Proceedings of Symposia in Applied Mathematics

Volume 42

Cryptology and Computational Number Theory

American Mathematical Society Short Course
August 6–7, 1989
Boulder, Colorado

Carl Pomerance, Editor

Shafi Goldwasser
J. C. Lagarias
Arjen K. Lenstra
Kevin S. McCurley
A. M. Odlyzko

American Mathematical Society
Other Titles in This Series

50 Robert Calderbank, editor, Different aspects of coding theory (San Francisco, California, January 1995)
49 Robert L. Devaney, editor, Complex dynamical systems: The mathematics behind the Mandelbrot and Julia sets (Cincinnati, Ohio, January 1994)
47 Ingrid Daubechies, editor, Different perspectives on wavelets (San Antonio, Texas, January 1993)
46 Stefan A. Burr, editor, The unreasonable effectiveness of number theory (Orono, Maine, August 1991)
45 De Witt L. Sumners, editor, New scientific applications of geometry and topology (Baltimore, Maryland, January 1992)
44 Béla Bollobás, editor, Probabilistic combinatorics and its applications (San Francisco, California, January 1991)
43 Richard K. Guy, editor, Combinatorial games (Columbus, Ohio, August 1990)
42 C. Pomerance, editor, Cryptology and computational number theory (Boulder, Colorado, August 1989)
41 R. W. Brockett, editor, Robotics (Louisville, Kentucky, January 1990)
40 Charles R. Johnson, editor, Matrix theory and applications (Phoenix, Arizona, January 1989)
39 Robert L. Devaney and Linda Keen, editors, Chaos and fractals: The mathematics behind the computer graphics (Providence, Rhode Island, August 1988)
38 Juris Hartmanis, editor, Computational complexity theory (Atlanta, Georgia, January 1988)
37 Henry J. Landau, editor, Moments in mathematics (San Antonio, Texas, January 1987)
36 Carl de Boor, editor, Approximation theory (New Orleans, Louisiana, January 1986)
35 Harry H. Panjer, editor, Actuarial mathematics (Laramie, Wyoming, August 1985)
34 Michael Anshel and William Gewirtz, editors, Mathematics of information processing (Louisville, Kentucky, January 1984)
33 H. Peyton Young, editor, Fair allocation (Anaheim, California, January 1985)
32 R. W. McKelvey, editor, Environmental and natural resource mathematics (Eugene, Oregon, August 1984)
31 B. Gopinath, editor, Computer communications (Denver, Colorado, January 1983)
28 R. Gnanadesikan, editor, Statistical data analysis (Toronto, Ontario, August 1982)
27 L. A. Shepp, editor, Computed tomography (Cincinnati, Ohio, January 1982)
25 S. I. Gass, editor, Operations research: mathematics and models (Duluth, Minnesota, August 1979)
24 W. F. Lucas, editor, Game theory and its applications (Biloxi, Mississippi, January 1979)
23 R. V. Hogg, editor, Modern statistics: Methods and applications (San Antonio, Texas, January 1980)
22 G. H. Golub and J. Oliger, editors, Numerical analysis (Atlanta, Georgia, January 1978)
21 P. D. Lax, editor, Mathematical aspects of production and distribution of energy (San Antonio, Texas, January 1976)

(Continued in the back of this publication)
Cryptology
and Computational
Number Theory
AMS SHORT COURSE LECTURE NOTES
Introductory Survey Lectures
published as a subseries of
Proceedings of Symposia in Applied Mathematics
Proceedings of Symposia in
APPLIED MATHEMATICS

Volume 42

Cryptology
and Computational
Number Theory

American Mathematical Society
Short Course
August 6–7, 1989
Boulder, Colorado

Carl Pomerance, Editor
Shafi Goldwasser
J. C. Lagarias
Arjen K. Lenstra
Kevin S. McCurley
A. M. Odlyzko

American Mathematical Society
Providence, Rhode Island
Table of Contents

Preface xi

Cryptology and Computational Number Theory—An Introduction
CARL POMERANCE 1

Primality Testing
ARJEN K. LENSTRA 13

Factoring
CARL POMERANCE 27

The Discrete Logarithm Problem
KEVIN S. McCURLEY 49

The Rise and Fall of Knapsack Cryptosystems
A. M. ODLYZKO 75

The Search for Provably Secure Cryptosystems
SHAFI GOLDWASSER 89

Pseudorandom Number Generators in Cryptography and Number
Theory
J. C. LAGARIAS 115

Odds and Ends from Cryptology and Computational Number Theory
KEVIN S. McCURLEY 145

Index 167
Preface

Although they are both ancient and noble subjects, it is only a phenomenon of the past dozen years or so that cryptology and computational number theory have become so intertwined. It is possible that in another dozen years they will part and again go their separate ways, since the primary cryptologic application of number theory is the apparent intractibility of certain computations. But for now they are together, and the union has brought ferment and rapid change to both subjects.

