Mihir Bellare

Curriculum vitae

June 2023

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: `mbellare@ucsd.edu`
Web Page: `cseweb.ucsd.edu/~mihir`

Contents

1 Research areas

Cryptography and security, with emphasis on provable security; computational complexity 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

- IACR Test of Time Award, 2022, for publication [116] from Crypto 2007.
- IACR Test of Time Award, 2021, for publication [108] from Crypto 2006.
- Levchin Prize (Real World Cryptography), 2019.
- 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.)
- ACM CCS Test of Time Award, 2011, for publication [81].
- IACR Fellow, 2012 (IACR = International Association of Cryptologic Research.
- NSF CAREER award, 1996.
- h-index = 110 (Source: Google Scholar)
- Over 63,000 citations (Source: Google Scholar)
- 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 TLS; SSL (3.0 and 3.1); IPSec; SSH; S-HTTP; NetBSD. 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 (FPE) now in use for encryption of credit-card

numbers in millions of transactions by Voltage Security (HP) and other companies. FPE is also used to authenticate pharmaceuticals, in India and Africa, against the threat of drug counterfeiting, which claims hundreds of lives a year. Method standardized as the FF1 scheme in NIST Special Publication 800-38G.

- 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.
- 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 Pfitzmann; *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-resistent cryptography, 2015–2018. Amount: $500,000.

- NSF grant CNS-1717640, PI, SaTC:Core:Small:Foundations of applied cryptography, 2017–2020. Amount: $325,000.
- NSF grant, CNS-2154272, PI, SaTC:Core:Small:Practice-Driven Cryptographic Theory, 2022–2025. Amount: $500,000.

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; IndoCrypt 2020; RWC 2021; RWC 2022; Asiacrypt 2022; Eurocrypt 2023.
- 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 Coroporation.
- 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

- ∗ Introduction to modern cryptography (CSE107)– Undergraduate, CSE Dept., UCSD.
- ∗ Modern Cryptography (CSE207)– Graduate, CSE Dept., UCSD.
- ∗ Seeing the Invisible (CSE 209B)— Cryptography, Society and Beyond, Graduate, CSE Dept., UCSD.
- ∗ Advanced topics in cryptography (CSE291, CSE208)– Graduate, CSE Dept., UCSD. Topics vary and have included: electronic payment mechanisms, zero knowledge protocols, paring-based cryptography, obfuscation, random oracles.
- ∗ Cryptography and Information Security– A one week summer course, taught jointly with Shafi Goldwasser at MIT.
- ∗ Introduction to the theory of computation (CSE 105)– Undergraduate, CSE Dept., UCSD.
- ∗ Mathematics for algorithms and systems analysis (CSE 21)– Under, CSE Dept., UCSD.
- ∗ Computability and complexity (CSE 200)– Graduate, CSE Dept., UCSD.

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)	89
Other cryptography conferences (PKC, TCC, FSE, FC, CT-RSA, ICALP, ...)	33
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. Goldreich 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. Goldreich 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. Goldreich 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. Goldreich 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 comparitive 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. Goldreich 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. Desmdedt 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 blockcipher. *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. Stepanovs 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. Stepanovs 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. Stepanovs. 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. Stepanovs 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. Deterring 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. Stepanovs. 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.

[179] M. Backendal, M. Bellare, J. Sorrell and J. Sun. The Fiat-Shamir Zoo: Relating the Security of Different Signature Variants. *Secure IT Systems – 23rd Nordic Conference, NordSec 2018*, Lecture Notes in Computer Science Vol. 11252, N. Gruschka, ed., Springer 2018.

[180] M. Bellare, R. Ng and B. Tackmann. Nonces Are Noticed: AEAD Revisited. *Advances in Cryptology – CRYPTO 2019*, Lecture Notes in Computer Science Vol. 11692, A. Boldyreva, D. Micciancio, eds., Springer 2019.

[181] M. Bellare, W. Dai and L. Li. The Local Forking Lemma and Its Application to Deterministic Encryption. *Advances in Cryptology – ASIACRYPT 2019*, Lecture Notes in Computer Science Vol. 11923, S. Galbraith, S. Moriai, eds., 2019.

[182] V. Arte and M. Bellare. Dual-Mode NIZKs: Possibility and Impossibility Results for Property Transfer. *Progress in Cryptology – INDOCRYPT 2020*, Lecture Notes in Computer Science Vol. 12578, K. Bhargavan, E. Oswald, M. Prabhakaran, eds., Springer 2020.

