Literaturverzeichnis

[AF90] M. Abadi und J. Feigenbaum, *Secure Circuit Evaluation.* J. Cryptology 2 (1990), 1-12.

[AFK89] M. Abadi, J. Feigenbaum und J. Kilian, *On Hiding Information from an Oracle.* JCSS 39 (1989), 21-50.

[Bab85] L. Babai, *Trading Group Theory for Randomness.* Proc. 17. STOC 1985, 421-429.

[BBE92] C. H. Bennet, G. Brassard und K. Ekert, *Quanten-Kryptographie.* Spektrum der Wissenschaft, Dezember 1992, 96-104.

[BAN89] M. Burrows, M. Abadi und R. M. Needham, *A Logic of Authentication.* Rep. 39. Digital Equipment Corporation Systems Research Center, Palo Alto, Calif., Feb. 1989.

[BAN90] M. Burrows, M. Abadi und R. M. Needham, *A Logic of Authentication.* ACM Transactions on Computer Systems, Vol. 8, Nr. 1 (1990), 18-36.

[Bau93] F. L. Bauer, *Kryptologie.* Springer Verlag, 2. Auflage, Heidelberg 1997.

[BB84] C. H. Bennet und G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing.* Proc. IEEE Conf. on Computers, Systems and Signal Processing, Banjalore, Indien (1984), 175-179.

[BB85] C. H. Bennet und G. Brassard, *An Update on Quantum Cryptography.* CRYPTO '84, Springer LNCS 196 (1985), 475-480.

[BDG88] J. L. Balcázar, J. Díaz und J. Gabarró, *Structural Complexity I.* Springer Verlag 1988.

[Beu96] A. Beutelspacher, *Kryptologie.* 5. Auflage, Verlag Vieweg, Wiesbaden 1994.

[BFL90] L. Babai, L. Fortnow und C. Lund, *Nondeterministic Exponential Time has Two-Prover Interactive Proofs.* Proc. 31. FOCS 1990, 16-25.

[BFM88] M. Blum, P. Feldman und S. Micali, *Non-Interactive Zero-Knowledge Proof Systems and Applications.* Proc 20. STOC 1988.

[BGGHKMR88] M. Ben-or, O. Goldreich, S. Goldwasser, J. Hastad, J. Kilian, S. Micali und P. Rogaway, *Everything Provable is Provable in Zero-Knowledge.* CRYPTO '88, Springer LNCS 403, 37-56.

[BGKW88] M. Ben-or, S. Goldwasser, J. Kilian, A. Wigderson, *Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions.* Proc. 20. STOC 1988, 113-122.

[Bie96] W. Bieser, *Sachstand der gesetzlichen Regelung zur digitalen Signatur.* In: Digitale Signaturen, P. Horster (Hrsg.), Vieweg Verlag, Wiesbaden 1996.

[Bih93] Eli Biham, *On Modes of Operation.* Proceedings of Fast Software Encryption 1, Cambridge Security Workshop, 1993, Springer LNCS 809.

[Blu86] M. Blum, *How to Prove a Theorem So No One Else Can Claim It.* Proceedings of the International Congress of Mathematicians, Berkeley, CA, 1986, 1444-1451.

[BM88] L. Babai und S. Moran, *Arthur-Melin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes.* JCSS 36 (1988), 254-276.

[BP82] H. Beker und F. Piper, *Cipher Systems. The Protection of Communication.* Northwood, London 1982.

[Bra88] G. Brassard, Modern Cryptology. Springer LNCS 325.

[BR92] A. Beutelspacher und U. Rosenbaum, *Projektive Geometrie.* Vieweg-Verlag 1992.

[BRK95] A. Bartholomé, J. Rung und H. Kern: *Zahlentheorie für Einsteiger.* Verlag Vieweg, Braunschweig und Wiesbaden 1995.

[BS93] A. Beutelspacher und J. Schwenk, *Was ist Zero-Knowledge?* Math. Semesterberichte 40 (1993), 73-85.

[BS96] A. Beutelspacher und J. Schwenk, *Was ist ein Beweis?* Überblicke Mathematik 1996, Vieweg Verlag, Wiesbaden 1996.

[CFN88] D. Chaum, A. Fiat und M. Naor, *Untraceable Electronic Cash.* Proc. CRYPTO '88, Springer LNCS 403, 319-327.

[CFPR96] D. Coppersmith, M. Franklin, J. Patarin and M. Reiter, *Low-Exponent RSA with Related Messages.* EUROCRYPT '96, Springer LNCS 1070, 1-9.