In August 1989 at the summer AMS meeting in Boulder, Colorado, nearly 200 people attended a short course on cryptology and computational number theory. Six articles in this book are based on the six presentations given at the short course. I am very happy to include an additional article, Kevin McCurley’s “Odds and ends...” paper, which includes many other interesting interconnections between cryptology and computational number theory.

I wish to take this opportunity to thank Monica Foulkes and Jim Maxwell for helping insure the success of the short course and Carrie Tucker for her help in the production of this book. Thanks also go to Bob Kurshan for talking me into organizing the short course in the first place. Finally, on behalf of my fellow speakers I wish to thank the short course participants whose enthusiasm made it all worthwhile.

Carl Pomerance
Index

abelian variety test, 14, 22
Adleman, L., 6, 11, 12, 22, 24, 60, 71, 79, 87, 99, 112, 113, 120, 142, 146, 152, 155, 163, 164, 166
Aho, A. V., 71
Alexi, W. B., 102, 112, 132, 134, 135, 139, 157, 164
Alford, W. R., 44, 46
Allender, E., 139
Altman, N. S., 139
Angluin, D., 112
Atkin, A.O.L., 23
Babai, L., 139
Bach, E., 24, 46, 72, 139, 146, 164
Ben-David, S., 139
Ben-Or, M., 112, 113, 132, 133, 139
Berger, R., 112
Berlekamp, E., 112, 148, 164
Berlekamp-Massey algorithm, 148
Beth, T., 72, 112
Beyer, W. R., 139
Blahut, R. E., 164
Blake, I. F., 68, 69
Blum, L., 112, 119, 120, 136, 139, 164
Blum, M., 55, 72, 92, 103, 104, 105, 112, 118, 119, 120, 126, 132, 135, 136, 139, 164
Boolelan circuit, 125
Boppana, R., 126, 128, 139
Bos, J., 164
Bosma, W., 24
Boyar, J., 137, 140, 164
Brassard, G., 72, 87, 112, 115, 140
Brent, R. P., 133, 140
Brickell, E. F., 11, 72, 80, 87, 164
Brillhart, J., 24, 46, 72, 153, 164
Brudno, A. A., 117, 140
Buchmann, J., 72, 163, 164
Buhler, J., 29, 66
Canfield, E. R., 72
Carmichael numbers, 5, 14
Caron, T. R., 44
cellular automata, 121
cellular automata generators, 139
certificate of primality, 14, 22
chain of primes, 16, 22
Chaitin, G. J., 117, 140
Chaum, D., 72, 164
Chor, B., 87, 102, 112, 132, 133, 134, 135, 139, 140, 157, 164
Chor-Rivest cryptosystem, 86
chosen plaintext attack, 129
Chudnovsky, D. V., 24
Chudnovsky, G. V., 24
ciphertext, 129
Cohen, H., 24
coin flipping, 104
Collet, P., 117, 140
combination of congruences, 27, 43
complex multiplication field, 23
complex multiplication test, 14, 23
composition, 122
combutational complexity, 52
computational incompressibility, 117
computational information theory, 118
computationally randomness-increasing, 124
computationally zero-knowledge, 110
continued fraction method, 43
continued fractions, 82, 136
Coppersmith, D., 56, 64, 68, 69, 71, 72, 164
Coster, M., 164
Cot, N., 112
Coveyou, R., 140
Cunningham, Lt.Col. A.J.C., 60