[183] M. Bellare and W. Dai. The Multi-Base Discrete Logarithm Problem: Tight Reductions and Non-rewinding Proofs for Schnorr Identification and Signatures. *Progress in Cryptology – INDOCRYPT 2020*, Lecture Notes in Computer Science Vol. 12578, K. Bhargavan, E. Oswald, M. Prabhakaran, eds., Springer 2020.

[184] V. Arte, M. Bellare and L. Khati. Incremental Cryptography Revisited: PRFs, Nonces and Modular Design. *Progress in Cryptology – INDOCRYPT 2020*, Lecture Notes in Computer Science Vol. 12578, K. Bhargavan, E. Oswald, M. Prabhakaran, eds., Springer 2020.

[185] M. Bellare, H. Davis and F. Günther. Separate Your Domains: NIST PQC KEMs, Oracle Cloning and Read-Only Indifferentiability. *Advances in Cryptology – EUROCRYPT 2020*, Lecture Notes in Computer Science Vol. 12106, A. Canteaut, Y. Ishai, eds., Springer 2020.

[186] M. Bellare and I. Stepanovs. Security Under Message-Derived Keys: Signcryption in iMessage. *Advances in Cryptology – EUROCRYPT 2020*, Lecture Notes in Computer Science Vol. 12107, A. Canteaut, Y. Ishai, eds., Springer 2020.

[187] M. Bellare, W. Dai and P. Rogaway. Reimagining Secret Sharing: Creating a Safer and More Versatile Primitive by Adding Authenticity, Correcting Errors, and Reducing Randomness Requirements. *Proceedings on Privacy Enhancing Technologies*, Vol. 2020, No. 4, 2020.

[188] M. Bellare and W. Dai. Chain Reductions for Multi-signatures and the HBMS Scheme. *Advances in Cryptology – ASIACRYPT 2021*, Lecture Notes in Computer Science Vol. 13093, M. Tibouchi, H. Wang, eds., 2021.

[189] M. Bellare and V. T. Hoang. Efficient Schemes for Committing Authenticated Encryption. *Advances in Cryptology – EUROCRYPT 2022*, Lecture Notes in Computer Science Vol. 13276, O. Dunkelman and S. Dziembowski, eds., Springer 2022.

[190] M. Bellare, E. Crites, C. Komlo, M. Maller, S. Tessaro and C. Zhu. Better than Advertised Security for Non-interactive Threshold Signatures. *Advances in Cryptology – CRYPTO 2022*, Lecture Notes in Computer Science Vol. 13510, Y. Dodis, T. Shrimpton, eds., Springer 2022.

[191] M. Bellare, H. Davis and Z. Di. Hardening Signature Schemes via Derive-then-Derandomize: Stronger Security Proofs for EdDSA. *Public Key Cryptography, PKC '23*, Lecture Notes in Computer Science Vol. 13940, A. Boldyreva, V. Kolesnikov, eds., Springer, 2023.

[192] M. Bellare and L. Shea. Flexible Password-Based Encryption: Securing Cloud Storage and Provably Resisting Partitioning-Oracle Attacks. *Topics in Cryptology – CT-RSA '23*, Lecture Notes in Computer Science Vol. 13871, M. Rosulek ed., Springer 2023.

[193] M. Backendal, M. Bellare, F. Günther and M. Scarlata. When Messages are Keys: Is HMAC a Dual-PRF? *Advances in Cryptology – CRYPTO 2023*, Lecture Notes in Computer Science Vol. 14085, H. Handschuh, A. Lysyanskaya, eds., Springer 2023.

10.5 Technical reports and manuscripts

[194] M. Bellare. The spectral norm of finite functions. MIT Laboratory for Computer Science Technical Report TR–465, 1991.

[195] M. Bellare, E. Basturk, C. S. Chow, and R. Guérin. Secure transport protocols for high-speed networks. IBM Research Report 19981, March 1994.

[196] M. Bellare and P. Rogaway. Distributing keys with perfect forward secrecy. Manuscript, January 1994.

10.6 Standards documents

[197] H. Krawczyk, M. Bellare and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. *Internet RFC 2104*, February 1997.

[198] 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

[199] 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.

[200] 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.

[201] M. Bellare and P. Rogaway. Block cipher mode of operation for secure length preserving encryption. US Patent 5,673,319, September 1997.

[202] S. Goldwasser and M. Bellare. Time delayed key escrow. US Patent 5,768,388, June 1998.

[203] 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.

[204] M. Bellare and P. Rogaway. Probabilistic signature scheme. US Patent 6,266,771 B1, July 24, 2001.

[205] 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.

[206] 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.

[207] 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.

[208] 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.

[209] 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.

[210] 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.

[211] 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.

[212] 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.

[213] R. Sandhu, B. Schoppert, R Ganesan, M Bellare and C. deSa. Asymmetric crypto-graphy with rolling key security. US Patent 8,099,607, 2012.

