Literaturverzeichnis

[1] Adams, Carlisle und Stephen Farrell: *Internet X.509 Public Key Infrastructure: Certificate Management Protocol (CMP)*. RFC 4210, September 2005. `http://tools.ietf.org/html/rfc4210`.

[2] Adams, Carlisle und Steve Lloyd: *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley, 2. Auflage, 2002.

[3] Aggarwal, Divesh und Ueli M. Maurer: *Breaking RSA Generically Is Equivalent to Factoring*. In: Joux, Antoine (Herausgeber): *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 5479 der Reihe *Lecture Notes in Computer Science*, Seiten 36–53. Springer, 2009.

[4] Agrawal, Manindra, Neeraj Kayal und Nitin Saxena: *PRIMES is in P*. Annals of Mathematics, 160(2):781–793, 2004.

[5] Ajtai, Miklós: *Generating Hard Instances of Lattice Problems (Extended Abstract)*. In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (STOC 1996)*, Seiten 99–108. ACM Press, 1996.

[6] Ajtai, Miklós und Cynthia Dwork: *A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence*. In: *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing (STOC 1997)*, Seiten 284–293. ACM Press, 1997.

[7] Alexi, Werner, Benny Chor, Oded Goldreich und Claus-Peter Schnorr: *RSA and Rabin Functions: Certain Parts are as Hard as the Whole*. SIAM Journal on Computing, 17(2):194–209, 1988.

[8] Aoki, Kazumaro und Yu Sasaki: *Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1*. In: Halevi, Shai (Herausgeber): *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Proceedings*, Band 5677 der Reihe *Lecture Notes in Computer Science*, Seiten 70–89. Springer, 2009.

[9] Asokan, N., Valtteri Niemi und Pekka Laitinen: *On the Usefulness of Proof-of-Possession*. In: *Proceedings of the 2nd Annual PKI Research Workshop*, Seiten 122–127, 2003. `http://middleware.internet2.edu/pki03/PKI03-proceedings.html`.

[10] Austin, Tom: *PKI: A Wiley Tech Brief*. John Wiley & Sons, Inc., 2001.

[11] Barkan, Elad, Eli Biham und Nathan Keller: *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*. Journal of Cryptology, 21(3):392–429, 2008.

[12] Bauer, Friedrich L.: *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie*. Springer, 3. Auflage, 2000.

R. Küsters, T. Wilke, *Moderne Kryptographie*, DOI 10.1007/978-3-8348-8288-2,
© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

[13] Bellare, Mihir: *New Proofs for NMAC and HMAC: Security without Collision-Resistance*. In: Dwork, Cynthia (Herausgeber): *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Proceedings*, Band 4117 der Reihe *Lecture Notes in Computer Science*, Seiten 602–619. Springer, 2006.

[14] Bellare, Mihir, Alexandra Boldyreva und Adriana Palacio: *An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem*. In: Cachin, Christian und Jan Camenisch (Herausgeber): *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 3027 der Reihe *Lecture Notes in Computer Science*, Seiten 171–188. Springer, 2004.

[15] Bellare, Mihir, Ran Canetti und Hugo Krawczyk: *Keying Hash Functions for Message Authentication*. In: Koblitz, Neal (Herausgeber): *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Proceedings*, Band 1109 der Reihe *Lecture Notes in Computer Science*, Seiten 1–15. Springer, 1996.

[16] Bellare, Mihir, Anand Desai, Eron Jokipii und Phillip Rogaway: *A Concrete Security Treatment of Symmetric Encryption*. In: *Proceedings of the 38th Annual Symposium on Foundations of Computer Science (FOCS 1997)*, Seiten 394–403. IEEE Computer Society, 1997.

[17] Bellare, Mihir, Oded Goldreich und Anton Mityagin: *The Power of Verification Queries in Message Authentication and Authenticated Encryption*. Cryptology ePrint Archive, Report 2004/309, 2004. `http://eprint.iacr.org/`.

[18] Bellare, Mihir, Roch Guérin und Phillip Rogaway: *XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions*. In: Coppersmith, Don (Herausgeber): *Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Proceedings*, Band 963 der Reihe *Lecture Notes in Computer Science*, Seiten 15–28. Springer, 1995.

[19] Bellare, Mihir, Dennis Hofheinz und Eike Kiltz: *Subtleties in the Definition of IND-CCA: When and How Should Challenge-Decryption be Disallowed?* Cryptology ePrint Archive, Report 2009/418, 2009. `http://eprint.iacr.org/`.

[20] Bellare, Mihir, Joe Kilian und Phillip Rogaway: *The Security of Cipher Block Chaining*. In: Desmedt, Yvo (Herausgeber): *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Proceedings*, Band 839 der Reihe *Lecture Notes in Computer Science*, Seiten 341–358. Springer, 1994.

[21] Bellare, Mihir, Joe Kilian und Phillip Rogaway: *The Security of the Cipher Block Chaining Message Authentication Code*. Journal of Computer and System Sciences, 61(3):362–399, 2000.

[22] Bellare, Mihir und Tadayoshi Kohno: *Hash Function Balance and Its Impact on Birthday Attacks*. In: Cachin, Christian und Jan Camenisch (Herausgeber): *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 3027 der Reihe *Lecture Notes in Computer Science*, Seiten 401–418. Springer, 2004.