Cunningham project, 45
Damgård, I. B., 162, 164
data compression, 122
data encryption standard, 8, 51, 79, 130
<table>
<thead>
<tr>
<th>Term</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Davenport, J. H.</td>
<td>69, 72, 164</td>
</tr>
<tr>
<td>Davis, J. A.</td>
<td>43, 46, 163</td>
</tr>
<tr>
<td>de Jonge, W.</td>
<td>164</td>
</tr>
<tr>
<td>DeMillo, R. A.</td>
<td>72</td>
</tr>
<tr>
<td>den Boer, B.</td>
<td>72</td>
</tr>
<tr>
<td>Desmedt, Y. G.</td>
<td>81, 87</td>
</tr>
<tr>
<td>deterministic polynomial-time primality test</td>
<td>15</td>
</tr>
<tr>
<td>Deuring, M.</td>
<td>40, 46</td>
</tr>
<tr>
<td>Devroye, L.</td>
<td>115, 140</td>
</tr>
<tr>
<td>Dickman-de Bruijn function</td>
<td>34</td>
</tr>
<tr>
<td>Diffie-Hellman problem</td>
<td>51, 54</td>
</tr>
<tr>
<td>Diffie, W.</td>
<td>9, 12, 50, 51, 71, 72, 89, 97, 98, 112, 121, 140, 155, 164</td>
</tr>
<tr>
<td>digital signature</td>
<td>1, 7</td>
</tr>
<tr>
<td>diophantine approximation</td>
<td>81</td>
</tr>
<tr>
<td>discrete exponential bit generator</td>
<td>132</td>
</tr>
<tr>
<td>discrete exponential generator</td>
<td>120</td>
</tr>
<tr>
<td>discrete logarithms</td>
<td>8, 49, 92, 120, 131, 146</td>
</tr>
<tr>
<td>division point method</td>
<td>20, 22</td>
</tr>
<tr>
<td>Dixon, J. D.</td>
<td>24</td>
</tr>
<tr>
<td>Dobkin, D. P.</td>
<td>112</td>
</tr>
<tr>
<td>Donn, J. S.</td>
<td>164</td>
</tr>
<tr>
<td>DOWNRUN</td>
<td>16</td>
</tr>
<tr>
<td>Dubner, H.</td>
<td>16, 25</td>
</tr>
<tr>
<td>e-indistinguishable</td>
<td>123</td>
</tr>
<tr>
<td>Eckmann, J.-P.</td>
<td>117, 140</td>
</tr>
<tr>
<td>Eichenauer, J.</td>
<td>140</td>
</tr>
<tr>
<td>Eier, R.</td>
<td>81, 87</td>
</tr>
<tr>
<td>ElGamal, T.</td>
<td>72, 154, 164</td>
</tr>
<tr>
<td>elliptic curve</td>
<td>19, 38</td>
</tr>
<tr>
<td>elliptic curve factoring method</td>
<td>27, 38, 45</td>
</tr>
<tr>
<td>encryption oracle</td>
<td>129</td>
</tr>
<tr>
<td>entropy</td>
<td>118, 124</td>
</tr>
<tr>
<td>Erdös, P.</td>
<td>12, 72</td>
</tr>
<tr>
<td>Estes, D. R.</td>
<td>152, 163, 164</td>
</tr>
<tr>
<td>Euclid's algorithm</td>
<td>4</td>
</tr>
<tr>
<td>Evertse, J.-H.</td>
<td>72, 164</td>
</tr>
<tr>
<td>expansive</td>
<td>116</td>
</tr>
<tr>
<td>exponentiation ciphers</td>
<td>1</td>
</tr>
<tr>
<td>Faedeva, V. N.</td>
<td>165</td>
</tr>
<tr>
<td>factor base</td>
<td>32, 43</td>
</tr>
<tr>
<td>factoring</td>
<td>4, 27, 131, 146</td>
</tr>
<tr>
<td>factoring polynomials</td>
<td>67</td>
</tr>
<tr>
<td>factorization</td>
<td>53</td>
</tr>
<tr>
<td>Fermat's &quot;little&quot; theorem</td>
<td>4, 14</td>
</tr>
<tr>
<td>Fiat, A.</td>
<td>111, 112</td>
</tr>
<tr>
<td>Fishman, G.</td>
<td>140</td>
</tr>
<tr>
<td>Foregger, T. H.</td>
<td>87, 119</td>
</tr>
<tr>
<td>Friedl, K.</td>
<td>164</td>
</tr>
<tr>