[214] M. Bellare and P. Rogaway. Systems and methods for distributing and securing data. US Patent 8,155,322, 2012.

[215] R. Sandhu, B. Schoppert, R. Ganesan, M. Bellare and C. deSa. Roaming utilizing an asymmetric key pair. US Patent 8,213,608, 2012.

[216] R. Sandhu, B. Schoppert, R Ganesan, M Bellare and C. deSa. Securing multifactor split key asymmetric crypto keys. US Patent 8,340,287, 2012.

[217] 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.

[218] C. Mueller, M. Bellare, S. Yale, P. Hazel and P. Catinella. System and method for variable length encryption. US Patent 8,769,279, 2014.

[219] 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.

[220] 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.

[221] J. Kunin, M. Bellare, N. Pasricha. System and method for generating and managing product authentication codes. US Patent 9,432,337, 2016.

[222] M. Bellare and P. Rogaway. Systems and methods for distributing and securing data. US Patent 9,407,431, 2016.

[223] C. Mueller and M. Bellare. Variable-length cipher system and method. US Patent 9,361,617, 2016.

[224] C. Mueller, M. Bellare, S. Yale, P. Hazel and P. Catinella. System and method for variable length encryption. US Patent 9,294,268, 2016.

[225] 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.

[226] M. Bellare and P. Rogaway. Systems and methods for distributing and securing data. US Patent 9,774,449, 2017.

[227] C. Mueller, M. Bellare, S. Yale, P. Hazel and P. Catinella. System and method for variable length encryption. US Patent 10,007,910, 2018.

[228] P. Kolte, S. Jackson, P. Shanmugavelayutham, M. Bellare and N. Chenette. System and method for performing equality and less than operations on encrypted data with quasigroup operations. US Patent 11,190,339, 2021.

[229] P. Kolte, S. Jackson, P. Shanmugavelayutham and M. Bellare. System and method for adding and comparing integers encrypted with quasigroup operations in AES counter mode encryption. US Patent 11,101,980, 2021.

[230] M. Bellare and P. Kolte. Format preserving encryption (FPE) system and method for long strings. US Patent 11,637,690.

11 Mentoring

11.1 Postdocs

- David Pointcheval. → Professor, Ecole Normale Superièure, Paris, France.
- Eike Kiltz. → Professor, Ruhr Universitat Bochum, Germany.
- David Cash. → Professor, Department of Computer Science, Rutgers University → Professor, Department of Computer Science, University of Chicago.
- Stefano Tessaro. → Professor, Department of Computer Science, University of California Santa Barbara → Professor, Department of Computer Science, University of Washington.
- Viet Tung Hoang. → Professor, Department of Computer Science, Florida State University.
- Bjoern Tackmann. → IBM Research Zurich.
- Felix Günther. → Postdoc, ETH Zürich → IBM Research Zürich.
- Doreen Riepel.

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. → Professor, Ecole Normale Superièure, Paris, France → DFINITY
- Chanathip Namprempre, Ph.D 2002. → Professor, Department of Computer Science and Electrical Engineering, Thamassat University, Thailand.
- Alexandra Boldyreva, Ph.D 2004. → Professor, Department of Computer Science, Georgia Institute of Technology.
- Adriana Palacio, Ph.D 2006. → Professor, Department of Computer Science, Bowdoin College → ...

- ∗ Tadayoshi Kohno, Ph.D 2006. → Professor, Department of Computer Science, University of Washington.
- ∗ Anton Mityagin, Ph.D 2006. → Researcher, Microsoft Corporation → ...
- ∗ Tom Ristenpart, Ph.D 2009. → Professor, Department of Computer Science, University of Wisconsin Madison → Professor, Cornell University.
- ∗ Sarah Meiklejohn (co-advised with Stefan Savage), Ph.D 2014. → Professor, University College London.
- ∗ Sriram Keelveedhi, Ph.D 2014. → Google → Snap.
- ∗ Wei Dai, PhD 2021 → Anoma → Bain Capital.
- ∗ Ruth Ng (co-advised with David Cash), PhD 2021 → DSO National Laboratories.
- ∗ Igors Stepanovs, PhD 2019 → Postdoc, ETH Zurich → ...
- ∗ Joseph Jaeger, PhD 2019 → Postdoc, U. of Washington → Professor, Georgia Tech.
- ∗ Hannah Davis, current.
- ∗ Laura Shea (co-advised with Nadia Heninger), current.
- ∗ Rishabh Ranjan, current.

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 → 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.

  - Jiahao Sun. → PhD Georgia Tech
  - Matilda Backendal. → PhD ETH

12 Personal Information

US Citizen.