[23] Bellare, Mihir und Chanathip Namprempre: *Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm*. In: Okamoto, T. (Herausgeber): *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*, Band 1976 der Reihe *Lecture Notes in Computer Science*, Seiten 531–545. Springer, 2000.

[24] Bellare, Mihir und Phillip Rogaway: *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*. In: *ACM Conference on Computer and Communications Security (CCS 1993)*, Seiten 62–73. ACM Press, 1993.

[25] Bellare, Mihir und Phillip Rogaway: *Optimal asymmetric encryption — How to encrypt with RSA*. In: Santis, Alfredo De (Herausgeber): *Advances in Cryptology, EUROCRYPT 1994, Workshop on the Theory and Application of Cryptographic Techniques*, Band 950 der Reihe *Lecture Notes in Computer Science*, Seiten 92–111. Springer, 1995.

[26] Bellare, Mihir und Phillip Rogaway: *The Exact Security of Digital Signatures - How to Sign with RSA and Rabin*. In: Maurer, Ueli M. (Herausgeber): *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Proceeding*, Band 1070 der Reihe *Lecture Notes in Computer Science*, Seiten 399–416. Springer, 1996.

[27] Bellare, Mihir und Phillip Rogaway: *Code-Based Game-Playing Proofs and the Security of Triple Encryption*. Cryptology ePrint Archive, Report 2004/331, 2004. `http://eprint.iacr.org/`.

[28] Bellare, Mihir, Phillip Rogaway und David Wagner: *The EAX Mode of Operation*. In: Roy, Bimal K. und Willi Meier (Herausgeber): *Fast Software Encryption, 11th International Workshop, FSE 2004, Revised Papers*, Band 3017 der Reihe *Lecture Notes in Computer Science*, Seiten 389–407. Springer, 2004. Siehe auch `http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html` für weitere bei NIST eingereichte Betriebsarten.

[29] Bernstein, Daniel J.: *Cache-timing Attacks on AES*, 2005. Technischer Bericht. `http://cr.yp.to/papers.html#cachetiming`.

[30] Bertoni, Guido, Joan Daemen, Michael Peeters und Gilles Van Assche: *On the Indifferentiability of the Sponge Construction*. In: Smart, Nigel P. (Herausgeber): *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 4965 der Reihe *Lecture Notes in Computer Science*, Seiten 181–197. Springer, 2008.

[31] Biham, Eli und Orr Dunkelman: *A Framework for Iterative Hash Functions - HAIFA*. Cryptology ePrint Archive, Report 2007/278, 2007. `http://eprint.iacr.org/`.

[32] Biham, Eli und Adi Shamir: *Differential Cryptanalysis of DES-like Cryptosystems*. Journal of Cryptology, 4(1):3–72, 1991.

[33] Biham, Eli und Adi Shamir: *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993.

[34] Biham, Eli und Adi Shamir: *Differential Cryptanalysis of the Full 16-Round DES.* In: *Advances in Cryptology - CRYPTO '92, Proceedings of the 12th Annual International Cryptology Conference*, Band 740 der Reihe *Lecture Notes in Computer Science*, Seiten 487–496. Springer, 1993.

[35] Biryukov, Alex, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich und Adi Shamir: *Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds.* In: Gilbert, Henri (Herausgeber): *Advances in Cryptology - EUROCRYPT 2010, Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Band 6110 der Reihe *Lecture Notes in Computer Science*, Seiten 299–319. Springer, 2010.

[36] Biryukov, Alex, Dmitry Khovratovich und Ivica Nikolic: *Distinguisher and Related-Key Attack on the Full AES-256.* In: Halevi, Shai (Herausgeber): *Advances in Cryptology - CRYPTO 2009, Proceedings of the 29th Annual International Cryptology Conference*, Band 5677 der Reihe *Lecture Notes in Computer Science*, Seiten 231–249. Springer, 2009.

[37] Black, John und Phillip Rogaway: *CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions.* In: Bellare, Mihir (Herausgeber): *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Proceedings*, Band 1880 der Reihe *Lecture Notes in Computer Science*, Seiten 197–215. Springer, 2000.

[38] Black, John, Phillip Rogaway und Thomas Shrimpton: *Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV.* In: Yung, Moti (Herausgeber): *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Proceedings*, Band 2442 der Reihe *Lecture Notes in Computer Science*, Seiten 320–335. Springer, 2002.

[39] Bleichenbacher, Daniel: *Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1.* In: *Advances in Cryptology - CRYPTO 1998, 18th Annual Cryptology Conference. Proceedings*, Band 1462 der Reihe *Lecture Notes in Computer Science*, Seiten 1–12. Springer, 1998.

[40] Blum, Manuel und Silvio Micali: *How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits.* SIAM Journal on Computing, 13(4):850–864, 1984.

[41] Boldyreva, Alexandra, David Cash, Marc Fischlin und Bogdan Warinschi: *Foundations of Non-malleable Hash and One-Way Functions.* In: Matsui, Mitsuru (Herausgeber): *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*, Band 5912 der Reihe *Lecture Notes in Computer Science*, Seiten 524–541. Springer, 2009.

[42] Boneh, Dan: *The Decision Diffie-Hellman Problem.* In: Buhler, Joe (Herausgeber): *Algorithmic Number Theory, Proceedings of the Third International Symposium, ANTS-III*, Band 1423 der Reihe *Lecture Notes in Computer Science*, Seiten 48–63. Springer, 1998.