<td>Frieze, A. M.</td>
<td>88, 137, 140</td>
</tr>
<tr>
<td>Frobenius, G.</td>
<td>151, 165</td>
</tr>
<tr>
<td>Frumkin, M. A.</td>
<td>72</td>
</tr>
<tr>
<td>Fuji-Hara, R.</td>
<td>68, 72</td>
</tr>
<tr>
<td>Fujioka, A.</td>
<td>166</td>
</tr>
<tr>
<td>Fürer, M.</td>
<td>115, 140</td>
</tr>
<tr>
<td>Furst, M. L.</td>
<td>88, 115, 140</td>
</tr>
<tr>
<td>Garey, M. R.</td>
<td>88, 119, 140</td>
</tr>
<tr>
<td>Gauss, K. F.</td>
<td>49, 70, 72</td>
</tr>
<tr>
<td>Gauss's class number problem</td>
<td>163</td>
</tr>
<tr>
<td>Gaussian integer method</td>
<td>64</td>
</tr>
<tr>
<td>Gerver, J.</td>
<td>43, 46</td>
</tr>
<tr>
<td>Goldberg, A.</td>
<td>141</td>
</tr>
<tr>
<td>Goldreich, O.</td>
<td>99, 102, 103, 111, 112, 113, 119, 122, 126, 130, 132, 134, 135, 139, 157, 164</td>
</tr>
<tr>
<td>Goldwasser, S.</td>
<td>22, 24, 52, 99, 100, 103, 110, 112, 113, 119, 126, 130, 140, 162, 165</td>
</tr>
<tr>
<td>Goos, G.</td>
<td>112</td>
</tr>
<tr>
<td>Gordon, D. M.</td>
<td>72</td>
</tr>
<tr>
<td>Gowaerts, R.J.M.</td>
<td>81, 87</td>
</tr>
<tr>
<td>Graves-Morris, Peter</td>
<td>164</td>
</tr>
<tr>
<td>greatest common divisor</td>
<td>4</td>
</tr>
<tr>
<td>Günther, C. G.</td>
<td>72</td>
</tr>
<tr>
<td>Gustavson, F. G.</td>
<td>165</td>
</tr>
<tr>
<td>Hafner, J.</td>
<td>50, 165</td>
</tr>
<tr>
<td>hard-core predicate</td>
<td>102, 128</td>
</tr>
<tr>
<td>Hardy, G. H.</td>
<td>49</td>
</tr>
<tr>
<td>Hartmanis, J.</td>
<td>112</td>
</tr>
<tr>
<td>hash function</td>
<td>122</td>
</tr>
<tr>
<td>Hasse, H.</td>
<td>40, 46</td>
</tr>
<tr>
<td>Hastad, J.</td>
<td>99, 107, 113, 119, 122, 128, 140</td>
</tr>
<tr>
<td>Hazlewood, D. G.</td>
<td>73</td>
</tr>
<tr>
<td>Hellman, M. E.</td>
<td>9, 12, 50, 51, 58, 71, 72, 73, 88, 89, 97, 98, 112, 113, 121, 140, 155, 164</td>
</tr>
<tr>
<td>Henry, P. S.</td>
<td>88</td>
</tr>
<tr>
<td>Hermite, C.</td>
<td>153</td>
</tr>
<tr>
<td>Hilbert's basis theorem</td>
<td>138</td>
</tr>
<tr>
<td>Hirschfeld, R.</td>
<td>126, 139</td>
</tr>
<tr>
<td>Holdridge, D. B.</td>
<td>43, 46</td>
</tr>
<tr>
<td>Hopcroft, J. E.</td>
<td>71</td>
</tr>
<tr>
<td>Hua, L. K.</td>
<td>165</td>
</tr>
<tr>
<td>Huang, M.-D.</td>
<td>22, 24</td>
</tr>
<tr>
<td>Huynh, D. T.</td>
<td>117, 140</td>
</tr>
<tr>
<td>identity-based cryptosystems</td>
<td>159</td>
</tr>
<tr>
<td>Imai, H.</td>
<td>165</td>
</tr>
<tr>
<td>Impagliazzo, R.</td>
<td>88, 111, 113, 122, 127, 128, 140, 141</td>
</tr>
<tr>
<td>index calculus method</td>
<td>60</td>
</tr>
<tr>
<td>information</td>
<td>124</td>
</tr>
<tr>
<td>information theory</td>
<td>118</td>
</tr>
<tr>
<td>Ingemarsson, I.</td>
<td>112</td>
</tr>
<tr>
<td>interactive proof systems</td>
<td>107</td>
</tr>
<tr>
<td>inverting circuit</td>
<td>128</td>
</tr>
<tr>
<td>inverting RSA</td>
<td>131</td>
</tr>
</tbody>
</table>
INDEX

