture Notes in Computer Science Vol. 8874, P. Sarkar and T. Iwata eds, Springer, 2014.
- [156] M. BELLARE AND T. RISTOV. A characterization of chameleon hash functions and new, efficient designs. *Journal of Cryptology* Vol. 27, No. 4, 2014, pp. 799–823.
- [157] M. BELLARE, V. T. HOANG. Resisting randomness subversion: Efficient deterministic and hedged public-key encryption in the standard model. *Advances in Cryptology – EUROCRYPT 2015*, Lecture Notes in Computer Science Vol. 9057, E. Oswald and M. Fischlin eds., Springer 2015.
- [158] M. BELLARE AND S. KEELVEEDHI. Interactive Message-Locked Encryption and Secure Deduplication. *Public Key Cryptography, PKC '15*, Lecture Notes in Computer Science Vol. 9020, J. Katz ed, Springer, 2015.
- [159] M. BELLARE AND V. T. HOANG. Adaptive Witness Encryption and Asymmetric Password-Based Cryptography. *Public Key Cryptography, PKC '15*, Lecture Notes in Computer Science Vol. 9020, J. Katz ed, Springer, 2015.
- [160] M. BELLARE, R. DOWSLEY AND S. KEELVEEDHI. How Secure is Deterministic Encryption? *Public Key Cryptography, PKC '15*, Lecture Notes in Computer Science Vol. 9020, J. Katz ed, Springer, 2015.
- [161] M. BELLARE, D. HOFHEINZ AND E. KILTZ. Subtleties in the definition of IND-CCA: When and how should challenge decryption be disallowed? *Journal of Cryptology* Vol. 28, No. 1, 2015, pp. 29–48.
- [162] M. BELLARE, I. STEPANOV AND S. TESSARO. Contention in Cryptoland: Obfuscation, Leakage and UCE. *Theory of Cryptography – 13th International Conference, TCC 2016-A*, Lecture Notes in Computer Science Vol. 9563, E. Kushilevitz and T. Malkin, eds., Springer, 2016.
- [163] M. BELLARE AND I. STEPANOV. Point-Function Obfuscation: A Framework and Generic Constructions. *Theory of Cryptography – 13th International Conference, TCC 2016-A*, Lecture Notes in Computer Science Vol. 9563, E. Kushilevitz and T. Malkin, eds., Springer, 2016.
- [164] M. BELLARE, D. BERNSTEIN AND S. TESSARO. Hash-Function based PRFs: AMAC and its Multi-User Security. *Advances in Cryptology – EUROCRYPT 2016*, Lecture Notes in Computer Science Vol. 9665/9666, M. Fischlin and J. Coron, eds., Springer 2016.



- [165] M. BELLARE AND B. TACKMANN. Nonce-Based Cryptography: Retaining Security when Randomness Fails. *Advances in Cryptology – EUROCRYPT 2016*, Lecture Notes in Computer Science Vol. 9665/9666, M. Fischlin and J. Coron, eds., Springer 2016.
- [166] M. BELLARE, I. STEPANOV AND B. WATERS. New Negative Results on Differing-Inputs Obfuscation. *Advances in Cryptology – EUROCRYPT 2016*, Lecture Notes in Computer Science Vol. 9665/9666, M. Fischlin and J. Coron, eds., Springer 2016.
- [167] M. BELLARE, D. KANE AND P. ROGAWAY. Big-Key Symmetric Encryption: Resisting Key Exfiltration. *Advances in Cryptology – CRYPTO 2016*, Lecture Notes in Computer Science Vol. 9814, M. Robshaw and J. Katz, eds., Springer 2016.
- [168] M. BELLARE AND B. TACKMANN. The Multi-user Security of Authenticated Encryption: AES-GCM in TLS 1.3. *Advances in Cryptology – CRYPTO 2016*, Lecture Notes in Computer Science Vol. 9814, M. Robshaw and J. Katz, eds., Springer 2016.
- [169] M. BELLARE, V. T. HOANG AND S. TESSARO. Message-Recovery Attacks on Feistel-Based Format Preserving Encryption. *Proceedings of the 23rd Annual Conference on Computer and Communications Security, ACM*, 2016.
- [170] M. BELLARE, B. POETTERING AND D. STEBILA. From Identification to Signatures, Tightly: A Framework and Generic Transforms. *Advances in Cryptology – ASIACRYPT 2016*, Lecture Notes in Computer Science Vol. 10032, J. H. Cheon, T. Takagi, eds., 2016.
- [171] M. BELLARE, G. FUCHSBAUER AND A. SCAFURO. NIZKs with an Untrusted CRS: Security in the Face of Parameter Subversion. *Advances in Cryptology – ASIACRYPT 2016*, Lecture Notes in Computer Science Vol. 10032, J. H. Cheon, T. Takagi, eds., 2016.
- [172] M. BELLARE, B. POETTERING AND D. STEBILA. Detering Certificate Subversion: Efficient Double-Authentication-Preventing Signatures. *Public Key Cryptography, PKC '17*, Lecture Notes in Computer Science Vol. 10175, S. Fehr ed, Springer, 2017.
- [173] M. BELLARE, A. C. SINGH, J. JAEGER, M. NYAYAPATI AND I. STEPANOV. Ratcheted Encryption and Key Exchange: The Security of Messaging. *Advances in Cryptology – CRYPTO 2017*, Lecture Notes in Computer Science Vol. 10403, J. Katz and H. Shacham, eds., Springer 2017.
- [174] M. BELLARE, J. JAEGER AND J. LEN. Better Than Advertised: Improved Collision-Resistance Guarantees for MD-Based Hash Functions. *Proceedings of the 24th Annual Conference on Computer and Communications Security, ACM*, 2017.
- [175] M. BELLARE AND W. DAI. Defending Against Key Exfiltration: Efficiency Improvements for Big-Key Cryptography via Large-Alphabet Subkey Prediction. *Proceedings of the 24th Annual Conference on Computer and Communications Security, ACM*, 2017.
- [176] M. BELLARE AND V. T. HOANG. Identity-Based Format-Preserving Encryption. *Proceedings of the 24th Annual Conference on Computer and Communications Security, ACM*, 2017.
- [177] M. ABDALLA, M. BELLARE AND G. NEVEN. Robust Encryption. *Journal of Cryptology* Vol. 31, No. 2, 2018, pp. 307–350. [Journal version of [131].]
- [178] B. AUERBACH, M. BELLARE AND E. KILTZ. Public-Key Encryption Resistant to Parameter Subversion and Its Realization from Efficiently-Embeddable Groups. *Public Key Cryptography, PKC '18*, Lecture Notes in Computer Science Vol. 10769, M. Abdalla, R. Dahab, eds., Springer, 2018.

