Seminar über Computeralgebra (Kryptologie) WS 2001/2002

VORTRAG 1: DAS RSA-VERFAHREN *(Stephan Kreitz)* — 7. Nov. 2001
Beschreibung des Verfahrens, elektronische Unterschriften, elektronisches Bargeld, wichtige Vorsichtsmaßnahmen, z.B. nach **[Bu]**, §7.2

VORTRAG 2: PRIMZAHLERKENNUNG *(Christine Dollinger)* — 21. Nov. 2001
Sieb des ERATOSTHENES, FERMAT-Test, Überblick über Primzahlverteilung, Komplexität der Primzahlerkennung: **[CP]**, §3.1–3; **[Ri]**, Chap. 4 Anfang; **[F]**, §11)

VORTRAG 3: LANGZAHLARITHMETIK *(Heinz Kredel)* — 28. Nov. 2001
Grundrechenarten, MONTGOMERY-Trick
Hauptreferenz ist **[CP]**, §9, 1–3, alternativ auch **[MOV]**, §14.1–3. Eine ausführlichere Darstellung der Theorie ist in **[Kn]** zu finden. Für Implementierungsfragen kann man bei entsprechendem Interesse **[W]** oder **[TS]** konsultieren.

VORTRAG 4: FAKTORISIERUNG *(Wolfgang K. Seiler)* — 5. Dez. 2001
FERMAT-Verfahren, quadratisches Sieb, Ausblick: Zahlkörpersieb
[CP], §5.1.1, §6.1, Überblick über §6.2

VORTRAG 5: VORSICHTSMASSNAHMEN BEI RSA *(Andreas Bergauer)* — 12. Dez. 2001
DAN BONEH: Twenty Years of Attacks on the RSA Cryptosystem, *Notices of the AMS*, Feb. 1999, *oder* http://www.ams.org/notices/199902/boneh.pdf

VORTRAG 6: DISKRETE LOGARITHMEN *(Dirk Schmerenbeck)* — 19. Dez. 2001
Anwendung in Kryptoverfahren,Berechnung nach Baby Step-Giant Step Methode, Berechnung mit Indexmethode (**[Bu]**, Kap. 9, vor allem Abschnitte 1, 3 und 6)

VORTRAG 7: ELLIPTISCHE KURVEN FÜR DIE PRIMZAHLERKENNUNG UND FÜR DIE FAKTORISIERUNG GANZER ZAHLEN *(Martin Schlichenmaier)* — 9. Jan. 2002
[CP], §7.1+2+4+6, **[Ko]**, VI.1+3

VORTRAG 8: STRUKTUR DER GRUPPE EINER ELLIPTISCHEN KURVE UND DARAUF AUFBAUENDE KRYPTOVERFAHREN *(Cristian Serban)* — 16. Jan. 2002
[Ko], VI.2, **[CP]**, §7.5, Hintergrundmaterial in **[M]**, **[BSS]**, **[Ro]**

VORTRAG 9: RECHNEN AUF ELLIPTISCHEN KURVEN *(N.N.)* — 23. Jan. 2002
D.V. CHUDNOVSKY, G.V. CHUDNOVSKY: Sequences of numbers generated by addition in formal groups and new primality and factorization tests, *Adv. Appl. Math.* **7** (1986), 385-434

VORTRAG 10: QUADRATISCHE RESTE UND IHRE ANWENDUNGEN AUF KRYPTOGRAPHISCHE PROTOKOLLE *(N.N.)* — 30. Jan. 2002
[Ko], IV.5. Zumindest erwähnt werden sollte auch SHAMIRs Satz, wonach es für jedes mathematische Verfahren, dessen Speicherbedarf höchstens polynomial mit der Länge der Eingabedaten steigt, ein interaktives Beweisverfahren gibt; siehe dazu Abschnitt 8 von S. GOLDWASSER: Interactive proofs and applications, *Proc. Int. Congr. Math., Kyoto 1990, Vol. II,* 1521-1535 .

Literatur

[BSS] IAN F. BLAKE, GADIEL SEROUSSI, NIGEL PAUL SMART: Elliptic curves in cryptography, *Cambridge University Press,* 2000

[Bu] JOHANNES BUCHMANN: Einführung in die Kryptographie, *Springer,* 1999

[CP] RICHARD CRANDALL, CARL POMERANCE: Prime numbers: a computational perspective, *Springer,* 2001

[F] OTTO FORSTER: Algorithmische Zahlentheorie, *Vieweg,* 1996

[Kn] DONALD KNUTH: The art of computer programming II: Seminumerical algorithms, *Addison Wesley*

[Ko] NEAL KOBLITZ: A Course in Number Theory and Cryptography, *Springer,* ^{2}1994

[M] ALFRED J. MENEZES: Elliptic curve public key cryptosystems, *Kluwer,* 1993

[MOV] ALFRED J. MENEZES, PAUL C. VAN OORSCHOT, SCOTT A. VANSTONE: Handbook of applied cryptography, *CRC Press,* 1997

[Ri] HANS RIESEL: Prime numbers and computer methods for factorization, *Birkhäuser,* ^{2}1985

[Ro] MICHAEL ROSING: Implementing Elliptic Curve Cryptography, *Manning,* 1998

[TS] TAN KIAT SHI, WILLI-HANS STEEB: SymbolicC++: An introduction to computer algebra using object-oriented programming, *Springer,* 1998

[W] MICHAEL WELSCHENBACH: Kryptographie in C und C++, *Springer,* 1998