IP, 108
Itoh, T., 73
Iwaniec, H., 24
Jacobi, C. G. J., 70, 73
Jacobi sum test, 13, 17, 18
Jacobi symbol, 134
Jannson, B., 141
Johnson, D. S., 88, 119, 140
Jones, A., 112
Jutila, M., 24
Kannan, R., 88, 136, 140, 141
Karloff, H., 141
Karp, P., 119, 129, 141
Kharitonov, M., 141
Kilian, J., 22, 24, 105, 113
Kim, S. H., 12
Kleinberg, E. M., 141
Knapsack cryptosystems, 1, 10, 76
Knapsack problem, 75
Kneading map, 121, 130
Knuth, D. E., 4, 12, 24, 73, 115, 119, 122, 124, 137, 141, 146, 165
Ko, K. 117, 141
Koblitz, N., 11, 73
Kolmogorov, A. N., 117, 118, 141
Kolmogorov-random, 117
Koyania, K., 73
Kraitchik, M., 42, 43, 46, 60, 73
Kranakis, E., 127, 134, 141
Krawczyk, H., 122, 139, 140, 141, 165
Kreher, D. L., 88
Krylov, A. N., 147
Kung, H. T., 133, 140
Lagarias, J. C., 11, 80, 84, 88, 113, 119, 128, 138, 139, 140, 141
Lagger, H., 88
LaMacchia, B., 66, 73, 165
Lee, P. J., 72
Lamé's theorem, 4
Lattice basis reduction algorithm, 84, 136, 138
Legendre symbol, 134
Lehmer, D. H., 24, 43, 46, 72
Lehre, J., 140
Lenstra, A. K., 28, 44, 46, 73, 88, 136, 141, 152
Lenstra, Jr., H. W., 24, 27, 28, 29, 40, 45, 46, 64, 66, 73, 83, 84, 88, 136, 141
Levin, L., 102, 103, 111, 112, 122, 127, 128, 140, 141
Lichtenstein, D., 112
Lidl, R., 165
Limited decryption oracle, 130
Linear congruential generators, 137
Linear feedback shift registers, 149
Linear sieve, 64
Lipton, R., 99, 113, 119, 129, 140, 141
Long, D. L., 6, 12, 55, 73, 132, 156, 165
Lovász, L., 84, 88, 136, 141
Low-density knapsacks, 80
Luby, M., 111, 113, 119, 121, 122, 127, 128, 130, 139, 140, 141
Lund, C., 164
Manasse, M. S., 28, 44, 46, 73
Manders, K., 112
Marsaglia, G., 119, 122, 124, 141
Martin-Löf, P., 117, 141
Massey, J. L., 73, 141, 148, 149, 165
Matsumoto, T., 165
Maurer, U. M., 141
McClellan, J. H., 165
McCready, E. M., 117, 142
McCurley, K. S., 71, 73, 120, 163, 164, 165
McLellan, V., 165
Menezes, A., 70, 73
Merkle-Hellman cryptosystem, 79
Merkle, R. C., 12, 60, 73, 88, 113
Meyer, A. R., 117, 142
Micali, S., 55, 72, 99, 100, 110, 111, 112, 113, 118, 120, 126, 127, 129, 130, 132, 135, 139, 140, 142, 165
Miller, G. L., 14, 24, 112
Miller, J. C. P., 74
Miller, V., 73
Modified Rabin bit generator, 131, 134
Modified square generator, 134
Montgomery, P. L., 43, 45, 46, 162, 165
Moore, L., 140
Morain, F., 24
Morrison, M., 46
Mullin, R. C., 68, 72
Multiple polynomial variation, 33
Multiplicative congruential generator, 119
Multivariate polynomial congruences, 152
Naor, M., 88, 111, 122, 142, 165
Needham, R. M., 50
Negligible probability, 129
Network implementations, 44
Niederreiter, H., 124, 142, 165
Nisan, N., 117, 139, 142
Nonlinearity, 117
Nonuniform models of computation, 118
Nonuniform next-bit test, 126
Nonuniform one-way collection, 127
Number field sieve, 28
Oblivious transfer, 105
Odlyzko, A. M., 11, 18, 50, 64, 66, 67, 68, 69, 71, 72, 73, 80, 84, 87, 88, 113, 142, 145, 155, 161, 164, 165
Odoni, R. W. K., 73
Ohta, K., 73
Okamoto, E., 73, 159, 165
Okamoto, T., 70, 73
\( \frac{1}{p} \) generator, 119, 136
one-time pad, 116
one-way collection of circuits, 128
one-way function, 50, 93, 111, 118, 127
one-way predicates, 95
Ong, H., 152, 154, 165
Orponen, P., 141