[43] Boneh, Dan: *Twenty years of attacks on the RSA cryptosystem.* Notices of the American Mathematical Society (AMS), 46(2):203–213, 1999.

[44] Boneh, Dan: *Simplified OAEP for the RSA and Rabin Functions*. In: Kilian, Joe (Herausgeber): *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Proceedings*, Band 2139 der Reihe *Lecture Notes in Computer Science*, Seiten 275–291. Springer, 2001.

[45] Brumley, David und Dan Boneh: *Remote timing attacks are practical*. Computer Networks, 48(5):701–716, 2005.

[46] Buhler, Joe P., Hendrik W. Lenstra und Carl B. Pomerance: *Factoring integers with the number field sieve*. In: Lenstra, Arjen K. und Jr. Hendrik W. Lenstra (Herausgeber): *The Development of the Number Field Sieve*, Seiten 50–94. Springer, 1993.

[47] Callas, Jon, Lutz Donnerhacke, Hal Finney, David Shaw und Rodney Thayer: *OpenPGP Message Format*. RFC 4880, November 2007. `http://tools.ietf.org/html/rfc4880`.

[48] Canetti, Ran, Oded Goldreich und Shai Halevi: *On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes*. In: Naor, Moni (Herausgeber): *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Proceedings*, Band 2951 der Reihe *Lecture Notes in Computer Science*, Seiten 40–57. Springer, 2004.

[49] Canetti, Ran, Oded Goldreich und Shai Halevi: *The random oracle methodology, revisited*. Journal of the ACM, 51(4):557–594, 2004.

[50] Chaum, David, Eugène van Heijst und Birgit Pfitzmann: *Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer*. In: Feigenbaum, Joan (Herausgeber): *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Proceedings*, Band 576 der Reihe *Lecture Notes in Computer Science*, Seiten 470–484. Springer, 1991.

[51] Cochran, Martin: *Notes on the Wang et al. 2^{63} SHA-1 Differential Path*. Cryptology ePrint Archive, Report 2007/474, 2007. `http://eprint.iacr.org/`.

[52] Cocks, Clifford: *Split Knowledge Generation of RSA Parameters*. In: Darnell, Michael (Herausgeber): *Cryptography and Coding, 6th IMA International Conference, Cirencester, Proceedings*, Band 1355 der Reihe *Lecture Notes in Computer Science*, Seiten 89–95. Springer, 1997.

[53] Contini, Scott und Yiqun Lisa Yin: *Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions*. In: Lai, Xuejia und Kefei Chen (Herausgeber): *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*, Band 4284 der Reihe *Lecture Notes in Computer Science*, Seiten 37–53. Springer, 2006.

[54] Coron, Jean-Sébastien: *On the Exact Security of Full Domain Hash*. In: Bellare, Mihir (Herausgeber): *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Proceedings*, Band 1880 der Reihe *Lecture Notes in Computer Science*, Seiten 229–235. Springer, 2000.

[55] Coron, Jean-Sébastien: *Optimal Security Proofs for PSS and Other Signature Schemes*. In: Knudsen, Lars R. (Herausgeber): *Advances in Cryptology - EUROCRYPT 2002,*

International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings, Band 2332 der Reihe *Lecture Notes in Computer Science*, Seiten 272–287. Springer, 2002.

[56] Coron, Jean-Sébastien, Yevgeniy Dodis, Cécile Malinaud und Prashant Puniya: *Merkle-Damgård Revisited: How to Construct a Hash Function*. In: *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptolog Conference, Proceedings*, Band 3621 der Reihe *Lecture Notes in Computer Science*, Seiten 430–448. Springer, 2005.

[57] Cramer, Ronald und Victor Shoup: *Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack*. SIAM Journal on Computing, 33(1):167–226, 2003.

[58] Crandall, Richard und Carl B. Pomerance: *Prime Numbers: A Computational Perspective*. Springer, 2. Auflage, 2005.

[59] Daemen, Joan und Vincent Rijmen: *The Design of Rijndael: AES — The Advanced Encryption Standard*. Springer, 2002.

[60] Damgård, Ivan: *Collision Free Hash Functions and Public Key Signature Schemes*. In: Chaum, David und Wyn L. Price (Herausgeber): *Advances in Cryptology - EUROCRYPT '87, Workshop on the Theory and Application of Cryptographic Techniques, Proceedings*, Band 304 der Reihe *Lecture Notes in Computer Science*, Seiten 203–216. Springer, 1987.

[61] Damgård, Ivan: *A Design Principle for Hash Functions*. In: Brassard, Gilles (Herausgeber): *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Proceedings*, Band 435 der Reihe *Lecture Notes in Computer Science*, Seiten 416–427. Springer, 1989.

[62] Daum, Magnus und Stefan Lucks: *The Story of Alice and her Boss: Hash Functions and the Blind Passenger Attack*. EUROCRYPT 2005 Rump Session. `http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/rump_ec05.pdf`.

[63] Dietzfelbinger, Martin: *Primality Testing in Polynomial Time — From Randomized Algorithms to "PRIMES is in P"*. Springer, 2004.

[64] Diffie, W. und M.E. Hellman: *New Directions in Cryptography*. IEEE Transactions on Information Theory, IT-22(6):644–654, November 1976.

[65] Dobbertin, Hans: *The status of MD5 after a recent attack*. CryptoBytes (the Technical Newsletter of RSA Laboratories), 2(1-6), 1996.