## 10.5 Technical reports and manuscripts

- [179] M. BELLARE. The spectral norm of finite functions. MIT Laboratory for Computer Science Technical Report TR-465, 1991.
- [180] M. BELLARE, E. BASTURK, C. S. CHOW, AND R. GUÉRIN. Secure transport protocols for high-speed networks. IBM Research Report 19981, March 1994.
- [181] M. BELLARE AND P. ROGAWAY. Distributing keys with perfect forward secrecy. Manuscript, January 1994.

## 10.6 Standards documents

- [182] H. KRAWCZYK, M. BELLARE AND R. CANETTI. HMAC: Keyed-Hashing for Message Authentication. *Internet RFC 2104*, February 1997.
- [183] M. ABDALLA, M. BELLARE AND P. ROGAWAY. DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem. Contribution to IEEE P1363, March 1999.

## 10.7 Patents

- [184] 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, and US Patent 5,757,913, May 1998.
- [185] 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.
- [186] M. BELLARE AND P. ROGAWAY. Block cipher mode of operation for secure length preserving encryption. US Patent 5,673,319, September 1997.
- [187] S. GOLDWASSER AND M. BELLARE. Time delayed key escrow. US Patent 5,768,388, June 1998.
- [188] M. BELLARE, J. GARAY, C. JUTLA AND M. YUNG. Method for electronic payment system with issuer control. US Patent 5,999,625, December 7, 1999.
- [189] M. BELLARE AND P. ROGAWAY. Probabilistic signature scheme. US Patent 6,266,771 B1, July 24, 2001.
- [190] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Authentication Protocol Using a Multi-Factor Asymmetric Key Pair. US Patent 7,386,720, June 10, 2008.
- [191] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Technique for asymmetric crypto-key generation. US Patent 7,565,527, July 21, 2009.
- [192] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Secure login using a multifactor split asymmetric crypto-key with persistent key security. US Patent 7,571,471, August 4, 2009.
- [193] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Asymmetric key pair having a kiosk mode. US Patent 7,596,697, September 29, 2009.
- [194] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Asymmetric key pair having a kiosk mode. US Patent 7,599,493, October 6, 2009.
- [195] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Multiple factor private portion of an asymmetric key. US Patent 7,630,493, December 8, 2009.