\( p - 1 \) factoring method, 37, 45
Peralta, R., 55, 73, 112, 166
perfect zero-knowledge, 110
permuted kernel problem, 161
Peterson, G. L., 117, 142
Pocklington, H. C., 24
Pocklington’s theorem, 16
Pohlig, S. C., 58, 73
Pollard, J. M., 28, 45, 46, 60, 65, 73, 74, 152, 153, 154, 166
polynomial equations, 161
polynomial length-increasing, 125
polynomial size, 125
polynomial time, 3
polynomial-time indistinguishable, 99
polynomially indistinguishable, 125
Pomerance, C., 12, 18, 24, 25, 27, 29, 43, 44, 46, 52, 64, 66, 72, 73, 145, 163
power generator, 120
Powers, R. E., 43, 46
predicting collection, 126
prediction problems, 136
primality testing, 4, 13
primality testing using elliptic curves, 19, 21
principal square root, 120
private-key block cryptosystem, 129
private key cryptosystem, 116
probabilistic encryption, 100
probabilistic compositeness test, 15
probabilistic polynomial-time algorithms, 132, 133, 134
probable prime, 15
pseudorandom bit generators, 116; 123, 125
pseudorandom bits, 116
pseudorandom number generators, 116
pseudorandom sequences, 148
pseudosquares, 91
public key, 1, 7
public-key encryption, 97
Purdy, G. B., 133, 142, 166
quadratic residue(s), 91, 120
quadratic residuosity, 91, 101, 157
quadratic sieve factoring method, 27, 29, 43
Rabin, M. O., 25, 91, 95, 105, 113, 131, 142, 166
Rackoff, C., 99, 110, 112, 113, 121, 129, 130, 141, 142
Rader, C. M., 165
Radziszowski, S. P., 88
Raghavan, P., 141
random bits, 115
random curve test, 14, 22
random functions, 130
random primes, 6
reconstruction problems, 136
reduced basis, 84
Reeds, J., 119, 122, 138, 139, 141
Reif, J. H., 142
repeated doubling method, 41
repeated squaring algorithm, 3
Reynier, J. M., 73
Ribenboim, P., 25
Riesel, H., 25, 74
Rineisen, R. D., 87
Rivest, R. L., 6, 12, 74, 79, 87, 99, 113, 120, 142, 155, 165, 166
Roberts, F. S., 87
Rogaway, P., 113
Rompel, J., 122, 128, 142
Roof, H., 139
RSA cryptosystem, 1, 6, 95, 97, 98, 99, 120, 155, 156, 162
RSA bit generator, 120, 131
Rubinsteins, R. Y., 119, 142
Rudich, S., 141
Rueppel, R. A., 166
Rumely, R. S., 24, 25
Sanders, P. W., 73
Savage, J., 119, 142
Schnorr, C. P., 74, 88, 102, 112, 132, 134, 135, 139, 142, 152, 154, 157, 164, 165, 166
Schöning, U., 141
Schoof, R. J., 20, 22, 25, 40
Schrift, A. W., 135, 142
Schroeppe, R., 64, 72, 164
Schuster, R. G., 115, 116, 142
second step, 42
secret-exchange, 106
secret-key cryptosystem, 96
secure private-key block cryptosystem, 129
seed, 116
self-initialization, 36
Selfridge, J. L., 24, 25, 72
INDEX

