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.

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

[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, Heidelberg 1993.

[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.

[Beu94] A. Beutelspacher, *Kryptologie.* 4. Auflage, Verlag Vieweg, Braunschweig und 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.

[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.

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

[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.

[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.

[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 xxx, *Digital Signature Standard.* Federal Information Processing Standard, Draft, National Institute of Standards and Technology, US Department of Commerce, Washington D. C. (1991).

[FR94] W. Fumy und H. P. Ries, *Kryptographie.* Oldenbourg Verlag München ^{2}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.

[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.

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

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

[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.

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

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

[Kra86] Kranakis, *Primality and Cryptography.* Wiley-Teubner 1986.

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

[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.

[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., 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. Rueppl, *Analysis and Design of Stream Ciphers.* Springer Verlag Berlin 1986.

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

[Schn94] B. Schneier, *Applied Cryptography.* Wiley New York 1994.

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

[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.

[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.

[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.

[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

Stichwortverzeichnis

Kryptologie

von Albrecht Beutelspacher

4., verb. Aufl. 1994. VIII, 179 Seiten. Kartoniert.
ISBN 3-528-38990-7

Aus dem Inhalt: YHUVWHKHQ VLH GDV? – Wenn nicht, sollten Sie dieses Buch lesen. Es bietet eine reich illustrierte, leichtverdauliche und amüsante Einführung in die Kryptologie. Diese Wissenschaft beschäftigt sich damit, Nachrichten vor unbefugtem Lesen und unberechtigter Änderung zu schützen. Ein besonderer Akzent liegt auf der Behandlung moderner Entwicklungen. Dazu gehören insbesondere Zugangskontrolle zu Rechnern, elektronische Unterschrift und Bezahlen mit Chipkarte.

„Selbst ein Hinweis auf den idealen Ort für die Lektüre fehlt nicht: In der Badewanne soll sie besonders geeignet sein."

Frank Braatz in à la card aktuell, März 1993

Verlag Vieweg · Postfach 15 46 · 65005 Wiesbaden

Codierungstheorie

von Ralph-Hardo Schulz

1991. VIII, 227 Seiten. Kartoniert.
ISBN 3-528-06419-6

Diese Einführung in die Codierungstheorie ist aus Vorlesungen für Mathematik- und Informatik-Studenten entstanden. Angesprochen werden Themen aus den Gebieten: Quellencodierung, Prüfzeichenverfahren, fehlerkorrigierende Codes und Kryptosysteme. Begriffe, Methoden und Sätze sind bis ins Detail ausführlich dargestellt und durch viele einfache Beispiele erläutert.

Über den Autor: Dr. rer. nat. Ralph-Hardo Schulz ist Professor im Fachbereich Mathematik der Freien Universität Berlin.

Verlag Vieweg · Postfach 15 46 · 65005 Wiesbaden