[CG399] Crypto-Gram March 15, 1999, http://www.counterpane.com/crypto-gram-9903.html.

[Cha81] D. Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* Comm. ACM 24 (1981), 84-88.

[Cha85] D. Chaum, *Security without Identification: Transaction Systems to Make Big Brother Obsolete.* Comm. ACM 28 (1985), 1030-1044.

[Cha88] D. Chaum, *The Dining Cryptographers Problem: Unconditional Sender and Receiver Untraceability.* J. Cryptology Vol 1 Nr. 1 (1988), 65-75.

[Cop85] D. Coppersmith, *Cheating at mental Poker.* Proc. CRYPTO 85, H. C. Williams (ed.), Springer LNCS 218, 104-107.

[Cop97] D. Coppersmith, *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities.* J. Cryptology Vol 10 Nr. 4 (1997), 233-260.

[CR88] B. Chor and R. Rivest, *A Knapsack-Type Public Key Cryptosystem Based on Arithmetic in Finite Fields.* IEEE Transactions on Information Theory, 45 (1988), 901-909.

[Cre86] C. Crepeau, *A zero-knowledge Poker protocol that achieves confidentiality of the players' strategy* or *How to achieve an electronic Poker face.* Proc. CRYPTO '86, A. M. Odlyzko (ed.), Springer LNCS 263, 239-247.

[Cre87] C. Crepeau, *Equivalence between two flavours of Oblivious Transfer.* Proc. CRYPTO '87, Springer LNCS 293, 350-354.

[Dif92] W. Diffie, *The first ten years of Public Key Cryptography.* In: Contemporary Cryptology: The Science of Information Integrity, G. J. Simmons, ed., IEEE Press 1992, 65-134.

[DH76] W. Diffie und M. E. Hellman, *New Directions in Cryptography.* IEEE Transactions on Information Theory, 6, November 1976, 644-654.

[Dob96] H. Dobbertin, *Welche Hash-Funktionen sind für digitale Signaturen geeignet?* In: Digitale Signaturen, P. Horster (Hrsg.), Vieweg Verlag, Wiesbaden 1996.

[EFF99] Cracking DES. Electronic Frontier Foundation. http://www.eff.org/descracker/.

[EGL85] S. Even, O. Goldreich, A. Lempel, *A randomized protocol for signing contracts.* Comm. ACM 28 (1985), 6, 637-647.

[ElG85] T. ElGamal, *A Public Key Cryptosystem and a Signature Scheme based on Diskrete Logarithms.* IEEE Trans. on Information Theory, Vol. IT-31 (1985), 469-472.

[EP91] European Patent Application 0 428 252 A2, *A System for Controlling Access to Broadcast Transmissions.* (1991)

[Fei92] J. Feigenbaum, *Overview of Interactive Proof Systems and Zero-Knowledge.* In: Contemporary Cryptology: The Science of Information Integrity, G. J. Simmons, ed., IEEE Press 1992, 423-439.

[FeS90] U. Feige und A. Shamir, *Zero Knowledge Proofs of Knowledge in Two Rounds.* CRYPTO '89, Springer LNCS 435, 526-544.

[FIPS91] FIPS PUB 186, *Digital Signature Standard.* Federal Information Processing Standard, National Institute of Standards and Technology, US Department of Commerce, Washington D. C. (1994).

[FR94] W. Fumy und H. P. Ries, *Kryptographie.* Oldenbourg Verlag, 2. Auflage, München 1994.

[FS87] A. Fiat und A. Shamir, *How to Prove Yourself: Practical Solutions to Identification and Signature Problems.* CRYPTO '86, Springer LNCS 263, 186-194.

[GS91] J. W. Goebel und J. Scheller, *Elektronische Unterschriftsverfahren in der Telekommunikation.* Verlag Vieweg, Brauschweig und Wiesbaden 1991.

[GMR85] S. Goldwasser, S. Micali und C. Rackoff, *The Knowledge Complexity of Interactive Proof Systems.* Proc. 17. STOC 1985, 291-304.

[GMR89] S. Goldwasser, S. Micali und C. Rackoff, *The Knowledge Complexity of Interactive Proof Systems.* SIAM J. Comput. 8(1) (1989), 186-208.

[GMW86] O. Goldreich, S. Micali und A. Wigderson, Proofs that Yield Nothing but their Validity and a Methodology of Cryptographic Protocol Design. Proc. 27. FOCS 1986, 171-185.

[GO94] O. Goldreich und Y. Oren, *Definitions and Properties of Zero-Knowledge Proof Systems.* J. Cryptology, Vol. 7 Nr. 1 (1994), 1-32.