semantically secure, 100
Shallit, J., 46, 166
Shamir, A., 6, 9, 11, 12, 74, 79, 80, 81, 82, 88, 99, 107, 111, 112, 113, 117, 120, 132, 133, 135, 139, 140, 142, 152, 154, 155, 159, 161, 165, 166
Shanks, D., 56, 57, 59, 74
Shannon, C., 89, 99, 113, 118, 119, 142, 148, 166
Shub, M., 112, 119, 120, 136, 139, 164
Silver, R., 58
Silverman, J. H., 25, 45, 46
Silverman, R. D., 44, 45, 46
Simmons, G. J., 43, 46
Sipser, M., 142
Sloan, R. H., 99, 113, 129, 140
smooth integers, 27, 58
sparse linear systems, 147
square generator, 120
statistic, 123
statistical test, 123
statistically zero-knowledge, 110
Stern, J., 142
Stockmeyer, L., 140, 142
subset-sum problem, 10, 75
superincreasing sequences, 10, 77
Szegedy, M., 139

$^T$-incompressible, 117
$^T$-pseudorandom number generator, 123
Tanaka, K., 159, 165
Tedrick, T., 112
Tijdeman, R., 24
Tong, P., 112
trapdoor functions, 94
trapdoor predicates, 95
trial division, 4
Trilling, S., 127, 142
truncation operator, 122
Tsay, L.-U., 141
Tsujii, S., 73, 166
Tuckerman, B., 24, 72
two-party protocols, 104
Tygar, J. D., 142
Ullman, J. D., 71

uniform models of computation, 118
uniform polynomial pseudorandom bit generator, 125
unpredictability paradox, 118
user identification, 111
Uspenskii, V. A., 141

Vallée, B., 27, 47
van de Graf, J., 72, 164, 166
van der Hulst, M.-P., 24
Vandewalle, J. P., 81, 87
van Heyst, E., 164
Vanstone, S., 68, 70, 72, 73
Varadharajan, V., 73
Vazirani, U. V., 113, 135, 143
Vazirani, V. V., 113, 135, 143
vector recurrences, 138
Wagstaff, Jr., S. S., 24, 25, 72, 74
Watanabe, O., 141
Waterhouse, W. C., 40
Western, A. E., 74
Wiedemann, D. H., 67, 74, 147, 166
Wiedemann’s coordinate recurrence method, 67, 147
Wigderson, A., 55, 73, 111, 112, 117, 132, 135, 142
Wilbur, R. E., 117, 142
Wilf, H. S., 88
Wilkes, M. V., 74
Williams, H. C., 16, 25, 45, 72, 92, 163, 164, 166
Williamson, K., 139
Winograd, S., 164
witness, 14
Wolfram, S., 121, 139, 143
Woll, H., 143, 166
Wunderlich, M. C., 25

Yacobi, Y., 72
Yao, A., 124, 126, 141, 143
Yung, M., 122, 141, 142, 165

zero knowledge, 90, 107, 109, 162
Zuckerman, D., 141
Other Titles in This Series

(Continued from the front of this publication)

20  J. P. LaSalle, editor,  The influence of computing on mathematical research and education
    (University of Montana, August 1973)
19  J. T. Schwartz, editor,  Mathematical aspects of computer science (New York City, April
    1966)
18  H. Grad, editor,  Magneto-fluid and plasma dynamics (New York City, April 1965)
17  R. Finn, editor,  Applications of nonlinear partial differential equations in mathematical
    physics (New York City, April 1964)
16  R. Bellman, editor,  Stochastic processes in mathematical physics and engineering (New
    York City, April 1963)
15  N. C. Metropolis, A. H. Taub, J. Todd, and C. B. Tompkins, editors,  Experimental
    arithmetic, high speed computing, and mathematics (Atlantic City and Chicago, April
    1962)
14  R. Bellman, editor,  Mathematical problems in the biological sciences (New York City,
    April 1961)
13  R. Bellman, G. Birkhoff, and C. C. Lin, editors,  Hydrodynamic instability (New York
    City, April 1960)
12  R. Jakobson, editor,  Structure of language and its mathematical aspects (New York City,
    April 1960)
11  G. Birkhoff and E. P. Wigner, editors,  Nuclear reactor theory (New York City, April
    1959)
10  R. Bellman and M. Hall, Jr., editors,  Combinatorial analysis (New York University, April
    1957)
  G. Birkhoff and R. E. Langer, editors,  Orbit theory (Columbia University, April 1958)
  L. M. Graves, editor,  Calculus of variations and its applications (University of Chicago,
    April 1956)
  L. A. MacColl, editor,  Applied probability (Polytechnic Institute of Brooklyn, April 1955)
  J. H. Curtiss, editor,  Numerical analysis (Santa Monica City College, August 1953)
  A. E. Heins, editor,  Wave motion and vibration theory (Carnegie Institute of Technology,
    June 1952)
  M. H. Martin, editor,  Fluid dynamics (University of Maryland, June 1951)
  R. V. Churchill, editor,  Elasticity (University of Michigan, June 1949)
  A. H. Taub, editor,  Electromagnetic theory (Massachusetts Institute of Technology, July
    1948)
  E. Reissner, editor,  Non-linear problems in mechanics of continua (Brown University,
    August 1947)