Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr

Seminar

Neue Anwendungen kryptographischer Algorithmen

WS 1996/97

Prof. Dr. E.W. Mayr und Prof. Dr. A. Steger, unter Mitarbeit von
Stefan Bischof, Thomas Erlebach, Thomas Friedetzky, Volker Heun,
Ulla Koppenhagen, Klaus Kühnle, Hans Stadtherr

Themenliste

1. Grundlagen zu Einweg-Funktionen

[1] J. Grollmann, A.L. Selman: Complexity Measures for Public-Key Cryptosystems. Proc. 25th IEEE Symposium on Foundations of Computer Science (FOCS), 1984, pp. 495–503.

[2] J. Grollmann, A.L. Selman: Complexity Measures for Public-Key Cryptosystems. SIAM J. Comp. 17(2):309–335, 1988.

2. Kandidaten für Einweg-Funktionen

[3] A.C. Yao: Theory and Application of Trapdoor Functions. Proc. 23rd IEEE Symposium on Foundations of Computer Science (FOCS), 1982, pp. 80–91.

[4] S. Goldwasser, S. Micali: Probabilistic Encryption. J. CSS 28, pp. 270–299, 1984. [nur Kapitel 6, pp. 291–297]

[5] J. Grollmann, A.L. Selman: Complexity Measures for Public-Key Cryptosystems. SIAM J. Comp. 17(2):309–335, 1988. [nur Kapitel 4.3, pp. 329–330]

3. Einweg-Hashfunktionen

[6] M. Naor, M. Yung: Universal One-Way Hash Functions and their Cryptographic Application. Proc. 21st Annual ACM Symposium on Theory of Computing (STOC), 1989, pp. 33–43.

[7] R. Impagliazzo, M. Naor: Efficient Cryptographic Schemes Provably as Secure as Subset Sum. Proc. 30th IEEE Symposium on Foundations of Computer Science (FOCS), 1989, pp. 236–241.

4. Primzahl-Tests

[8] R. Solovay, V. Strassen: A fast Monte-Carlo test for primality. SIAM J. Comp. 6, pp. 84-86, 1977.

[9] R. Solovay, V. Strassen: Erratum: A fast Monte-Carlo test for primality. SIAM J. Comp. 7, p. 118, 1978.

[10] M.O. Rabin: Probabilistic algorithm for testing primality. J. Number Theory 12, pp. 128-138, 1980.

[11] G.L. Miller: Riemann's hypothesis and tests for primality. J. CSS 13, pp. 300–317, 1976.

5. Digitale Signaturen: DSS und DSA

[12] B. Schneier: Applied Cryptography (Second Edition). Chapter 20: Public-Key Digital Signature Algorithms. John Wiley & Sons, 1996, pp. 483–502.

[13] NIST: The Digital Signature Standard. Comm. of the ACM, July 1992, Vol. 35, No. 7, pp. 36–40.

[14] R.L. Rivest, M.E. Hellman, J.C. Anderson: Responses to NIST's Proposal. Comm. of the ACM, July 1992, Vol. 35, No. 7, pp. 41–54.

6. Aufteilung geheimer Information

[15] G.J. Simmons: Contemporary Cryptology. Chapter 9: An Introduction to Shared Secret and/or Shared Control Schemes and Their Application. IEEE Press, 1992, pp. 441–497.

7. Sicherheit von Kryptosystemen und nachweisbar faire Poker-Spiele

[16] S. Goldwasser, S. Micali: Probabilistic Encryption and How To Play Mental Poker Keeping Secret All Partial Information. Proc. 14th Annual ACM Symposium on Theory of Computing (STOC), 1982, pp. 365–377.

[17] S. Goldwasser, S. Micali: Probabilistic Encryption J. CSS 28, pp. 270–299, 1984.

8. Interaktives Beweisen ohne Preisgabe zusätzlicher Informationen

[18] S. Goldwasser, S. Micali, C. Rackoff: The Knowledge Complexity of Interactive Proof-Systems. Proc. 17th Annual ACM Symposium on Theory of Computing (STOC), 1985, pp. 291–304.

[19] S. Goldwasser, S. Micali, C. Rackoff: The Knowledge Complexity of Interactive Proof Systems. SIAM J. Comp. 18(1):186–208, 1989.

[20] O. Goldreich, S. Micali, A. Wigderson: Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design. Proc. 27th IEEE Symposium on Foundations of Computer Science (FOCS), 1986, pp. 174–187.

[21] O. Goldreich, S. Micali, A. Wigderson: Proofs that Yield Nothing But their Validity or ALll Languages in NP Have Zero-Knowledge Proof Systems. J. ACM 38(1):691–729, 1991.

9. Der Fiat-Shamir-Zero-Knowledge-Test und seine Anwendung in Smartcards

[22] A. Fiat, A. Shamir: How To Prove Yourself: Practical Solutions to Identification and Signature Problems. Advances in Cryptology – CRYPTO '86, pp. 186–194.

[23] U. Feige, A. Fiat, A. Shamir: Zero Knowledge Proofs of Identity. Proc. 19th nnual ACM Symposium on Theory of Computing (STOC), 1987, pp. 210–217

[24] U. Feige, A. Fiat, A. Shamir: Zero Knowledge Proofs of Identity. Journal of Cryptology 1:77–94, 1988.

[25] A. Shamir: Memory Efficient Variants of Public-Key Schemes for Smart Card Applications. Advances in Cryptology – EUROCRYPT '94, pp. 445–449.

10. Digitales Bargeld

[26] T. Okamoto, K. Ohta: Universal Electronic Cash. Advances in Cryptology – CRYPTO '91, pp. 324–337.

11. Broadcast-Verschlüsselung

[27] A. Fiat, M. Naor: Broadcast Encryption. Advances in Cryptology – CRYPTO '93, pp. 480–491.

12. Elektronische Wahlen

[28] K. Sako, J. Kilian: Secure Voting using partially compatible homomorphisms. Advances in Cryptology – CRYPTO '94, pp. 411–424.

13. Inkrementelle Kryptographie

[29] M. Bellare, O. Goldreich, S. Goldwasser: Incremental cryptography: the case of hashing and signing. Advances in Cryptology – CRYPTO '94, pp. 217–233.