[HMP95] P. Horster, V. Michels und H. Petersen, *Das Meta-ElGamal Signaturverfahren und seine Anwendungen.* Proc. VIS'95, Vieweg Verlag, Wiesbaden 1995, 207-228.

[Hor85] P. Horster, *Kryptologie.* BI-Verlag, Mannheim 1985.

[IY87] R. Impagliazzo und M. Yung, *Direct Minimum-Knowledge Computations.* CRYPTO '87, Springer LNCS 293 (1988), 40-51.

[Jun90] D. Jungnickel, *Graphen, Netzwerke und Algorithmen.* BI Wissenschaftsverlag, 2. Auflage 1990.

[Ker92] A. G. Kersten, *Shared Secret Schemes aus Geometrischer Sicht.* Mitt. aus dem Math. Sem. Giessen, Heft 208 (1992).

[KH92] H.-J. Knobloch und P. Horster, *Eine Krypto-Toolbox für Smartcard-Chips mit speziellen Calculation Units.* Proc. 2. GMD-SmartCard Workshop, Darmstadt (1992).

[Kil88] J. Kilian, *Founding Cryptography on Oblivious Transfer.* Proc. 20. STOC 1988, 20-31.

[KMM94] R. Kemmerer, C. Meadows und J. Millen, *Three Systems for Cryptographic Protocol Analysis.* J. Cryptology Vol. 7 Nr. 2 (1994), 79-130.

[Knu69] D. E. Knuth, *The Art of Computer Programming. Volume 2/Seminumerical Algorithms.* Addison-Wesley, Reading, Mass., 1969.

[KR95] B. Kaliski and M. Robshaw, *The Secure Use of RSA.* CryptoBytes Vol. 1 No.3, RSA Laboratories, Autumn 1995.

[Kra86] E. Kranakis, *Primality and Cryptography.* Teubner Verlag, Stuttgart 1986.

[LS90] D. Lapidot und A. Shamir, *Publicly Verifiable Non-Interactive Zero-Knowledge Proofs.* CRYPTO '90, Springer LNCS 537, 339-356.

[Mas90] J. L. Massey, *Folien des Seminars „Cryptography: Fundamentals and Applications".* Advanced Technology Seminars (1990).

[Mau94] U. Maurer, *Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Diskrete Logarithms.* CRYPTO '94, Springer LNCS 839, 271-281.

[McE78] R. McEliece, *A Public-Key Cryptosystem based on Algebraic Coding Theory.* DSN Progress Report, 42-44 (1978), 114-116.

[MH78] R. C. Merkle und M. E. Hellman, *Hiding Information and Signatures in Trapdoor Knapsacks.* IEEE Transactions on Information Theory, 24 (1978), 525-530.

[Mey76] Kurt Meyberg, *Algebra Teil 2.* Carl Hanser Verlag München, April 1976

[Moo92] J. H. Moore, *Protocol Failures in Cryptosystems.* In: Contemporary Cryptology, Hrsg. G. J. Simmons, IEEE Press 1992.

[MOV97] A. J. Menezes, P. C. van Oorschot und S. A. Vanstone, *Handbook of Applied Cryptography.* CRC Press, New York 1997.

[NIST00] National Institute of Standards and Technology, *Advanced Encryption Standard.* www.nist.gov/aes.

[NR96] K. Nyberg und R. Rueppel, *Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem.* Designs, Codes and Cryptography, 7, 61-81 (1996).

[NS78] R. M. Needham und M. D. Schroeder, *Using Encryption for Authentication in Large Networks of Computers.* Comm. ACM Vol. 21 Nr. 12 (1978), 993-999.

[OR87] D. Otway und O. Ries, *Efficient and Timely Mutual Authentication.* Operating Systems Review Vol. 21 Nr. 1 (1987), 8-10.

[PEM97] Network Working Group, RfC 1421, http://ftp.gwdg.de/pub/rfc/rfc1421.txt.

[PGP] Pretty Good Privacy International, http://www.pgpi.com.

[PGV93] B. Preneel, R. Govaerts und J. Vandewalle, *Information Authentication: Hash Functions and Digital Signatures.* In: Computer Security and Industrial Cryptography, Hrsg. B. Preneel, R. Govaerts und J. Vandewalle, Springer LNCS 741 (1993), 87-131.

[Pre93] B. Preneel, *Standardization of Cryptographic Techniques.* In: Computer Security and Industrial Cryptography, Hrsg. B. Preneel, R. Govaerts und J. Vandewalle, Springer LNCS 741 (1993), 162-173.