[66] Dobbertin, Hans: *Cryptanalysis of MD4*. Journal of Cryptology, 11(4):253–271, 1998.

[67] Dodis, Yevgeniy, Iftach Haitner und Aris Tentes: *On the (In)Security of RSA Signatures*. Cryptology ePrint Archive, Report 2011/087, 2011. `http://eprint.iacr.org/`.

[68] Dodis, Yevgeniy, Thomas Ristenpart und Thomas Shrimpton: *Salvaging Merkle-Damgård for Practical Applications*. In: *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 5479 der Reihe *Lecture Notes in Computer Science*, Seiten 371–388. Springer, 2009.

[69] Dolev, Danny, Cynthia Dwork und Moni Naor: *Non-malleable Cryptography*. SIAM Journal on Computing, 30(2):391–437, 2000.

[70] Electronic Frontier Foundation: *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1998.

[71] ElGamal, Taher: *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. In: *Advances in Cryptology, Proceedings of CRYPTO '84*, Band 196 der Reihe *Lecture Notes in Computer Science*, Seiten 10–18. Springer, 1985.

[72] Ellision, Carl und Bruce Schneier: *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure*. Computer Security Journal, 16(1):1–7, 2000.

[73] Feistel, Horst: *Cryptography and Computer Privacy*. Scientific American, 228(5):15–23, 1973.

[74] Fiat, Amos und Adi Shamir: *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*. In: *Advances in Cryptology - CRYPTO '86, Proceedings*, Band 263 der Reihe *Lecture Notes in Computer Science*, Seiten 186–194. Springer, 1986.

[75] Fouque, Pierre-Alain, Gaëtan Leurent und Phong Q. Nguyen: *Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5*. In: Menezes, Alfred (Herausgeber): *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Proceedings*, Band 4622 der Reihe *Lecture Notes in Computer Science*, Seiten 13–30. Springer, 2007.

[76] Friedman, William F.: *Edgar Allan Poe, Cryptographer*. American Literature, 8(3):266–280, November 1936.

[77] Fujisaki, Eiichiro, Tatsuaki Okamoto, David Pointcheval und Jacques Stern: *RSA-OAEP Is Secure under the RSA Assumption*. In: Kilian, Joe (Herausgeber): *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Proceedings*, Band 2139 der Reihe *Lecture Notes in Computer Science*, Seiten 260–274. Springer, 2001.

[78] Garcia, Flavio D., Peter van Rossum, Roel Verdult und Ronny Wichers Schreur: *Wirelessly Pickpocketing a Mifare Classic Card*. In: *30th IEEE Symposium on Security and Privacy (S&P 2009)*, Seiten 3–15. IEEE Computer Society, 2009.

[79] Goethe, Johann Wolfgang von: *Wilhelm Meisters Lehrjahre*. Unger, 1795. Siehe auch `http://www.gutenberg.org/browse/authors/g` für eine elektronische Fassung.

[80] Goldreich, Oded: *Foundations of Cryptography – Basic Tools*, Band I. Cambridge University Press, 2001.

[81] Goldreich, Oded: *Foundations of Cryptography – Basic Applications*, Band II. Cambridge University Press, 2004.

[82] Goldreich, Oded, Shafi Goldwasser und Silvio Micali: *How to Construct Random Functions (Extended Abstract).* In: *25th Annual Symposium on Foundations of Computer Science (FOCS 1984)*, Seiten 464–479. IEEE Computer Society, 1984.

[83] Goldreich, Oded, Shafi Goldwasser und Silvio Micali: *On the Cryptographic Applications of Random Functions.* In: Blakley, G. R. und David Chaum (Herausgeber): *Advances in Cryptology, Proceedings of CRYPTO '84, Proceedings*, Band 196 der Reihe *Lecture Notes in Computer Science*, Seiten 276–288. Springer, 1984.

[84] Goldreich, Oded, Shafi Goldwasser und Silvio Micali: *How to construct random functions.* Journal of the ACM, 33(4):792–807, 1986.

[85] Goldwasser, Shafi und Silvio Micali: *Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information.* In: *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, Seiten 365–377. ACM Press, 1982.

[86] Goldwasser, Shafi und Silvio Micali: *Probabilistic Encryption.* Journal of Computer and System Sciences, 28(2):270–299, April 1984. Zunächst erschienen in STOC 1982.

[87] Goldwasser, Shafi, Silvio Micali und Ron L. Rivest: *A digital signature scheme secure against adaptive chosen-message attacks.* SIAM Journal on Computing, 17(2):281–308, 1988.

[88] Goldwasser, Shafi, Silvio Micali und Andrew Chi-Chih Yao: *Strong Signature Schemes.* In: *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, Seiten 431–439. ACM Press, 1983.

[89] Gordon, Dan M.: *Discrete logarithms in GF(p) using the number field sieve.* SIAM Journal on Discrete Mathematics, 6:124–138, 1993.

[90] Gutmann, Peter: *PKI: it's not dead, just resting.* Computer, 35(8):41–49, August 2002.

[91] Håstad, Johan und Mats Näslund: *The security of all RSA and discrete log bits.* Journal of the ACM, 51(2):187–230, 2004.

[92] Heys, Howard M.: *A Tutorial on Linear and Differential Cryptanalysis.* Cryptologia, 26:189–221, 2002.

