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

Seminar
Kryptographische Verfahren
Sommersemester 2001
9. Januar 2001

Seminar

Kryptographische Verfahren

Sommersemester 2001
Prof. Dr. Ernst W. Mayr,
Prof. Dr. Angelika Steger

Themenliste

1. Grundlegende kryptographische Algorithmen: Diffie-Hellmann und ElGamal

   [1] Beutelspacher, S. 28-32; Buchmann, S. 127-135 (Stinson, 162-177)

2. Grundlegende kryptographische Algorithmen: RSA

   [2] Beutelspacher, S. 18-22; Buchmann, S. 112-123

3. Digitale Signaturen

   [3] Buchmann, S. 175-188; Stinson S. 202-213

4. Authentifizierung mit Zero-Knowledge-Verfahren

   [4] Beutelspacher, S. 39-67; Stinson S. 385-398, Goldwasser-Skript

5. Ein-Weg-Hashfunktionen

   [5] Buchmann, S. 165-174; Stinson S. 232-254

6. Verfahren zur Schlüsselverwaltung

   [6] Beutelspacher, S. 92-104; Stinson S. 258-279, Goldwasser-Skript

7. Teilen von Information

   [7] Beutelspacher, S. 68-71; Stinson S. 326-358

8. Sichere Broadcasts

    [8] A. Fiat, M. Naor. Broadcast encryption. CRYPTO93, S. 480–491, 1993.

9. Schließen von Verträgen

    [9] Beutelspacher, S. 14-15, 104-112; Schneier, S. 86-95, 116-124

10. Digitales Bargeld

    [10] Beutelspacher, S. 86-88, T. Okamoto, K. Ohta. Universal Electronic Cash, CRYPTO91, S. 324–337, 1991. Goldwasser-Skript

11. Elektronische Wahlen

    [11] Beutelspacher, S. 88-91; Schneier, S. 125-134; K. Sako, J. Kilian. Secure voting using partially compatible homomorphisms. CRYPTO94, S. 411-424, 1994. Goldwasser-Skript

12. Primzahltests

    [12] Buchmann, S. 103-110; Stinson, S. 129-138

13. Faktorisierung

    [13] Buchmann, S. 137-147; Stinson, S. 150-156

14. Berechnung des diskreten Logarithmus

    [14] Buchmann, S. 149-164; Stinson, S. 164-177