[PSW95] B. Pfitzmann, M. Schunter und M Waidner, *How to Break Another „Provably Secure" Payment System.* EUROCRYPT '95, Springer LNCS 921, 121-132.

[QG90] J.-J., M., M., M., Quisquater und L., M., G., A., G., S. Guillou, *How to explain Zero-Knowledge to your Children.* CRYPTO '89, Springer LNCS 435, 628-631.

[RSA78] R. Rivest, A. Shamir und L. Adleman, *A Method for Obtaining Digital Signatures and Public Key Cryptosystems.* Comm. ACM, Vol. 21, Nr. 2 (1978), 120-126.

[Rue86] R. Rueppel, *Analysis and Design of Stream Ciphers.* Springer Verlag Berlin 1986.

[Sal90] A. Salomaa, *Public-Key Cryptography.* Springer Verlag Berlin Heidelberg 1990.

[Sch96] J. Schwenk, *Conditional Access.* In: taschenbuch der telekom praxis 1996, Hrsg. B. Seiler, Verlag Schiele & Schön, Berlin.

[Schn90] C. P. Schnorr, *Efficient Identification and Signature Schemes for Smart Cards.* CRYPTO '89, Springer LNCS 435 (1990), 239-251.

[Schn96] B. Schneier, *Angewandte Kryptographie.* Addison-Wesley, Bonn 1996.

[SET97] VISA New Technologies, http://www.visa.com/nt/ecomm/set/

[Sha49] C. E. Shannon, *Communication theory of secrecy systems.* Bell. Sys. Tech. J. 30 (1949), 657-715.

[Sha79] A. Shamir, *How to Share a Secret.* Comm. ACM, Vol. 24, Nr. 11 (1979), 612-613.

[Sha90] A. Shamir, *IP = PSPACE.* Proc. 31. FOCS 1990, 11-15.

[SigG] http://www.datenschutz-und-datensicherheit.de/dudserver/signatur.htm

[SigG97] Gesetz zur digitalen Signatur (Signaturgesetz - SigG). Bundesgesetzblatt I S. 1870, 1872 (oder http://www.regtp.de/tech_reg_tele/start/in_06-02-01-00-00_m/index.html)

[SigG01] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften. www.dud.de/dud/documents/sigg010214.pdf

[SigV97] Verordnung zur digitalen Signatur (Signaturverordnung - SigV) www.regtp.de/tech_reg_tele/start/in_06-02-01-00-00_m/index.html

[Sim92] G. J. Simmons (Hrsg.), Contemporary Cryptology. IEEE Press 1992.

[Sim94] G. J. Simmons, *Cryptanalysis and Protocol Failures.* Comm. ACM Vol. 37 Nr. 11 (1994), 56-65.

[Sim94a] G. J. Simmons, *Proofs of Soundness (Integrity) of Cryptographic Protocols.* J. Cryptology Vol. 7 Nr. 2 (1994), 69-77.

[SMIME] IETF S/MIME Mail Security (smime) working group, *RFC 2311, 2312, 2630, 2632.* http://www.ietf.org/html.charters/smime-charter.html

[SRA79] A. Shamir, R. L. Rivest, L. M. Adleman, *Mental Poker.* Technical report MIT/LCS/TM-125, 1979.

[Ste92] A. Steinacker, *Anonyme Kommunikation in Netzen.* B.I.-Wissenschaftsverlag, Mannheim 1993.

[Sti95] D. R. Stinson, Cryptography. CRC Press Boca Raton, London, Tokyo 1995.

[IMC] Internet Mail Consortium, http://www.imc.org.

[TLS] IETF Transport Layer Security (tls) working group, *The TLS Protocol Version 1.0 (RFC2246).* http://www.ietf.org/html.charters/tls-charter.html

[TMN90] M. Tatebayashi, N. Matsuzaki und D. B. Newman, *Key Distribution Protocol for Digital Mobile Communication Systems.* CRYPTO '89, Springer LNCS 435, 324-333.

[WA75] H. Wußing und W. Arnold, *Biographien bedeutender Mathematiker.* Aulis Verlag Deubner & Co., Köln 1975.

Verwendete Abkürzungen:

FOCS: IEEE Symposium on the Foundations of Computer Science
JCSS: Journal of Computer and System Sciences
LNCS: Lecture Notes in Computer Science
STOC: ACM Symposium on the Theory of Computing

Für einige Verweise gab es zum Zeitpunkt der Drucklegung (noch) keine gedruckten Referenzen. Wir haben uns aber bemüht, nur solche Internet-Adressen zu zitieren, die auch längerfristig verfügbar sind.

Stichwortverzeichnis