[93] Hohenberger, Susan und Brent Waters: *Short and Stateless Signatures from the RSA Assumption.* In: Halevi, Shai (Herausgeber): *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Proceedings*, Band 5677 der Reihe *Lecture Notes in Computer Science*, Seiten 654–670. Springer, 2009.

[94] Impagliazzo, Russell und Michael Luby: *One-way Functions are Essential for Complexity Based Cryptography (Extended Abstract).* In: *30th Annual Symposium on Foundations of Computer Science (FOCS 1989)*, Seiten 230–235. IEEE Computer Society, 1989.

[95] Iwata, Tetsu und Kaoru Kurosawa: *OMAC: One-Key CBC MAC*. In: Johansson, Thomas (Herausgeber): *Fast Software Encryption, 10th International Workshop, FSE 2003, Revised Papers*, Band 2887 der Reihe *Lecture Notes in Computer Science*, Seiten 129–153. Springer, 2003.

[96] Iwata, Tetsu und Kaoru Kurosawa: *Stronger Security Bounds for OMAC, TMAC, and XCBC*. In: Johansson, Thomas und Subhamoy Maitra (Herausgeber): *Progress in Cryptology - INDOCRYPT 2003, 4th International Conference on Cryptology in India, Proceedings*, Band 2904 der Reihe *Lecture Notes in Computer Science*, Seiten 402–415. Springer, 2003.

[97] Joux, Antoine, David Naccache und Emmanuel Thomé: *When e-th Roots Become Easier Than Factoring*. In: Kurosawa, Kaoru (Herausgeber): *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*, Band 4833 der Reihe *Lecture Notes in Computer Science*, Seiten 13–28. Springer, 2007.

[98] Kahn, David: *The Codebreakers: The Story of Secret Writing*. Scribner, New York City, 2. Auflage, 1996.

[99] Kasiski, Friedrich Wilhelm: *Die Geheimschriften und die Dechiffrierkunst*. Mittler & Sohn, Berlin, 1863.

[100] Katz, Jonathan: *Digital Signatures*. Springer, 1. Auflage, 2010.

[101] Katz, Jonathan und Yehuda Lindell: *Introduction to Modern Cryptography*. Chapman & Hall/CRC Press, 2008.

[102] Kaufman, Charlie, Raida Perlman und Mike Speciner: *Network Security: Private Communication in a Public World*. Series in Computer Networking and Distributed Systems. Prentice Hall, 2. Auflage, 2002.

[103] Kerckhoffs, Auguste: *La cryptographie militaire*. Journal des Sciences militaires, IX :5–38, Januar 1883.

[104] Kerckhoffs, Auguste: *La Cryptographie Militaire*. Librairie Militaire de L. Baudoin & Cie., Paris, 1883.

[105] Kim, Jongsung, Alex Biryukov, Bart Preneel und Seokhie Hong: *On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract)*. In: Prisco, Roberto De und Moti Yung (Herausgeber): *Security and Cryptography for Networks, 5th International Conference, SCN 2006, Proceedings*, Band 4116 der Reihe *Lecture Notes in Computer Science*, Seiten 242–256. Springer, 2006.

[106] Kleinjung, Thorsten, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman J. J. te Riele, Andrey Timofeev und Paul Zimmermann: *Factorization of a 768-Bit RSA Modulus*. In: Rabin, Tal (Herausgeber): *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference. Proceedings*, Band 6223 der Reihe *Lecture Notes in Computer Science*, Seiten 333–350. Springer, 2010.

[107] Koblitz, Neal: *Elliptic curve cryptosystems*. Mathematics of Computation, 48:203–209, 1987.

[108] Koblitz, Neal: *A Course in Number Theory and Cryptography*. Graduate Texts in Mathematics. Springer, 2. Auflage, 2006.

[109] Kocher, Paul C.: *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*. In: *Advances in Cryptology - CRYPTO '96, Proceedings of the 16th Annual International Cryptology Conference*, Band 1109 der Reihe *Lecture Notes in Computer Science*, Seiten 104–113. Springer, 1996.

[110] Kohlas, Reto und Ueli M. Maurer: *Reasoning about Public-Key Certification: On Bindings between Entities and Public Keys*. In: Franklin, Matthew K. (Herausgeber): *Financial Cryptography, Third International Conference, FC'99, Proceedings*, Band 1648 der Reihe *Lecture Notes in Computer Science*, Seiten 86–103. Springer, 1999.

[111] Kohnfelder, Loren M.: *Towards a practical public-key cryptosystem*. Bachelorarbeit, MIT, Mai 1978.

[112] Krawczyk, Hugo: *The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?)*. In: Kilian, Joe (Herausgeber): *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Proceedings*, Band 1462 der Reihe *Lecture Notes in Computer Science*, Seiten 310–331. Springer, 2001.

[113] Krawczyk, Hugo, Mihir Bellare und Ran Canetti: *HMAC: Keyed-hashing for message authentication*. RFC 2104, February 1997. `http://www.ietf.org/rfc/rfc2104.txt`.

[114] Krengel, Ulrich: *Einführung in die Wahrscheinlichkeitstheorie und Statistik*. Vieweg, Braunschweig u. a., 3. Auflage, 1991.

[115] Leurent, Gaëtan: *MD4 is Not One-Way*. In: Nyberg, Kaisa (Herausgeber): *Fast Software Encryption, 15th International Workshop, FSE 2008, Revised Selected Papers*, Band 5086 der Reihe *Lecture Notes in Computer Science*, Seiten 412–428. Springer, 2008.