- [196] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Multifactor split asymmetric crypto-key with persistent key security. US Patent 7,734,045, June 8, 2010.
- [197] R. GANESAN, R. SANDHU, A. COTTRELL, B. SCHOPPERT AND M. BELLARE. Protecting one-time passwords against man-in-the-middle attacks. US Patent 7,840,993, November 23, 2010.
- [198] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Asymmetric cryptography with rolling key security. US Patent 8,099,607, 2012.
- [199] M. BELLARE AND P. ROGAWAY. Systems and methods for distributing and securing data. US Patent 8,155,322, 2012.
- [200] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Roaming utilizing an asymmetric key pair. US Patent 8,213,608, 2012.
- [201] R. SANDHU, B. SCHOPPERT, R. GANESAN, M. BELLARE AND C. DESA. Securing multifactor split key asymmetric crypto keys. US Patent 8,340,287, 2012.
- [202] R. ORSINI, M. O'HARE, M. BELLARE AND P. ROGAWAY. Systems and methods for securing data using multi-factor or keyed dispersal. US Patent 8,473,756, 2013.
- [203] C. MUELLER, M. BELLARE, S. YALE, P. HAZEL AND P. CATINELLA. System and method for variable length encryption. US Patent 8,769,279, 2014.
- [204] K. LAUTER, M. BELLARE, J. BENALOH, M. CHASE, E. HORVITZ AND C. KARKANIAS. User-specified sharing of data via policy and/or inference from a hierarchical cryptographic store. US Patent 8,837,718, 2014.
- [205] M. O'HARE, R. ORSINI, M. BELLARE AND P. ROGAWAY. Systems and methods for securing data using multi-factor or keyed dispersal. US Patent 9,098,718, 2015.
- [206] J. KUNIN, M. BELLARE, N. PASRICHA. System and method for generating and managing product authentication codes. US Patent 9,432,337, 2016.
- [207] M. BELLARE AND P. ROGAWAY. Systems and methods for distributing and securing data. US Patent 9,407,431, 2016.
- [208] C. MUELLER AND M. BELLARE. Variable-length cipher system and method. US Patent 9,361,617, 2016.
- [209] C. MUELLER, M. BELLARE, S. YALE, P. HAZEL AND P. CATINELLA. System and method for variable length encryption. US Patent 9,294,268, 2016.
- [210] M. O'HARE, R. ORSINI, M. BELLARE AND P. ROGAWAY. Systems and methods for securing data using multi-factor or keyed dispersal. US Patent 9,825,927, 2017.
- [211] M. BELLARE AND P. ROGAWAY. Systems and methods for distributing and securing data. US Patent 9,774,449, 2017.

## 11 Mentoring

### 11.1 Postdocs

- \* David Pointcheval. → Ecole Normale Supérieure, Paris, France.
- \* Eike Kiltz. → Ruhr Universität Bochum, Germany.
- \* David Cash. → Department of Computer Science, Rutgers University → Department of Computer Science, University of Chicago.

- \* Stefano Tessaro. → Department of Computer Science, University of California Santa Barbara → Department of Computer Science, University of Washington.
- \* Viet Tung Hoang. → Department of Computer Science, Florida State University.
- \* Bjoern Tackmann. → IBM Research Zurich.

## 11.2 Ph.D students

- \* Anand Desai, Ph.D 2000. → NTT Corporation.
- \* Jeehea Lee (née An), Ph.D 2001. → Softmax Corporation.
- \* Michel Abdalla, Ph.D 2001. → Ecole Normale Supérieure, Paris, France.
- \* Chanathip Namprempre, Ph.D 2002. → Assistant Professor, Department of Computer Science and Electrical Engineering, Thamassat University, Thailand.
- \* Alexandra Boldyreva, Ph.D 2004. → Assistant Professor, Department of Computer Science, Georgia Institute of Technology. (Ranked #8 by US News and World Report.)
- \* Adriana Palacio, Ph.D 2006. → Assistant Professor, Department of Computer Science, Bowdoin College.
- \* Tadayoshi Kohno, Ph.D 2006. → Assistant Professor, Department of Computer Science, University of Washington. (Ranked #6 by US News and World Report.)
- \* Anton Mityagin, Ph.D 2006. → Researcher, Microsoft Corporation.
- \* Tom Ristenpart, Ph.D 2009. → Assistant Professor, Department of Computer Science, University of Wisconsin Madison (ranked #13 by US News and World Report) → Associate Professor, Cornell University (ranked #6 by US News and World Report).
- \* Sarah Meiklejohn, Ph.D 2014. → Assistant Professor, UCL (University College London)
- \* Sriram Keelveedhi, Ph.D 2014. → Google.

## 11.3 MS students

- \* Eron Jokipii, MS 1997.
- \* Sara Miner, MS 2000.
- \* Michael Semanko, MS 2001.
- \* Haixia Shi, MS 2005.
- \* Chong Zhang, MS 2005.
- \* Sarah Shoup, MS 2008.
- \* Todor Ristov, MS 2009.
- \* Rafael Bao Dowsley, MS 2012.

## 11.4 BS students

- \* Adam O'Neill, BS 2005. → PhD Georgia Tech → Assistant Professor University of Massachusetts Amherst.
- \* Darrell Carbajal, BS 2006.
- \* Asha Camper Singh, BS 2016. → Salesforce
- \* Maya Nyayapati, BS 2016. → Salesforce
- \* Julia Len, BS 2018. → PhD Cornell
- \* Lucy Li, BS 2018. → PhD Cornell
- \* Jiahao Sun
- \* Matilda Backendal

## 12 Personal Information

US Citizen.