[116] Luby, Michael und Charles Rackoff: *How to Construct Pseudorandom Permutations from Pseudorandom Functions*. SIAM Journal on Computing, 17(2):373–386, 1988.

[117] Lucks, Stefan: *Design Principles for Iterated Hash Functions*. Cryptology ePrint Archive, Report 2004/253, 2004. `http://eprint.iacr.org/`.

[118] Lyubashevsky, Vadim, Daniele Micciancio, Chris Peikert und Alon Rosen: *SWIFFT: A Modest Proposal for FFT Hashing*. In: Nyberg, Kaisa (Herausgeber): *Fast Software Encryption, 15th International Workshop, FSE 2008, Revised Selected Papers*, Band 5086 der Reihe *Lecture Notes in Computer Science*, Seiten 54–72. Springer, 2008.

[119] Matsui, Mitsuru: *Linear Cryptanalysis Method for DES Cipher*. In: Helleseth, Tor (Herausgeber): *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, Proceedings*, Band 765 der Reihe *Lecture Notes in Computer Science*, Seiten 386–397. Springer, 1994.

[120] Matsui, Mitsuru: *The First Experimental Cryptanalysis of the Data Encryption Standard*. In: Desmedt, Yvo (Herausgeber): *Advances in Cryptology - CRYPTO '94, Proceedings of the 14th Annual International Cryptology Conference*, Band 839 der Reihe *Lecture Notes in Computer Science*, Seiten 1–11. Springer, 1994.

[121] Maurer, Ueli M.: *New Approaches to Digital Evidence*. Proceedings of the IEEE, 92(6):933–947, 2004.

[122] Maurer, Ueli M. und Stefan Wolf: *The Relationship Between Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms*. SIAM Journal on Computing, 28(5):1689–1721, 1999.

[123] Menezes, Alfred J., Paul C. van Oorschot und Scott A. Vanstone: *Handbook of applied cryptography*. CRC Press series on discrete mathematics and its applications. CRC Press, 1996.

[124] Merkle, Ralph C.: *One Way Hash Functions and DES*. In: Brassard, Gilles (Herausgeber): *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Proceedings*, Band 435 der Reihe *Lecture Notes in Computer Science*, Seiten 428–446. Springer, 1989.

[125] Micciancio, Daniele und Shafi Goldwasser: *Complexity of Lattice Problems — A Cryptographic Perspective*. Springer International Series in Engineering and Computer Science. Springer, 2002.

[126] Miller, Gary L.: *Riemann's Hypothesis and Tests for Primality*. Journal of Computer and System Sciences, 13(3):300–317, 1976.

[127] Miller, Victor S.: *Use of Elliptic Curves in Cryptography*. In: Williams, Hugh C. (Herausgeber): *Advances in Cryptology - CRYPTO '85, Proceedings*, Band 218 der Reihe *Lecture Notes in Computer Science*, Seiten 417–426. Springer, 1986.

[128] Miyaguchi, Shoji, Kazuo Ohta und Masahiko Iwata: *Confirmation that Some Hash Functions Are Not Collision Free*. In: Damgård, Ivan (Herausgeber): *Advances in Cryptology – EUROCRYPT '90, Workshop on the Theory and Application of Cryptographic Techniques, Proceedings*, Band 473 der Reihe *Lecture Notes in Computer Science*, Seiten 326–343. Springer, 1991.

[129] Naor, Moni und Moti Yung: *Universal One-Way Hash Functions and their Cryptographic Applications*. In: *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, Seiten 33–43. ACM Press, 1989.

[130] Naor, Moni und Moti Yung: *Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks*. In: *Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing (STOC 1990)*, Seiten 427–437. ACM Press, 1990.

[131] Nielsen, Michael A. und Isaac L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[132] Odlyzko, Andrew M.: *Discrete Logarithms: The Past and the Future*. Designs, Codes, and Cryptography, 19(2/3):129–145, 2000.

[133] Pohlig, Stephen C. und Martin E. Hellman: *An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance*. IEEE Transactions on Information Theory, 24(1):106–110, 1978.

[134] Pollard, John M.: *Factoring with cubic integers*. In: Lenstra, Arjen K. und Jr. Hendrik W. Lenstra (Herausgeber): *The Development of the Number Field Sieve*, Seiten 4–10. Springer, 1993.

[135] Quisquater, Jean-Jaques und François Koene: *Side channel attacks: State of the Art*, October 2002. `http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf`. Aktuellere Informationen findet man z.B. unter `http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html` sowie `Sidechannelattacks.com`.

[136] Rabin, Michael O.: *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*. Technischer Bericht MIT/LCS/TR-212, MIT Laboratory for Computer Science, January 1979.

[137] Rabin, Michael O.: *Probabilistic Algorithm for Testing Primality*. Journal of Number Theory, 12(1):128–138, 1980.

[138] Rackoff, Charles und Daniel R. Simon: *Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack*. In: Feigenbaum, Joan (Herausgeber): *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Proceedings*, Band 576 der Reihe *Lecture Notes in Computer Science*, Seiten 433–444. Springer, 1992.

[139] Ristenpart, Thomas und Scott Yilek: *The Power of Proofs-of-Possession: Securing Multiparty Signatures against Rogue-Key Attacks*. In: Naor, Moni (Herausgeber): *Advances in Cryptology - EUROCRYPT 2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 4515 der Reihe *Lecture Notes in Computer Science*, Seiten 228–245. Springer, 2007.

[140] Rivest, Ronald L., Adi Shamir und Leonard M. Adleman: *A Method for Obbtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, 21(2):120–126, 1978.

[141] Rivest, Ron: *The MD5 Message-Digest Algorithm*. RFC 1321, April 1992. `http://tools.ietf.org/html/rfc1321`.

[142] Rogaway, Phillip und Thomas Shrimpton: *Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance*. In: Roy, Bimal K. und Willi Meier (Herausgeber): *Fast Software Encryption, 11th International Workshop, FSE 2004*, Band 3017 der Reihe *Lecture Notes in Computer Science*, Seiten 371–388. Springer, 2004.

[143] Rompel, John: *One-Way Functions are Necessary and Sufficient for Secure Signatures*. In: *Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing*, Seiten 387–394. ACM Press, 1990.

[144] Sasaki, Yu und Kazumaro Aoki: *Finding Preimages in Full MD5 Faster Than Exhaustive Search*. In: Joux, Antoine (Herausgeber): *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 5479 der Reihe *Lecture Notes in Computer Science*, Seiten 134–152. Springer, 2009.

[145] Schaad, Jim: *Internet X.509 Public Key Infrastructure: Certificate Request Message Format (CRMF)*. RFC 4211, September 2005. `http://www.ietf.org/rfc/rfc4211.txt`.

[146] Shanks, Daniel: *Class number, a theory of factorization and genera*. In: *Proceedings Symposia Pure Mathematics 20*, Seiten 415–440. AMS, Providence, R.I., 1971.

[147] Shannon, Claude Elwood: *A Mathematical Theory of Communication, Part I*. Bell System Technical Journal, 27:379–423, July 1948.

[148] Shannon, Claude Elwood: *A Mathematical Theory of Communication, Part II*. Bell System Technical Journal, 27:623–656, October 1948.

[149] Shannon, Claude Elwood: *Communication Theory of Secrecy Systems*. Bell System Technical Journal, 28(4):656–715, 1949. Ursprünglich erschienen in einem vertraulichen Bericht vom 1. September 1945 mit dem Titel *A Mathematical Theory of Cryptography*.

[150] Shor, Peter W.: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing, 26(5):1484–1509, 1997.

[151] Shoup, Victor: *OAEP Reconsidered*. In: Kilian, Joe (Herausgeber): *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Proceedings*, Band 2139 der Reihe *Lecture Notes in Computer Science*, Seiten 239–259. Springer, 2001.

[152] Shoup, Victor: *Sequences of games: a tool for taming complexity in security proofs*. Cryptology ePrint Archive, Report 2004/332, 2004. `http://eprint.iacr.org/`.

[153] Shoup, Victor: *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2005. Online verfügbar unter `http://www.shoup.net/ntb`.

[154] Singh, Simon: *The code book: the evolution of secrecy from Mary, Queen of Scots, to quantum cryptography*. Doubleday New York, NY, USA, 1999.

[155] Stevens, Marc, Arjen K. Lenstra und Benne de Weger: *Predicting the winner of the 2008 US presidential elections using a Sony PlayStation 3*. `http://www.win.tue.nl/hashclash/Nostradamus/`, 2007.

[156] Stevens, Marc, Alexander Sotirov, Jacob Appelbaum, Arjen K. Lenstra, David Molnar, Dag Arne Osvik und Benne de Weger: *Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate*. In: Halevi, Shai (Herausgeber): *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Proceedings*, Band 5677 der Reihe *Lecture Notes in Computer Science*, Seiten 55–69. Springer, 2009.

[157] Stinson, Douglas R.: *Cryptography — Theory and Practice*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, 3. Auflage, 2006.

[158] Suetonius Tranquillus, Gaius: *Vita Divi Iuli, 56*. `http://www.thelatinlibrary.com/suetonius/suet.caesar.html#56`.

[159] Tromer, Eran, Dag Arne Osvik und Adi Shamir: *Efficient Cache Attacks on AES, and Countermeasures*. Journal of Cryptology, 23(1):37–71, 2010.

[160] Tsiounis, Yiannis und Moti Yung: *On the Security of ElGamal Based Encryption*. In: Imai, Hideki und Yuliang Zheng (Herausgeber): *Public Key Cryptography, First International Workshop on Practice and Theory in Public Key Cryptography, PKC '98, Proceedings*, Band 1431 der Reihe *Lecture Notes in Computer Science*, Seiten 117–134. Springer, 1998.

[161] Vernam, Gilbert S.: *US Patent no. 1,310,719*. Beziehbar unter `http://patft.uspto.gov/netahtml/PTO/srchnum.htm` mit Suchbegriff »Utility: 1,310,719«. 22. Juli 1919.

[162] Vigenère, Blaise de: *Traicté Chiffres*. In: *Manuel de cryptographie*. Payot, Paris, 1951. Abschnitt 145.

[163] Wang, Xiaoyun, Xuejia Lai, Dengguo Feng, Hui Chen und Xiuyuan Yu: *Cryptanalysis of the Hash Functions MD4 and RIPEMD*. In: Cramer, Ronald (Herausgeber): *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 3494 der Reihe *Lecture Notes in Computer Science*, Seiten 1–18. Springer, 2005.

[164] Wang, Xiaoyun, Yiqun Lisa Yin und Hongbo Yu: *Finding Collisions in the Full SHA-1*. In: Shoup, Victor (Herausgeber): *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Proceedings*, Band 3621 der Reihe *Lecture Notes in Computer Science*, Seiten 17–36. Springer, 2005.

[165] Wang, Xiaoyun und Hongbo Yu: *How to Break MD5 and Other Hash Functions*. In: Cramer, Ronald (Herausgeber): *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniquees, Proceedings*, Band 3494 der Reihe *Lecture Notes in Computer Science*, Seiten 19–35. Springer, 2005.

[166] Wang, Xiaoyun, Hongbo Yu, Wei Wang, Haina Zhang und Tao Zhan: *Cryptanalysis on HMAC/NMAC-MD5 and MD5-MAC*. In: Joux, Antoine (Herausgeber): *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*, Band 5479 der Reihe *Lecture Notes in Computer Science*, Seiten 121–133. Springer, 2009.

[167] Wang, Xiaoyun, Hongbo Yu und Yiqun Lisa Yin: *Efficient Collision Search Attacks on SHA-0*. In: Shoup, Victor (Herausgeber): *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Proceedings*, Band 3621 der Reihe *Lecture Notes in Computer Science*, Seiten 1–16. Springer, 2005.

[168] Washington, Lawrence C.: *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and Its Applications. Chapman & Hall/CRC Press, 2003.

[169] Wayner, Peter: *British Document Outlines Early Encryption Discovery*. The New York Times, 24. Dezember 1997. `http://www.nytimes.com/library/cyber/week/122497encrypt.html`.

[170] Yao, Andrew Chi-Chih: *Theory and Applications of Trapdoor Functions (Extended Abstract)*. In: *23rd Annual Symposium on Foundations of Computer Science (FOCS 1982)*, Seiten 80–91. IEEE Computer Society, 1982.

[171] Zimmermann, Philip R.: *The Official PGP User's Guide*. MIT Press, 1995.

[172] *American National Standards Institute, ANSI X9.71: Keyed hash message authentication code*, 2000.

[173] *American National Standards Institute, ANSI X9.9: Financial Institution Message Authentication (Wholesale)*, 1981. Überarbeitet 1986.

[174] International Telecommunication Union (ITU). Telecommunication Standardization Sector of ITU: *ITU-T X.509*, November 2008. `http://www.itu.int/rec/T-REC-X.509/en`. Die erste Version diese Standards stammt aus dem Jahr 1988.

[175] *ISO/IEC 9797, Data cryptographic techniques — data integrity mechanism using a cryptographic check function employing a block cipher algorithm*, 1989.

[176] National Bureau of Standards: *Data encryption standard (DES)*, 1977. Federal Information Processing Standard (FIPS), publication 46.

[177] National Bureau of Standards: *DES modes of operation*, 1980. Federal Information Processing Standard (FIPS), publication 81.

[178] National Institute of Standards and Technology (NIST): *Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)*. Federal Register 62(117), 12. September 1997. `http://csrc.nist.gov/archive/aes/pre-round1/aes_9709.htm`.

[179] National Institute of Standards and Technology (NIST): *Secure Hash Standard*. Federal Register 72(212), 2. November 2007. `http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf`.

[180] National Institute of Standards and Technology (NIST): *Secure Hash Standard*, April 1995. Federal Information Processing Standard (FIPS), publication 180-1.

[181] National Institute of Standards and Technology (NIST): *Recommendation for Block Cipher Modes of Operation*, 2001. NIST Special Publication 800-38A. 2001 Edition. `http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf`.

[182] National Institute of Standards and Technology (NIST): *The keyed-hash message authentication code (HMAC)*, März 2002. Federal Information Processing Standard (FIPS), publication 198.

[183] National Institute of Standards and Technology (NIST): *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for AuthenticationSecure Hash Standard*, Mai 2005. NIST Special Publication 800-38B.

[184] National Institute of Standards and Technology (NIST): *Recommendation for key management part 1: General (revised)*, März 2007. NIST Special publication 800-57. `http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf`.

[185] National Institute of Standards and Technology (NIST): *Secure Hash Standard*, Oktober 2008. Federal Information Processing Standard (FIPS), publication 180-3.

[186] National Institute of Standards and Technology (NIST): *Digital Signature Standard (DSS)*, Juni 2009. Federal Information Processing Standard (FIPS), publication 186-3. Die erste Version dieses Standards stammt aus dem Jahr 1994.

[187] RSA — the security division of EMCRSA Laboratories: *The RSA challenge numbers.* Zunächst unter `http://www.rsa.com/rsalabs/node.asp?id=2093` nun unter `http://en.wikipedia.org/wiki/RSA_numbers` zu finden.

[188] RSA Laboratories: *PKCS#1: RSA Encryption Standard. Version 1.5*, November 1993. `http://www.rsa.com/rsalabs/node.asp?id=2125`.

[189] RSA Laboratories: *PKCS #10 v1.7: Certification Request Syntax Standard*, Mai 2000. `http://www.rsa.com/rsalabs/node.asp?id=2132`.

[190] RSA Laboratories: *PKCS#1 v2.1: RSA Cryptography Standard*, Juni 2002. `http://www.rsa.com/rsalabs/node.asp?id=2125`.

Stichwortverzeichnis

R. Küsters, T. Wilke, *Moderne Kryptographie*, DOI 10.1007/978-3-8348-8288-2,
© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011